國 立 政 治 大 學 應 用 數 學 系

碩 士 學 位 論 文

Deformation Theory of Representations of Profinite Groups

投射有限群表現之形變理論

碩士班學生: 周惠雯 撰

指導教授: 余屹正 博士

中華民國一百零二年一月三日

Mathematical science is in my opinion an indivisible whole, an organism whose vitality is conditioned upon the connection of its parts.

DAVID HILBERT, «Mathematical Problems»

謝　辭

滿紙荒唐言, 一把辛酸淚;
都云作者痴, 誰解其中味?　　　　　　　　　— 曹雪芹

在政大應數念了兩年半的書, 第一位要感謝的人就是我的指導教授: 余屹正老師。余老師在數學上的熱情是無可比擬的!他在課業上的要求異常嚴格、也很有耐心, 撥出很多時間答覆我的問題, 空出私人的時間幫我上課、教我寫習題, 也告訴我如何尋找參考資料, 時時關心我念書的進度, 逐字逐句批改我的論文, 讓我寫出來的的東西越來越嚴謹。我能順利地拿到學分、通過資格考以及完成論文的撰寫, 完全多虧了余老師, 他使我整個碩士生涯獲益良多、充滿驚奇。

第二位要感謝的是陳天進老師。實變函數論的課程內容對我來說相當的困難, 經過陳老師上課的講解, 並且補充了課本沒有的教材, 這些種種對我在消化課文、寫習題上幫助很大, 減輕我在學習過程中的負擔。陳老師教學非常的認真, 上課內容分量很豐富、也很完整, 修過陳老師所開的課之後, 感覺都很充實。

最後, 要感謝我的父母給予我的支持, 讓我順利的完成學業。

此篇論文獻給所有教過我的老師們、我的家人和朋友。

周惠雯 謹誌于

國立政治大學應用數學系

中華民國一百零一年十二月

Abstract

In this master thesis, we give an exposition of the deformation theory of representations for $\mathbf{GL}_1$ and $\mathbf{GL}_2$, respectively, of certain profinite groups. We give rigidity conditions of the fixed representation and verify several conditions for the representability. Finally, we interpret the Zariski tangent spaces of respective universal deformation rings as certain group cohomology and calculate the universal deformation for $\mathbf{GL}_1$.

Keywords: Profinite groups; Representations; Deformations; Universal deformations; Universal deformation rings; Zariski tangent space; Group cohomology

摘 要

在本碩士論文中, 我們闡述了投射有限群表現, 以及其形變理論。我們亦特別研究這些表示在 $\mathbf{GL}_1$ 和 $\mathbf{GL}_2$ 之形變, 並且給了可表示化的判定準則。最後, 我們解釋相對應的泛形變環之扎里斯基切空間與群餘調之關連, 並計算了 $\mathbf{GL}_1$ 的泛形變表現。

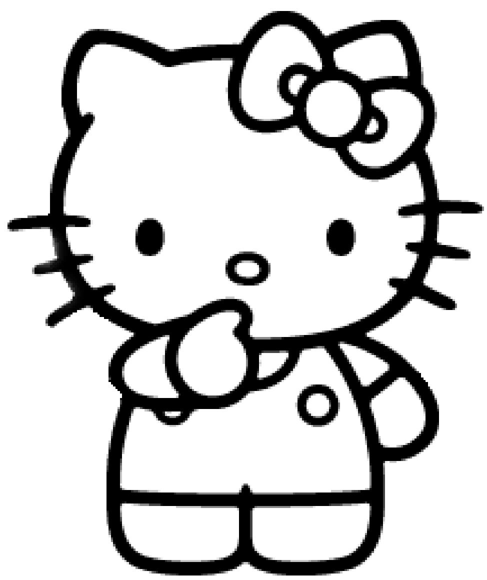
關鍵字:投射有限群; 表現; 形變; 泛形變; 泛形變環; 扎里斯基切空間; 群餘調

Notations

Item	Meaning
$\varnothing$	the empty set
$X \smallsetminus Y$	the set-theoretic difference of X and Y
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	integers, rationals, reals, complex numbers
p	a prime integer
G	a profinite group
$\mathbb{Z}_p$	the ring of p-adic integers
$\mathbb{Q}_p$	the field of p-adic numbers
$\mathrm{Gal}(L/K)$	the Galois group of the field extension L/K
$\mathbb{Q}_S$	the maximal separable extension of $\mathbb{Q}$ unramified outside S
G_S	$\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$
$\mathbf{GL}_n$	the general linear group of degree n
$\mathcal{G}$	a connected reductive group (usually stands for $\mathbf{GL}_1$ or $\mathbf{GL}_2$ in this master thesis)
k	a finite field of characteristic p
$\overline{\rho} : G \to \mathcal{G}(k)$	a fixed representation
$\underline{\mathrm{Hom}}(A, B)$	the set of all continuous homomorphisms $A \to B$
$W(k)$ or W	the ring of Witt vectors of k
$\mathrm{Ad}(\overline{\rho})$	the two-by-two matrices over k with G-action through $\overline{\rho}$ and by conjugation
$\underline{\mathbf{Sets}}$	the category of sets
$\underline{\mathbf{CNL}}_W$	the category of complete noetherian local W-algebras with residue field k
$\underline{\mathbf{CNL}}_W^0$	the subcategory of $\underline{\mathbf{CNL}}_W$ consisting of artinian objects
$\mathscr{D}_{\overline{\rho}}$ or $\mathscr{D}$	the deformation functor of $\overline{\rho}$

Contents

Dedicated to my immortal beloved …



Chapter 1

Introduction

First Scene:

An open place, Thunder and lighting.
Enter three witches.

Shakespeare, *Macbeth, Act I*

Nowadays, the idea to study deformations of representations of profinite groups is the achievement of the full Taniyama-Shimura-Weil conjecture proved by Diamond [7], Conrad, Diamond & Taylor [5], and Breuil et al. [2]. However, the concept goes back to the seminal article of Mazur [20]. Mazur's motivation was to give a conceptual framework for some discoveries of Hida [13] on ordinary families of Galois representations. It was the work of Wiles on Fermat's Last Theorem which made clear the importance of deformation theory developed by Mazur. The theory was a key technical tool in the proof by Wiles and Taylor-Wiles of Fermat's Last Theorem; cf. [31, 29].

Mazur's theory gives one a universal deformation ring which can be thought of as a parameter space for all lifts of a given residual representation (up to conjugation). The ring depends on the residual representation and on supplementary conditions one imposes on the lifts. If the residual representation is modular and if the deformation conditions are such that the p-adic lifts satisfy conditions that hold for modular Galois representations, then one expects in many cases that the natural homomorphism $R \to \mathbb{T}$ from the universal deformation ring R to a suitably defined Hecke algebra $\mathbb{T}$ is an isomorphism. The proof of such isomorphisms, called $R = \mathbb{T}$-theorems, is at the heart of the proof of Fermat's Last Theorem. It expresses that all p-adic Galois representation of the type described by R are modular and in particular they arise from geometry.

Many refinements of Wiles' methods have since been achieved and the theory has been vastly generalized to various settings of automorphic forms. $R = \mathbb{T}$ theorems, lie at the basis of the proof of the Taniyama-Shimura conjecture by Breuil, Conrad, Diamond and Taylor, the Sato-Tate conjecture by Clozel, Harris, & Taylor [4], Harris, Shepherd-Barron & Taylor [12], and Taylor [28], and the the Serre conjecture by Khare-Wintenberger [14, 15]. The proof of Fermat's Last Theorem was also the first strong evidence to the conjectures of Fontaine and Mazur [8]. This conjecture says that if a p-adic Galois representation satisfies certain local conditions that hold for Galois representations which arise from geometry, then this representation occurs in the p-adic étale cohomology of a variety over a number field. In fact, it is a major motivation for the formulation of the standard conditions on deformation functors. These conditions should (mostly) be local and reflect a geometric condition on a representation. Due to work of Emerton and independently Kisin [16], there has been much progress on the Fontaine-Mazur conjecture over $\mathbb{Q}$.

This master thesis focusses solely on the Mazur's deformation theory, especially for $\mathbf{GL}_1$ or $\mathbf{GL}_2$. Generally, one can also consider the representations into certain connected reductive groups; cf. Tiloiune [30]. The obstruction theory and the deformation conditions are left untouched; cf. Mazur [20, 21].

The subject of *Fourier transforms* is already implicitly such a theory: the exponential function is the equipment one needs to produce a canonical parametrization of the *"universal family"* of one-dimensional continuous complex unitary representations of the real line $\mathbb{R}$, viewed as a Lie group. For each real number a, putting $\chi_a(x) := \exp(2\pi i a x)$ we have that the universal family of representations of the above type is given parametrically by

$$\begin{aligned} \mathbb{R} &\rightarrow \underline{\mathrm{Hom}}(\mathbb{R}, \mathbb{C}^{\times}) \\ a &\mapsto \chi_a. \end{aligned}$$

This parameter space itself is again, canonically, the Lie group $\mathbb{R}$, and this miracle has repercussions throughout mathematics.

Generally speaking, the *"universal parametrization"* of all one-dimensional continuous complex unitary representations of any locally compact commutative topological group is treated by the theory of Pontrjagin. If G is a locally compact topological group, the *"Pontrjagin dual"* of G

$$\widehat{G} := \underline{\mathrm{Hom}}(\mathbb{R}, \mathbb{C}^{\times})$$

is the group parametrizing all degree one continuous unitary $\mathbb{C}$-valued representations of G. The fact that this parameter space of representations, $\widehat{G}$, is again a commutative locally compact topological group is key to the further elaboration of Pontrjagin's theory.

The more general question of appropriate parametrizations of finite, or infinite, dimensional linear representations of a given type, for a given group, is, of course, one of the great ongoing subjects for our studies. And the natural structure(s) that these parameter spaces come equipped with is, again, key to any further detailed study.

Let k be a finite field of characteristic p and let $W(k)$ be the ring of Witt vectors of k. Consider the category $\underline{\mathbf{CNL}}_W$ of the complete noetherian local W-algebras A with a surjective local homomorphism $\varphi : A \to k$; the morphisms of $\underline{\mathbf{CNL}}_W$ are the local W-algebra homomorphisms commute with the φ's.

A *representation* of the profinite group G is a continuous homomorphism

$$\rho : G \to \mathcal{G}(A),$$

where A is a topological, separated, commutative ring and $\mathcal{G}$ is a connected reductive group. We say that $(A, \widetilde{\rho})$ is a *lift* of ρ over A if A is an object in $\underline{\mathbf{CNL}}_W$ and $\widetilde{\rho}$ is a representation for which the following diagram commutes:

$$\begin{tikzcd} & \mathcal{G}(A) \arrow[d, "\varphi"] \\ G \arrow[ur, "\widetilde{\rho}"] \arrow[r, "\rho"'] & \mathcal{G}(k) \end{tikzcd}$$

where φ is the corresponding group homomorphism $\mathcal{G}(A) \to \mathcal{G}(k)$ induced by $\varphi : A \to k$. Two lifts $\widetilde{\rho}_1$ and $\widetilde{\rho}_2$ of ρ over A are said to be *strictly equivalent* if there exists a matrix M in $\ker(\mathcal{G}(A) \to \mathcal{G}(k))$ for which $\widetilde{\rho}_1(g) = M\widetilde{\rho}_2(g)M^{-1}$ for every g in G. An equivalence class of lifts is called a *deformation* of ρ.

For a representation $\rho : G \to \mathcal{G}(k)$, the *universal deformation ring* R is a lift (R, ρ^{u}) for which the following universal property holds: for any lift $(A, \widetilde{\rho})$ of ρ there exists a unique homomorphism $\varphi : R \to A$ such that the following diagram commutes:

$$\begin{tikzcd} & \mathcal{G}(R) \arrow[d, "\varphi"] \\ G \arrow[ur, "\rho^{\mathrm{u}}"] \arrow[r, "\widetilde{\rho}"'] & \mathcal{G}(A) \end{tikzcd}$$

We say that the profinite group G satisfies the *p-finiteness condition* Φ_p if for all open subgroups $G_0 \subset G$ of finite index, there are only a finite number of continuous homomorphisms from G_0 to $\mathbb{Z}/p\mathbb{Z}$. The main theorem is stated as follows:

Theorem (Mazur [20], Ramakrishna [23]). *Let $\mathcal{G}$ be $\mathbf{GL}_1$ or $\mathbf{GL}_2$. Suppose that G is a profinite group satisfying the p-finiteness condition Φ_p and $\overline{\rho} : G \to \mathcal{G}(k)$ is an absolutely irreducible representation. Then there exists a universal deformation ring R in $\underline{\mathbf{CNL}}_W$ and a universal deformation ρ^{u} of $\overline{\rho}$ to R,*

$$\rho^{\mathrm{u}} : G \to \mathcal{G}(R)$$

such that any deformation of $\overline{\rho}$ to a complete noetherian local W-algebra A is obtained from ρ^{u} via a unique morphism $R \to A$.

However de Smit and Lenstra proved in [6], following an argument due to Faltings, that we can skip the hypothesis of absolute irreducibility if we require the weaker condition $Z_{\overline{\rho}} = k$ for the representation $\overline{\rho} : G \to \mathcal{G}(k)$.

The structure of this master thesis is organized as follows: Chapter 1 gives a brief review of the theory of profinite groups and their representations. In Chapter 2, we explores the foundations of Mazur's theory on deformations. We also interpret the Zariski tangent spaces of universal deformation rings as certain group cohomology. Finally, in Chapter 3 we apply the deformation theory to representations and verify the representability conditions of Schlessinger's criteria. In the process, we shall see where the assumptions for the representability are needed. We also study the 1-dimensional representations, and we will compute the universal deformation ring. The two appendices on categories and functors and on group cohomology provide some fundamental facts we use freely in this master thesis.

Much of the current perspective on deformations of Galois representations is due to work of M. Kisin as is clear to everyone familiar with the topic. Moreover, we found his lecture notes [17] and his paper [18] are very helpful.

Chapter 2

Profinite Groups and their Representations

Algebra is the offer made by the devil to the mathematician. The devil says: "I will give you this powerful machine, it will answer any question you like. All you need to do is give me your soul: give up geometry and you will have this marvelous machine."

Michael Atiyah

In this chapter, we give an exposition of the theory of profinite groups and their representations. We also introduce a finiteness condition which is one of the crucial conditions for deformation theory. One can consult Serre's [27] or Neukirch's [22] books for further information on profinite groups.

§ 2.1. Projective limits

A *partial order* is a binary relation "$\leq$" over a set I which is *reflexive*, *antisymmetric*, and *transitive*, i.e., for all a, b, and c in I, we have that:

(a) $a \leq a$ (reflexivity);

(b) if $a \leq b$ and $b \leq a$, then $a = b$ (antisymmetry);

(c) if $a \leq b$ and $b \leq c$, then $a \leq c$ (transitivity).

A set with a partial order is called a *partially ordered set*. For example, the real numbers ordered by the standard *less-than-or-equal* relation $\leq$ and the set of natural numbers equipped with the relation of *divisibility* are partially ordered sets.

A *directed set* I is a partially ordered set such that for all $i, j \in I$ there exists a $k \in I$ with $i \leq k$ and $j \leq k$.

Definition 2.1.1. Let I be a directed set.

(1) A *projective system* of sets (groups, rings, etc.) indexed by I is a family $\mathcal{P} = \{I, S_i, f_{ij}\}$ of sets (groups, rings, etc.) S_i and maps (homomorphisms) $f_{ij} : S_j \to S_i$ such that

$$f_{ii} = \mathrm{id}_{S_i} \text{ for each } i \in I, \text{and } f_{ik} = f_{ij} \circ f_{jk} \text{ whenever } i \leq j \leq k.$$

(2) We say that $S = \varprojlim_{i \in I} S_i$ is a *projective limit* of the projective system $\mathcal{P}$ if it satisfies two conditions:

(a) S comes equipped with maps (homomorphisms) $f_i : S \to S_i$ for each $i \in I$ such that $f_i = f_{ij} \circ f_j$ if $i \leq j$.

(b) S is *universal*, i.e., for any other set (groups, rings, etc.) S' and any maps (homomorphisms) $g = \{g_i\}_{i \in I} : S' \to \mathcal{P}$, there exists a unique homomorphism $h : S' \to S$ such that $g_i = f_i \circ h$ for all $i \in I$.

To show the existence of S, we only have to let S be defined as the following set (group, ring, etc.)

$$S = \left\{ (\sigma_i)_{i \in I} \in \prod_{i \in I} S_i \,\middle|\, f_{ij}(\sigma_j) = \sigma_i \text{ if } i \leq j \right\}.$$

If the S_i are topological spaces and the f_{ij} are continuous maps, then S is a closed subspace of the topological space $\prod_{i \in I} S_i$.

§ 2.2. *Profinite groups*

A group G is called a *topological group* if it is a group and a topological space at the same time, and the group operations are continuous. Thus, the product: $(a, b) \mapsto ab$ and the inverse: $a \mapsto a^{-1}$ are continuous maps. The map $a \mapsto a^{-1}$ is a homeomorphism since it is an involution. If G is a topological group, for a fixed element $a \in G$, these two maps $g \mapsto ag$ and $g \mapsto ga$ are continuous by the continuity of the product. Thus, the left and the right multiplications are homeomorphisms. If the collection $\mathcal{U} = \{U\}$ is a system of open neighborhoods of the identity 1_G of G, then $a\mathcal{U} := \{aU \mid U \in \mathcal{U}\}$ and $\mathcal{U}a := \{Ua \mid U \in \mathcal{U}\}$ are systems of open neighborhoods of a in G.

Definition 2.2.1. A topological group G which is the projective limit of finite groups $\{G_i\}_{i\in I}$, each equipped with the discrete topology, is called a *profinite group*.

As we give these finite groups the discrete topology, they are then compact as topological spaces. By a theorem of Tychonoff, their product with product topology is then compact. Hence, G carries a natural compact Hausdorff topology.

Suppose G is a profinite group, so that $G = \varprojlim_{i\in I} G_i$, and let $K_i := \ker(f_i : G \to G_i)$. Then K_i is an open subgroup of G and $\mathcal{U} = \{K_i\}$ forms a basis of open neighborhoods of the identity of G. If $U \in \mathcal{U}$, then $G = \bigcup_{a\in G} aU$ is an open covering. By the compactness of G, we can find a finite subcovering such that $G = \bigcup_{i=1}^{h} aU$. This shows that any open subgroup $U \in \mathcal{U}$ is of finite index. Since G is compact, it is Hausdorff, and hence $\bigcap_{U\in\mathcal{U}} U = \{1_G\}$.

The following result gives an intrinsic characterization of profinite groups.

Theorem 2.2.2. *Let G be a compact Hausdorff group. Then the following assertions are equivalent:*

(i) G is profinite;

(ii) G is totally disconnected, i.e., the connected component of any point is the singleton set consisting only that point;

(iii) There is a collection $\mathcal{U}$ consisting of open normal subgroups of G that form a full system of neighborhoods of the identity in G.

Example 2.2.3. If p is a prime integer, then the rings $\mathbb{Z}/p^n\mathbb{Z}$, $n \in \mathbb{N}$, form a projective system with respect to the canonical projections $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$, $n \geq m$. The projective limit

$$\mathbb{Z}_p := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$$

is the *ring of p-adic integers*. $\mathbb{Z}_p$ is a pro-p-group, that is, a projective limit of finite p-groups.

Example 2.2.4. The rings $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$, form a projective system with respect to the projections $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for $m|n$, where the order in $\mathbb{N}$ is given by the divisibility $m|n$. The projective limit

$$\widehat{\mathbb{Z}} := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$$

is called the *Prüfer ring*. By the Chinese remainder theorem and passing to the projective limit, we have a canonical decomposition

$$\widehat{\mathbb{Z}} = \prod_{p\text{: prime}} \mathbb{Z}_p.$$

Example 2.2.5. Let L/K be a Galois extension of fields. The Galois group $\mathrm{Gal}(L/K)$ of this extension is, by construction, the projective limit of the Galois groups $\mathrm{Gal}(L_i/K)$ of the finite Galois extensions L_i/K which are contained in L/K; thus, it is a profinite group.

Example 2.2.6. A compact analytic group over the p-adic field $\mathbb{Q}_p$ is profinite, when viewed as a topological group. In particular, $\mathbf{SL}_n(\mathbb{Z}_p)$, $\mathbf{Sp}_{2n}(\mathbb{Z}_p)$, $\mathbf{GL}_n(\mathbb{Z}_p), \ldots$ are profinite groups.

§ 2.3. *Representations of profinite groups*

Let A be a topological, separated, commutative ring and let $\mathcal{G}$ be a connected reductive group.

Definition 2.3.1. A *representation* of the profinite group G is a continuous homomorphism

$$\rho : G \to \mathcal{G}(A);$$

here we equip G with the profinite topology and $\mathcal{G}(A)$ with the linear topology induced by A.

For example, let $\mathcal{G} = \mathbf{GL}_n$; we will consider the following kinds of topological rings A:

(i) *Artin representations*, i.e., $A = \mathbb{C}$, equipped with its usual topology. Because all compact totally disconnected subgroups of $\mathbf{GL}_n(\mathbb{C})$ are finite, these representations have finite image. (Cf. **Proposition 2.3.2**.)

(ii) *Mod p representations*, i.e., A is a finite field of characteristic p, or more generally, finite rings, like $\mathbb{F}_q$ (the finite field with q elements) or $(\mathbb{Z}/p^3\mathbb{Z})[X,Y]/(X^4,(X+Y)^2,Y^7)$.

We shall always equip them with the discrete topology. These representations arise from elliptic curves and modular forms, and they are the ones that Serre's conjecture tries to describe.

(iii) *p-adic representations*, i.e., $A = \mathbb{Z}_p$, $\mathbb{Q}_p$, or more generally a finite dimensional $\mathbb{Q}_p$-algebra. In this case, A is endowed with its natural topology of normed vector space over $\mathbb{Q}_p$, for which it is a topological $\mathbb{Q}_p$-algebra. The image of $G_{\mathbb{Q}}$ may be infinite (See the **Example 2.3.3** below).

(iv) Affinoid algebras over $\mathbb{Q}_p$. These are the natural coefficients when considering families of representations with coefficients of type (iii), which are exactly the zero-dimensional affinoid algebras.

(v) Any other interesting topological ring!

Proposition 2.3.2. *Suppose $A = \mathbb{C}$ and that G is a profinite group. Then every continuous representation $\rho : G \to \mathcal{G}(\mathbb{C})$ has finite image.*

Proof. It suffices to prove in the case $\mathcal{G} = \mathbf{GL}_n$. We give $\mathbb{C}^n$ the Euclidean norm: $|(x_1, \ldots, x_n)| = \sqrt{\sum_i |x_i|^2}$. For each linear transformation T on $\mathbb{C}^n$, we define $\|T\| = \sup_v |T(v)|$ where v runs through the $(n-1)$-dimensional sphere of radius 1. Then $\|\cdot\|$ is a well-defined norm and the topology of $\mathbf{GL}_n(\mathbb{C})$ is given by $\|\cdot\|$.

We will show that the identity matrix $\mathbb{1}$ is an isolated point; hence, by the compactness the image of ρ is finite.

Choosing a sufficiently small open (and hence compact) subgroup H of G, we may assume that $\rho(H)$ is contained in the open disk of radius $\frac{1}{2}$ centered at $\mathbb{1}$. Suppose that $T = \rho(u) \neq \mathbb{1}$ for $u \in H$. If all eigenvalues of T equal to 1, then the Jordan canonical form of T has non-diagonal entry. Thus for some large positive integer N, $\|T^N - \mathbb{1}\| > \frac{1}{2}$, a contradiction. Then T has an eigenvalue $\alpha \neq 1$. If $|\alpha| \neq 1$, it is obvious that $|\alpha^N - 1| > \frac{1}{2}$ for some large integer $|N|$. If $|\alpha| = 1$, the argument of α is small. Thus for an appropriate N, $|\alpha^N - 1| > \frac{1}{2}$, a contradiction. This shows that $\rho(H) = \{\mathbb{1}\}$. Since $[G : H] < \infty$, $\rho(G)$ is a finite group. ■

Example 2.3.3. Let $G_{\mathbb{Q}}$ be the absolute Galois group of $\overline{\mathbb{Q}}$ over $\mathbb{Q}$. Take $A = \mathbb{Q}_p$ and $\mathcal{G} = \mathbb{G}_m = \mathbf{GL}_1$. Let $\underline{\mathrm{Hom}}(G_{\mathbb{Q}}, \mathbb{G}_m(\mathbb{Q}_p))$ denote the set of all continuous homomorphisms from $G_{\mathbb{Q}}$ into $\mathbb{G}_m(\mathbb{Q}_p)$. We have

$$\underline{\mathrm{Hom}}(G_{\mathbb{Q}}, \mathbb{G}_m(\mathbb{Q}_p)) = \underline{\mathrm{Hom}}(G_{\mathbb{Q}}, \mathbb{Z}_p^\times) = \underline{\mathrm{Hom}}(G_{\mathbb{Q}}, \mu) \times \underline{\mathrm{Hom}}(G_{\mathbb{Q}}, 1 + q\mathbb{Z}_p),$$

where μ is the torsion subgroup of $\mathbb{Z}_p^\times$ and $q = 4$ if $p = 2$, $q = p$ if $p \neq 2$. Since $1 + q\mathbb{Z}_p$ is a pro-p abelian group, we have

$$\underline{\mathrm{Hom}}(G_{\mathbb{Q}}, 1 + q\mathbb{Z}_p) = \underline{\mathrm{Hom}}(G_{\mathbb{Q}}^{p-\mathrm{ab}}, 1 + q\mathbb{Z}_p)$$

where $G_{\mathbb{Q}}^{p-\mathrm{ab}}$ is the largest abelian pro-p quotient of $G_{\mathbb{Q}}$. The *Class Field Theory* implies that if $S \supset S_p := \{v \text{ place of } F | \; v|p\}$, then $G_{\mathbb{Q}}^{p-\mathrm{ab}}$ has positive $\mathbb{Z}_p$-rank, hence there exists a continuous representation $\rho : G_{\mathbb{Q}} \to \mathbf{GL}_1(\mathbb{Q}_p)$ with infinite image.

In this example, the assumption that S contains $S_p := \{v \text{ place of } F | \; v|p\}$ is essential in order to get *"interesting"* S-ramified Galois representation.

***Remark* 2.3.4.** Let $\mathcal{G}$ be a connected reductive group over a number field F, and let $G_{F,S} = \mathrm{Gal}(\overline{F}_S/F)$. Let K be a p-adic field with the ring of integers $\mathcal{O}$. The generalization of class field theory can be formulated as follows. Consider the space $Y_{\mathcal{G}} = \underline{\mathrm{Hom}}(G_{F,S}, \mathcal{G}(K))$ with the $\mathcal{G}(K)$-action by conjugation.

(i) Find a *"good"* parametrization of the quotient space $X_{\mathcal{G}} = \underline{\mathrm{Hom}}(G_{F,S}, \mathcal{G}(K))/\mathcal{G}(K)$.

(ii) Find a *"large"* complete noetherian local $\mathcal{O}$-algebra A and elements ρ in $X_{\mathcal{G}}(A) = \underline{\mathrm{Hom}}(G_{F,S}, \mathcal{G}(A))/\mathcal{G}(A)$ with *"large"* image.

There are two sources for these. Firstly, the Langlands correspondence. Secondly, the theory of motives via p-adic realization. Langlands' vision is that these two sources (arithmetic automorphic forms and motives) give the same collection of ρ's!

We have a blueprint for the future development programs as follows. Consider

(A) the set of arithmetic automorphic forms on $\mathcal{G}(\mathbb{A}_F)$ with eigenvalues taking values in certain K_0;

(B) $Y_{\mathcal{G}}(K) = \underline{\mathrm{Hom}}(G_{F,S}, \mathcal{G}(K))$;

(C) Motives over F with coefficients in K_0 and good reduction outside of S.

$$\begin{tikzcd}
\text{(A) arithmetic automorphic forms} \arrow[rr, dotted, "?"] \arrow[dr, "L_p"'] & & \text{(C) motives} \arrow[dl, "M_p"] \\
& \text{(B) } Y_{\mathcal{G}}(K) = \underline{\mathrm{Hom}}(G_{F,S}, \mathcal{G}(K)) &
\end{tikzcd}$$

From **(A)** to **(B)** we have global p-adic Langlands correspondence L_p, from **(C)** to **(B)** we have the p-adic realization M_p of motives. These two operations should be injective. Notice that the sets **(A)** and **(C)** are just countable sets, but **(B)** carries a topology. It is hope that there is a map from **(A)** to **(C)** linking these two, hence the image from **(A)** is contained in the image from **(C)**.

For $\mathcal{G} = \mathbf{GL}_1(K)$, this is essentially equivalent to class field theory. For $\mathbf{GL}_2(\mathbb{Q})$, this program still remains unproved.

For our purposes in this master thesis, we will be mostly interested in p-adic representation $G \to \mathbf{GL}_n(K)$ where K is a finite extension of $\mathbb{Q}_p$, and in families of such representations.

§ 2.4. *The p-finiteness condition*

Let G be a profinite group. The *pro-p-completion* of the profinite group G is $G^{(p)} := \varprojlim_N G/N$ where N runs through all closed normal subgroups whose index is a power of p. The *p-Frattini quotient* of G is the maximal continuous abelian quotient of G which is of exponent p. We recall the pro-p version of the *Burnside Basis Theorem*: Let G be a pro-p-group, and let $\mathrm{Fr}(G)$ be its pro-p-Frattini quotient. Then any lifting to G of a basis of $\mathrm{Fr}(G)$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$ is a set of topological generators for G.

Definition 2.4.1. We say that the profinite group G satisfies the *p-finiteness condition* Φ_p if for all open subgroups $G_0 \subset G$ of finite index, there are only a finite number of continuous homomorphisms from G_0 to $\mathbb{Z}/p\mathbb{Z}$.

The following lemma gives several equivalent statements of the p-finiteness condition.

Lemma 2.4.2. *Let G be a profinite group. The following conditions are equivalent:*

(i) the pro-p-completion of G is topological finitely generated,

(ii) the abelianisation of the pro-p-completion of G is a $\mathbb{Z}_p$-module of finite rank,

(iii) the p-Frattini quotient of G is finite,

(iv) the set of continuous homomorphisms from G to $\mathbb{Z}/p\mathbb{Z}$ is finite.

Proof. Clearly, a set of topological generators of the pro-p-completion becomes a set of generators over $\mathbb{Z}_p$ in the abelianisation, and becomes a basis of the p-Frattini quotient as a vector space over $\mathbb{Z}/p\mathbb{Z}$. Hence, it is clear that *(i)* implies *(ii)* and *(ii)* implies *(iii)*. Since any homomorphism $G \to \mathbb{Z}/p\mathbb{Z}$ must factor through the p-Frattini quotient, *(iii)* and *(iv)* are equivalent. The pro-p version of the *Burnside Basis Theorem* says that if the image in the p-Frattini quotient of a set $\{g_1, \ldots, g_r\}$ of elements of the pro-p-group $G^{(p)}$ is a basis for the quotient as a vector space over $\mathbb{Z}/p\mathbb{Z}$, then $g_1, \ldots, g_r$ topologically generate $G^{(p)}$. This shows that *(iii)* implies *(i)*. ■

Example 2.4.3. For K any number field, let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group. The structure of the Galois group G_K is not so well known. The *Kronecker-Weber theorem* asserts that the natural surjection $G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{cycl}}/\mathbb{Q}) = \widehat{\mathbb{Z}}^{\times}$ induces an isomorphism $G_{\mathbb{Q}}^{\mathrm{ab}} \simeq \widehat{\mathbb{Z}}^{\times}$. Let $\mathbb{Q}_S$ denote as the maximal extension of $\mathbb{Q}$ unramified outside a finite set S of primes and let $G_{\mathbb{Q},S}$ be the Galois group of $\mathbb{Q}_S/\mathbb{Q}$. Here are two famous open problems:

Conjecture (Shafarevic).

(i) The absolute Galois group $G_{\mathbb{Q}^{\mathrm{ab}}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}})$ of $\mathbb{Q}^{\mathrm{ab}}$ is a free profinite group of countable rank, where $\mathbb{Q}^{\mathrm{ab}}$ is the maximal abelian extension of $\mathbb{Q}$.

(ii) Is $G_{\mathbb{Q},S}$ topologically finitely generated?

Let us recall the theorem of Hermite and Minkowski, which is the first important fact about $G_{K,S}$.

Theorem 2.4.4 (Hermite-Minkowski). *Let K be a finite extension of $\mathbb{Q}$ and let S be a finite set of primes. If d is a positive integer, then there are only finitely many extensions L/K of degree d which are unramified outside S.*

An important consequence of the theorem of Hermite and Minkowski is that the set $\underline{\mathrm{Hom}}(G_{\mathbb{Q},S}, \mathbb{Z}/p\mathbb{Z})$ is finite, since each nontrivial homomorphism corresponds to an extension of degree p unramified outside S. Thus, if $G_0 \subset G_{\mathbb{Q},S}$ is an open subgroup then there exist only finite number of continuous homomorphisms from G_0 to $\mathbb{Z}/p\mathbb{Z}$. Hence, any finitely ramified Galois groups satisfy the p-finiteness condition Φ_p. This is an important example in the deformation theory.

Chapter 3

Deformation Theory

In these days the angel of topology and the devil of abstract algebra are fighting for every mathematical domain.

Hermann Weyl

The basic situation we want to study is as follows. We are given a profinite group G and a representation of G into matrices over a finite field k of characteristic $p > 0$. We try to understand all possible lifts of this representation to $\mathbf{GL}_n(A)$, where A is a complete noetherian local ring with residue k. It is not so clear what "understand all possible lifts" means, and so the main goal of this chapter is to make our question more precise. We begin by recalling some facts of the ring of Witt vectors, then we develop the correct problem of deformation we want to study.

§ 3.1. The ring of Witt vectors

The materials and the results in this section can be found in the Chapter 2 of Serre's book [25].

Let K be a field which is complete under a discrete valuation v with residue field k of characteristic $p > 0$. Let $\mathcal{O}$ denote the ring of integers of K and denote the uniformiser of $\mathcal{O}$ by ϖ. Then the projection $\mathcal{O} \to k$ has a unique multiplicative section which associates each $\lambda \in k$ to an element $[\lambda] \in \mathcal{O}$ called its *Teichmüller representative*. In fact, the construction of this section is:

$$[\lambda] = \lim_{n\to\infty} \left(\widehat{\lambda^{p^{-n}}}\right)^{p^n}$$

where $\lambda^{p^{-n}}$ denotes the unique element $x \in k$ such that $x^{p^n} = \lambda$ and $\widehat{x}$ denotes an lifting of x in $\mathcal{O}$. The limit is independent to the choice of the liftings of x and is a well-defined multiplicative section. Denote the set of such multiplicative representatives in $\mathcal{O}$ by $\mathcal{R}$.

Theorem 3.1.1. *With previous notations, every element $a \in \mathcal{O}$ can be written uniquely as a convergent series*

$$a = \sum_{n=0}^{\infty} [a_n] \varpi^n$$

with $[a_n] \in \mathcal{R}$. Moreover, there exists polynomials $S_0, S_1, \ldots, S_n, \ldots$ and $P_0, P_1, \ldots, P_n, \ldots$ such that if

$$a = \sum_{n=0}^{\infty} [a_n] \varpi^n \quad \text{and} \quad b = \sum_{n=0}^{\infty} [b_n] \varpi^n,$$

then we have

$$a + b = \sum_{n=0}^{\infty} \left[S_n(a_0^{p^{-n}}, \ldots, a_n, b_0^{p^{-n}}, \ldots, b_n) \right] \varpi^n$$

and

$$ab = \sum_{n=0}^{\infty} \left[P_n(a_0^{p^{-n}}, \ldots, a_n, b_0^{p^{-n}}, \ldots, b_n) \right] \varpi^n.$$

The last theorem gives more naturally the definition of the *Witt vectors* which follows: if A is an arbitrary commutative ring with identity, and if $\mathfrak{a} = (a_0, \ldots, a_n, \ldots)$, $\mathfrak{b} = (b_0, \ldots, b_n, \ldots)$ are elements of $A^{\mathbb{N}}$, we denote $W(A)$ as the set of such sequences with coefficients in A and equip $W(A)$ with the laws of composition defined below:

$$\begin{aligned} \mathfrak{a} + \mathfrak{b} &= (S_0(a_0, b_0), \ldots, S_n(a_0, \ldots, a_n, b_0, \ldots, b_n), \ldots) \\ \mathfrak{a} \cdot \mathfrak{b} &= (P_0(a_0, b_0), \ldots, P_n(a_0, \ldots, a_n, b_0, \ldots, b_n), \ldots) \end{aligned}$$

These make $W(A)$ into a commutative ring with identity, called the *ring of Witt vectors*.

***Remark* 3.1.2.** For $n \geq 1$, let $W_n(A) = A^n$ as a set. If p is invertible in A, we can equip $W_n(A)$ with a structure of a commutative ring which is isomorphic to A^n. For the sequence of rings $W_n(A)$, consider the maps

$$\begin{aligned} W_{n+1}(A) &\to W_n(A) \\ (a_0, a_1, \ldots, a_n) &\mapsto (a_0, a_1, \ldots, a_{n-1}). \end{aligned}$$

This is a surjective homomorphism of rings for each n. Then

$$W(A) \simeq \varprojlim_{n} W_n(A);$$

thus $W(A)$ can be viewed as a topological ring.

Example 3.1.3. The ring of Witt vectors of the finite field of order p is nothing but the ring of p-adic integers, that is, $W(\mathbb{F}_p) = \mathbb{Z}_p$.

***Remark* 3.1.4.** We have a canonical homomorphism

$$\begin{array}{rcl} W(k) & \to & \mathcal{O} \\ \mathfrak{a} = (a_0, \ldots, a_n, \ldots) & \mapsto & \sum_{n=0}^{\infty} \left[a_n^{p^{-n}} \right] \varpi^n \end{array}$$

This map is always injective and makes $\mathcal{O}$ as a $W(k)$-module of rank e, absolute ramification index. In particular, this map is a bijection if and only if $\mathcal{O}$ is unramified.

§ 3.2. *The deformation functor*

The strong motivation to study deformations of representations of profinite groups satisfying the p-finiteness condition Φ_p is that they play a crucial role in the proof of the modularity conjecture for elliptic curves over $\mathbb{Q}$ (work of Wiles, Taylor, Diamond, Breuil, and Conrad [31, 29, 2]).

In maximal generality, we begin with a profinite group G and a representation of G into certain matrices over a finite field. The basic question is: can we describe all lifts of this representation to appropriate p-adically complete rings? In order for the theory to work, we need to know that G satisfies the concerned finiteness condition.

Let K be a finite extension of $\mathbb{Q}_p$ with the valuation ring $\mathcal{O}$, the maximal ideal $\mathfrak{m}$, and the residue field k of characteristic p. Denote W to be the ring of Witt vectors with coefficients in k. We let $\mathcal{G}$ be the algebraic groups $\mathbf{GL}_1$ or $\mathbf{GL}_2$.

Consider the following topological spaces

$$\begin{array}{ll} Y = Y_{\mathcal{G}} := \underline{\mathrm{Hom}}(G, \mathcal{G}(\mathcal{O})) & \overline{Y} := \underline{\mathrm{Hom}}(G, \mathcal{G}(k)) \\ X = X_{\mathcal{G}} := Y/\mathcal{G}(\mathcal{O}) & \overline{X} := \overline{Y}/\mathcal{G}(k) \end{array}$$

where $\mathcal{G}(\mathcal{O})$ and $\mathcal{G}(k)$ act on Y and $\overline{Y}$ via conjugation respectively. The reduction homomorphism $\varphi : \mathcal{O} \to k$ induces serval homomorphisms: $\varphi : \mathcal{G}(\mathcal{O}) \to \mathcal{G}(k)$, resp. $\varphi_Y : Y \to \overline{Y}$, resp. $\varphi_X : X \to \overline{X}$. We have the following commutative diagram:

$$\begin{tikzcd} Y \arrow[r, "\varphi_Y"] \arrow[d, "\pi"'] & \overline{Y} \arrow[d, "\overline{\pi}"] \\ X \arrow[r, "\varphi_X"'] & \overline{X} \end{tikzcd}$$

If $\rho \in Y$, then the commutativity of the diagram reads as $\overline{\pi(\rho)} = \overline{\pi}(\overline{\rho})$. Fix $\pi(\rho) \in X$. If $\pi(\rho)'$ is close to $\pi(\rho)$, there exists $\rho' \in Y$ close to ρ such that $\overline{\rho'} = \overline{\rho}$. In other words, the neighborhood $U = \varphi_X^{-1}(\overline{\pi}(\overline{\rho}))$ of $\pi(\rho)$ in X is isomorphic to the quotient of $V = \varphi_Y^{-1}(\overline{\rho})$ by its stabilizer $\mathrm{Stab}(V)$ in $\mathcal{G}(\mathcal{O})$; $\mathrm{Stab}(V)$ is the inverse image by φ of the centralizer of $\overline{\rho}$:

$$\begin{aligned} \mathrm{Stab}(V) &= \{g \in \mathcal{G}(\mathcal{O}) \mid g\rho' g^{-1} \in V \text{ for all } \rho' \in V\} \\ &= \{g \in \mathcal{G}(\mathcal{O}) \mid \bar{g}\bar{\rho}\bar{g}^{-1} = \overline{\rho}\} \\ &= \varphi^{-1}(Z_{\overline{\rho}}) \subset \mathcal{G}(\mathcal{O}). \end{aligned}$$

So $U = V/\varphi^{-1}(Z_{\overline{\rho}}) = \{\rho' : G \to \mathcal{G}(\mathcal{O})\}/\varphi^{-1}(Z_{\overline{\rho}})$. Note that $\varphi^{-1}(Z_{\overline{\rho}})$ contains the group $Z_G(\mathcal{O})$ of $\mathcal{O}$-points of the center of $\mathcal{G}$.

Let $\underline{\mathbf{CNL}}_W$ be the category of the complete noetherian local W-algebras A with a surjective local homomorphism $\varphi : A \to k$; the morphisms of $\underline{\mathbf{CNL}}_W$ are the local W-algebra homomorphisms commute with the φ's. We will also denote by φ the corresponding group homomorphism $\mathcal{G}(A) \to \mathcal{G}(k)$.

Definition 3.2.1. Fix a representation $\overline{\rho} : G \to \mathcal{G}(k)$. For each object (A, φ) in $\underline{\mathbf{CNL}}_W$, we take $H_A = \varphi^{-1}(Z_{\overline{\rho}})$. Consider the covariant functor $\mathscr{D} = \mathscr{D}_{\overline{\rho}}$, called the *problem of deformation* *of* $\overline{\rho}$:

$$\begin{array}{rcl} \mathscr{D}: \underline{\mathbf{CNL}}_W & \to & \underline{\mathbf{Sets}} \\ (A,\varphi) & \mapsto & U_A = V_A/H_A = V_A/\varphi^{-1}(Z_{\overline{\rho}}). \end{array}$$

We call the element in $\mathscr{D}(A)$ a *deformation* of $\overline{\rho}$ to A.

***Remark* 3.2.2.** For any subgroup $H \subseteq \mathcal{G}(A)$, we say that two representations $\rho_i : G \to \mathcal{G}(A)$ for $i = 1, 2$ are *strictly equivalent* with respect to H, written as $\rho_1 \overset{H}{\sim} \rho_2$, if $\rho_2 = h\rho_1 h^{-1}$ for some $h \in H$. Thus, a deformation of $\overline{\rho}$ to A is in fact a strictly equivalence class of $\overline{\rho}$.

If $(A, \mathfrak{m})$ is a complete noetherian local ring with residue field k, then we have $A = \varprojlim_n A/\mathfrak{m}^n$.

Definition 3.2.3. We say that a functor $\mathscr{F}$ on $\underline{\mathbf{CNL}}_W$ is *continuous* if the canonical morphism $\mathscr{F}(A) \to \varprojlim_n \mathscr{F}(A/\mathfrak{m}^n)$ is an isomorphism.

Lemma 3.2.4. *The deformation functor* $\mathscr{D}$ *is continuous.*

Proof. We have to check this map $\mathscr{D}(A) \to \varprojlim_n \mathscr{D}(A/\mathfrak{m}^n)$ is bijective. Note that for each n the map $\mathcal{G}(A/\mathfrak{m}^{n+1}) \to \mathcal{G}(A/\mathfrak{m}^n)$ induced by $A/\mathfrak{m}^{n+1} \to A/\mathfrak{m}^n$ is surjective.

For the injectivity, let ρ and ρ' be two representations from G to $\mathcal{G}(A)$ such that for each $n \geq 1$ there exists an element g_n of $\mathcal{G}(A/\mathfrak{m}^n)$ such that for $\rho_n := \rho \pmod{\mathfrak{m}^n}$ and $\rho'_n := \rho' \pmod{\mathfrak{m}^n}$, we have $g_n\rho_n g_n^{-1} = \rho'_n$. For each n the set $X_n := \{g_n \in \mathcal{G}(A/\mathfrak{m}^n) |\, g_n\rho_n g_n^{-1} = \rho'_n\} \neq \emptyset$, and the transition maps induced by $A/\mathfrak{m}^{n+1} \to A/\mathfrak{m}^n$ define a projective system of nonempty finite sets $X_{n+1} \to X_n$. The projective limit $X := \varprojlim_n X_n$ is therefore nonempty and any element $g \in X$ satisfies $g\rho g^{-1} = \rho'$.

For the surjectivity, let $\{\rho_n\}$ be a system of representations from G to $\mathcal{G}(A/\mathfrak{m}^n)$ such that for each $m \geq n \geq 1$ there exists $g_n \in \mathcal{G}(A/\mathfrak{m}^n)$ such that $\rho_m \pmod{\mathfrak{m}^n} = g_n\rho_n g_n^{-1}$. Starting from $\rho'_1 = \rho_1$, one can construct representations ρ'_n conjugate to ρ_n such that $\rho'_{n+1} \pmod{\mathfrak{m}^n} = \rho'_n$ by induction. The system $\{\rho'_n : G \to \mathcal{G}(A/\mathfrak{m}^n)\}_n$ defines a representation ρ' with values in $\mathcal{G}(A)$ whose class in $\mathscr{D}(A)$ maps to the projective system $\{\pi(\rho_n)\}$ as desired. ■

***Remark* 3.2.5.** Let $\underline{\mathbf{CNL}}_W^0$ be the full subcategory of $\underline{\mathbf{CNL}}_W$ whose objects are artinian local rings with residue field k. Notice that the maximal ideal of an artinian local ring is always nilpotent and hence such rings are complete and noetherian. Note also that the objects of $\underline{\mathbf{CNL}}_W$ are pro-objects of $\underline{\mathbf{CNL}}_W^0$, that is, that any object of $\underline{\mathbf{CNL}}_W$ is a projective limit of objects of $\underline{\mathbf{CNL}}_W^0$. The continuity of deformation functor $\mathscr{D}$ shows that $\mathscr{D}$ is completely determined by its values on the full subcategory $\underline{\mathbf{CNL}}_W^0$. We will use this in a crucial way later, when we use the criteria of Schlessinger for representability, which apply to functors on artinian ring.

§ 3.3. *Pro-representability*

The question we want to ask about our deformation functor is whether it is *representable*.

Definition 3.3.1. We say that $\mathscr{D}$ is *pro-representable* by an object R in $\underline{\mathbf{CNL}}_W$ if there exists $R \in \mathrm{Obj}(\underline{\mathbf{CNL}}_W)$ such that the covariant functor

$$\begin{aligned} \mathbf{h}_R : \underline{\mathbf{CNL}}_W^0 &\to \underline{\mathbf{Sets}} \\ A &\to \underline{\mathrm{Hom}}_{\mathrm{localg}}(R, A) \end{aligned}$$

is naturally isomorphic to $\mathscr{D}$:

(a) For any object $A \in \mathrm{Obj}(\underline{\mathbf{CNL}}_W^0)$, there exist a bijection ι_A such that

$$\underline{\mathrm{Hom}}_{\mathrm{localg}}(R, A) \overset{\iota_A}{\simeq} \mathscr{D}(A).$$

(b) For any map $\alpha : A \to A'$, there is a commutative diagram

$$\begin{tikzcd} \underline{\mathrm{Hom}}_{\mathrm{localg}}(R, A) \arrow[r, "\iota_A"] \arrow[d, "\alpha_*"'] & \mathscr{D}(A) \arrow[d, "\mathscr{D}(\alpha)"] \\ \underline{\mathrm{Hom}}_{\mathrm{localg}}(R, A') \arrow[r, "\iota_{A'}"'] & \mathscr{D}(A') \end{tikzcd}$$

***Remark* 3.3.2.** Since the deformation functor $\mathscr{D}$ is continuous, then it is pro-representable as a functor on $\underline{\mathbf{CNL}}_W^0$ if and only if it is representable as a functor on $\underline{\mathbf{CNL}}_W$.

Lemma 3.3.3. *The following two statements are equivalent:*

(i) $\mathscr{D}$ *is representable by* R*;*

(ii) *there exists* $\xi \in \mathscr{D}(R)$ *such that for all* $\eta \in \mathscr{D}(A)$ *there is a unique morphism* $\alpha : R \to A$ *in* $\underline{\mathbf{CNL}}_W$ *such that* $\mathscr{D}(\alpha)(\xi) = \eta$.

Proof. Suppose that *(i)* holds. Consider

$$\iota_R : \underline{\mathrm{Hom}}_{\mathrm{localg}}(R, R) \simeq \mathscr{D}(R) \text{ and } \iota_R(\mathrm{id}) = \xi.$$

Since R represents $\mathscr{D}$, for all $\eta \in \mathscr{D}(A)$ there exists a morphism $\alpha : R \to A$ in $\underline{\mathbf{CNL}}_W$ such that $\iota_A(\alpha) = \eta$ and such that the following diagram commutes:

$$\begin{tikzcd} \underline{\mathrm{Hom}}_{\mathrm{localg}}(R,R) \arrow[r, "\iota_R"] \arrow[d, "\alpha_*"'] & \mathscr{D}(R) \arrow[d, "\mathscr{D}(\alpha)"] \\ \underline{\mathrm{Hom}}_{\mathrm{localg}}(R,A) \arrow[r, "\iota_A"'] & \mathscr{D}(A) \end{tikzcd}$$

So $\eta = \iota_A(\alpha) = \iota_A(\alpha \circ \mathrm{id}) = (\iota_A \circ \alpha_*)(\mathrm{id}) = \mathscr{D}(\alpha)(\iota_R(\mathrm{id})) = \mathscr{D}(\alpha)(\xi)$. This proves *(ii)*.

Conversely, suppose *(ii)* holds. Given (R, ξ), we define ι_A for each object A of $\underline{\mathbf{CNL}}_W$ by:

$$\begin{aligned} \iota_A : \underline{\mathrm{Hom}}_{\mathrm{localg}}(R, A) &\to \mathscr{D}(A) \\ \alpha &\mapsto \mathscr{D}(\alpha)(\xi) \end{aligned}$$

It is a bijection by assumption. Moreover, if $A \to A'$, we have a commutative diagram:

$$\begin{tikzcd} \underline{\mathrm{Hom}}_{\mathrm{localg}}(R,A) \arrow[r, "\iota_A"] \arrow[d, "\alpha_*"'] & \mathscr{D}(A) \arrow[d, "\mathscr{D}(\alpha)"] \\ \underline{\mathrm{Hom}}_{\mathrm{localg}}(R,A') \arrow[r, "\iota_{A'}"'] & \mathscr{D}(A') \end{tikzcd}$$

because

$$\begin{aligned}\mathscr{D}(\alpha)\circ\iota_A(\beta) &= \mathscr{D}(\alpha)\mathscr{D}(\beta)(\xi) = \mathscr{D}(\alpha\circ\beta)(\xi)\\ &= \mathscr{D}(\alpha_*(\beta))(\xi) = \iota_{A'}(\alpha_*(\beta)) = \iota_{A'}\circ\alpha_*(\beta).\end{aligned}$$

This proves *(i)*. ■

Proposition 3.3.4. *If (R,ξ) exists, it is unique up to a canonical isomorphism.*

Proof. Let (R,ξ) and (R',ξ') be two pairs, then for any A we have a bijection:

$$\begin{aligned}\iota_A : \underline{\mathrm{Hom}}_{\mathrm{localg}}(R,A) &\to \mathscr{D}(A)\\ \alpha &\mapsto \mathscr{D}(\alpha)(\xi)\\ \iota'_A : \underline{\mathrm{Hom}}_{\mathrm{localg}}(R',A) &\to \mathscr{D}(A)\\ \alpha &\mapsto \mathscr{D}(\alpha)(\xi')\end{aligned}$$

Taking $A = R'$ (resp. $A = R$), we obtain morphisms $\phi \in \underline{\mathrm{Hom}}_{\mathrm{localg}}(R,R')$ (resp. $\psi \in \underline{\mathrm{Hom}}_{\mathrm{localg}}(R',R)$) such that $\iota_{R'}(\phi) = \xi'$ (resp. $\iota'_R(\psi) = \xi$). We now have to show that

$$\begin{cases}\phi\circ\psi = \mathrm{id}_{R'}\\ \psi\circ\phi = \mathrm{id}_R\,.\end{cases}$$

To check second relation, for instance, it suffices to show that

$$\iota_R(\psi\circ\phi) = \xi.$$

This follows from the calculation

$$\begin{aligned}\iota_R(\psi\circ\phi) &= \mathscr{D}(\psi\circ\phi)(\xi) = \mathscr{D}(\psi)\circ\mathscr{D}(\phi)(\xi)\\ &= \mathscr{D}(\psi)(\iota_{R'}(\phi)) = \mathscr{D}(\psi)(\xi') = \iota'_R(\psi) = \xi.\end{aligned}$$

Similar calculation shows that $\iota'_{R'}(\phi\circ\psi) = \xi'$. ■

Definition 3.3.5. The pair (R, ξ) is called the *universal pair*.

For any object (A, φ) in $\underline{\mathbf{CNL}}_W$, we set $H_A = \varphi^{-1}(Z_{\overline{\rho}})$. For any morphism $\alpha : A \to A'$ in $\underline{\mathbf{CNL}}_W$, we define a map, still denoted by α, from $U_A = \underline{\mathrm{Hom}}(G, \mathcal{G}(A))/H_A$ to $U_{A'} = \underline{\mathrm{Hom}}(G, \mathcal{G}(A'))/H_{A'}$ given by $\pi(\rho) \mapsto \pi(\alpha \circ \rho)$.

Corollary 3.3.6. *$\mathscr{D}$ is representable by R if and only if there exists a continuous homomorphism $\rho^{\mathrm{u}} : G \to \mathcal{G}(R)$ such that for any object (A, φ) in $\underline{\mathbf{CNL}}_W$ and for any continuous homomorphism $\rho : G \to \mathcal{G}(A)$ with $\varphi(\rho) = \overline{\rho}$ there exists a unique local ring homomorphism $\alpha : R \to A$ such that the map $\alpha : U_R \to U_A$ sends $\pi(\rho^{\mathrm{u}})$ to $\pi(\rho)$.*

Definition 3.3.7. If $\mathscr{D}$ is representable by R, the ring R is called the *universal deformation ring of $\overline{\rho}$*, and the associated representation $\rho^{\mathrm{u}} : G \to \mathcal{G}(R)$ is called the *universal deformation of $\overline{\rho}$*.

§ 3.4. *Schlessinger's criteria*

In this section, we first recall a result of Grothendieck for a covariant functor $\mathscr{F} : \underline{\mathbf{CNL}}_W^0 \to \underline{\mathbf{Sets}}$ such that $\mathscr{F}(k) = \overline{\xi}$ to be pro-representable and then give useful criteria due to Schlessinger for the pro-representability.

Notice that the two categories $\underline{\mathbf{CNL}}_W^0$ and $\underline{\mathbf{Sets}}$ admit *fiber products*: Given any two morphisms $\alpha_i : A_i \to A_0$ in $\underline{\mathbf{CNL}}_W^0$, we define their *fiber product* $A_3 = A_1 \times_{A_0} A_2$ as

$$\begin{aligned} A_3 &:= \{(a_1, a_2) \in A_1 \times A_2 |\, \alpha_1(a_1) = \alpha_2(a_2)\} \\ \mathfrak{m}_3 &:= A_3 \cap (\mathfrak{m}_1 \times \mathfrak{m}_2). \end{aligned}$$

We see that $(A_3, \mathfrak{m}_3)$ is an object in $\underline{\mathbf{CNL}}_W^0$ and the projections $\beta_i : A_3 \to A_i$ are morphisms in $\underline{\mathbf{CNL}}_W^0$. We put $\beta_0 = \alpha_1 \circ \beta_1 = \alpha_2 \circ \beta_2$.

***Remark* 3.4.1.** The fiber product of noetherian rings does not need to be noetherian. Indeed, let $A = k[\![X, Y]\!]$, $B = k$ and $C = k[\![X]\!]$. Let $\alpha : A \to C$ be the map that sends Y to 0 and let $\beta : B \to C$ be the inclusion. The fiber product $A \times_C B$ is given by the subring $k \oplus Y \cdot k[\![X, Y]\!]$ in $k[\![X, Y]\!]$. The maximal ideal of $A \times_C B$ is $Y \cdot k[\![X, Y]\!]$, and the Zariski tangent space of $A \times_C B$ may be identified with the k-vector space $k[\![X]\!]$, which is infinite dimensional; that is, $A \times_C B$ is not noetherian. This is the reason why we consider the smaller category $\underline{\mathbf{CNL}}_W^0$.

Given two morphisms $\alpha_i : A_i \to A_0$ in $\underline{\mathbf{CNL}}_W^0$, by the universal property of fiber products we can get a natural map

$$\mathscr{F}(A_1 \times_{A_0} A_2) \xrightarrow{\mathscr{F}(\beta_1)\times_{\mathscr{F}(\beta_0)}\mathscr{F}(\beta_2)} \mathscr{F}(A_1) \times_{\mathscr{F}(A_0)} \mathscr{F}(A_2). \tag{3.1}$$

The result of Grothendieck for a pro-representable covariant functor $\mathscr{F}$ is characterized as follows:

Theorem 3.4.2 (Grothendieck [9]). *The covariant functor $\mathscr{F}$ is pro-representable if and only if*

(i) The map (3.1) *is bijective.*

(ii) $\mathscr{F}(k[\varepsilon])$ is a finite set.

As Mazur says in [20], the result of Grothendieck is difficult to use because its hypothesis is hard to check for all diagrams

$$\begin{tikzcd} A_1 \arrow[dr, "\alpha_1"'] & & A_2 \arrow[dl, "\alpha_2"] \\ & A_0 & \end{tikzcd}$$

The following criteria of Schlesinger could be viewed as basically a simplification of this result.

Theorem 3.4.3 (Schlessinger [24]). *Suppose the following four assumptions hold:*

(H1) *If α_1 is* small *(i.e., α_1 is surjective and $\ker(\alpha_1)$ is principal and is annihilated by $\mathfrak{m}_{A_1}$), then the map* (3.1) *is surjective.*

(H2) *If $\alpha_1 : A_1 \to A_0$ is the quotient map $k[\varepsilon] := k[t]/(t^2) \to k$, then the map* (3.1) *is bijective.*

(H3) *The tangent space $t_{\mathscr{F}} := \mathscr{F}(k[\varepsilon])$ of $\mathscr{F}$ is a finite dimensional k-vector space.*

(H4) *If $A_1 = A_2$, the maps $\alpha_i : A_i \to A_0$ are the same, and α_i is small, then the map* (3.1) *is bijective.*

Then $\mathscr{F}$ is pro-representable. In particular, there exists an object R in $\underline{\mathbf{CNL}}_W$ such that

$$\mathscr{F}(A) = \underline{\mathrm{Hom}}_{\mathrm{localg}}(R, A)$$

for every object A in $\underline{\mathbf{CNL}}_W^0$.

***Remark* 3.4.4.** The finiteness or finite-dimensionality condition is there to guarantee that the representing object is noetherian. (Cf. **Corollary 3.5.4**.)

In the next chapter, we will apply the criteria of Schlessinger to the deformation functor

$$\mathscr{D} = \mathscr{D}_{\overline{\rho}} : \underline{\mathbf{CNL}}_W \to \underline{\mathbf{Sets}}$$

given by

$$\mathscr{D}(A) = \{\text{deformations of } \overline{\rho} \text{ to } A\}.$$

§ 3.5. The Zariski tangent space and its cohomological interpretation

We have shown that the deformation functor is continuous (cf. **Lemma 3.2.4**). Suppose that the condition ***(H2)*** holds. We can endow the tangent space $t_{\mathscr{D}}$ of $\mathscr{D}$, defined by $\mathscr{D}(k[\varepsilon])$, with the structure of a k-vector space as follows: Consider the local ring homomorphism which we will simply label "$+$":

$$\begin{array}{ccc} k[\varepsilon] \times_k k[\varepsilon] & \xrightarrow{+} & k[\varepsilon] \\ (a + b\varepsilon, a + b'\varepsilon) & \mapsto & a + (b + b')\varepsilon. \end{array}$$

Let us apply $\mathscr{D}$ to it and use the condition ***(H2)***. We then obtain a map

$$+ : t_{\mathscr{D}} \times t_{\mathscr{D}} \to t_{\mathscr{D}}$$

called the *addition*. It is easy to see that this is a law of an abelian group with zero element given by $\overline{\rho}$. Similarly, for $\lambda \in k$, we see the local ring homomorphism

$$\begin{array}{ccc} k[\varepsilon] & \to & k[\varepsilon] \\ a + b\varepsilon & \mapsto & a + b\lambda\varepsilon. \end{array}$$

Applying $\mathscr{D}$, we then get a map called *multiplication by* λ. These laws turn $t_{\mathscr{D}}$ into a k-vector space.

Suppose that A is a complete local W-algebra with residue field k which is given as a projective limit $\varprojlim_{i\in I} A_i$ of a collection of discrete artinian quotients, where i runs through some directed index set I. We let $\mathfrak{m}$ and $\mathfrak{m}_i$ be the maximal ideals of A and A_i respectively.

Proposition 3.5.1. *The following two statements are equivalent:*

(i) A *is noetherian;*

(ii) $\dim_k(\mathfrak{m}_i/\mathfrak{m}_i^2)$ *is a bounded function of* i.

Proof. Suppose that A is noetherian. Then $\mathfrak{m}$ is generated, as an A-ideal, by a finite number d of elements of $\mathfrak{m}$. Since $\mathfrak{m}$ surjects to $\mathfrak{m}_i$, we have $\dim_k(\mathfrak{m}_i/\mathfrak{m}_i^2) \leq d$ for each i, so *(i)* implies *(ii)*.

Now assume that *(ii)* holds. We first claim that $\mathfrak{m}^a = \varprojlim_{i\in I} \mathfrak{m}_i^a$ for all $a \geq 0$. The assertion is trivial for $a = 0$, and we will proceed by induction on a. Assume the statement holds for a and consider the sequence of projective systems

$$0 \to \mathfrak{m}_i^{a+1} \to \mathfrak{m}_i^a \to \mathfrak{m}_i^a/\mathfrak{m}_i^{a+1} \to 0.$$

Assumption *(ii)* implies that $\mathfrak{m}_i^a/\mathfrak{m}_i^{a+1}$ also has bounded dimension, so the system on the right stabilizes. This implies that its limit is a finite dimensional k-vector space N. By the induction hypothesis we have a short exact sequence

$$0 \to \varprojlim_i \mathfrak{m}_i^{a+1} \to \mathfrak{m}^a \to N \to 0. \qquad (\heartsuit)$$

Choose elements $b_1, \ldots, b_l$ of $\mathfrak{m}^a$ whose images in N form a k-basis of N. For each i we have a surjection $A_i^l \to \mathfrak{m}_i^a$, sending $(x_1, \ldots, x_l)$ to $x_1b_1 + \cdots + x_lb_l$. Taking limits we deduce from the induction hypothesis that $\mathfrak{m}^a$ is generated by $b_1, \ldots, b_l$ as an A-ideal. We now have $l \geq \dim_k(\mathfrak{m}^a/\mathfrak{m}^{a+1}) \geq \dim_k(N) = l$, so $\mathfrak{m}^{a+1}$ is equal to the kernel of the map $\mathfrak{m}^a \to N$. By the sequence $(\heartsuit)$ above, this gives the induction step.

We now know that A is $\mathfrak{m}$-adically complete, and that $\mathfrak{m}$ is a finitely generated A-ideal. The graded ring $G(A) = \bigoplus_{a\geq 0} \mathfrak{m}^a/\mathfrak{m}^{a+1}$ is a finitely generated k-algebra, which is noetherian by

Hilbert's Basis Theorem. By [1], ***Corollary 10.25***, this implies that A is noetherian. This show *(i)*. ■

Definition 3.5.2. Let A be a complete noetherian local W-algebra, and let $\mathfrak{m}_A$ be its maximal ideal.

(1) The *Zariski cotangent space* of A is defined to be

$$t_A^* = \mathfrak{m}_A/(\mathfrak{m}_A^2, \mathfrak{m}_W),$$

where $(\mathfrak{m}_A^2, \mathfrak{m}_W) = \mathfrak{m}_A^2 + (\text{image of } \mathfrak{m}_W)A$. Note that t_A^* is a module over $W/\mathfrak{m}_W \simeq k$, that is, it is a k-vector space.

(2) The *Zariski tangent space* of A is the dual space of the cotangent space:

$$t_A = \operatorname{Hom}_k(t_A^*, k).$$

***Remark* 3.5.3.** Since A is noetherian, t_A^* is finite dimensional over k, so that there is no problem with the duality here.

Corollary 3.5.4. *If the deformation functor $\mathscr{D}$ is represented by a complete local W-algebra R, then the ring R is noetherian if and only if t_R^* is finite dimensional.*

Proof. Write R as a projective limit of its discrete artinian quotients R_i. Let $\mathfrak{m}_i$ be the maximal ideal of R_i. Recall that W is noetherian, so that the k-dimension d of $\mathfrak{m}_W/\mathfrak{m}_W^2$ is finite. It is clear that $\dim_k(\mathfrak{m}_i/(\mathfrak{m}_i^2 + \mathfrak{m}_W R_i))$ and $\dim_k(\mathfrak{m}_i/\mathfrak{m}_i^2)$ differ by at most d. Taking limit into account, t_R^* is finite dimensional over k if and only if the dimension of $\mathfrak{m}_i/\mathfrak{m}_i^2$ is bounded, which by **Proposition 3.5.1** is equivalent to R being noetherian. ■

The following lemma gives us a functorial interpretation of the Zariski tangent space:

Lemma 3.5.5. *If the deformation functor $\mathscr{D}$ is represented by an object R in $\underline{\mathbf{CNL}}_W$, then there is a canonical isomorphism of k-vector spaces*

$$t_R = \operatorname{Hom}_k(t_R^*, k) \simeq \underline{\operatorname{Hom}}_{\text{localg}}(R, k[\varepsilon]) = t_{\mathscr{D}}.$$

Proof. Let $A = k[\varepsilon]$ and let $\varphi : R \to A$. Write $\varphi(r) = \varphi_0(r) + \varphi_1(r)\varepsilon$. We have, from $\varphi(ab) = \varphi(a)\varphi(b)$, that $\varphi_0(ab) = \varphi_0(a)\varphi_0(b)$ and

$$\varphi_1(ab) = \varphi_0(a)\varphi_1(b) + \varphi_1(a)\varphi_0(b).$$

Thus, $\ker(\varphi_0) = \mathfrak{m}_A = k\varepsilon$. Since φ is W-linear, $\varphi_0(r) = \overline{r} = r \pmod{\mathfrak{m}_R}$, and thus φ kills $\mathfrak{m}_R^2$ and takes $\mathfrak{m}_R$ W-linearly into $k\varepsilon$. For $r \in W, \overline{r} = r\varphi(1) = \varphi(r) = \overline{r} + \varphi_1(r)\varepsilon$. Hence, φ_1 kills W. Note that any element of $a \in R$ can be written as $a = r + x$ with $r \in W$ and $x \in \mathfrak{m}_R$. Thus, φ is completely determined by the restriction of φ_1 to $\mathfrak{m}_R$, which factors through t_R^*. We can then write $\varphi : r + x \mapsto \overline{r} + \varphi_1(x)\varepsilon$ and regard φ_1 as a k-linear map from t_R^* into k. Thus $\varphi \mapsto \varphi_1$ induces a linear map $L : \underline{\mathrm{Hom}}_{\mathrm{localg}}(R, k[\varepsilon]) \to \mathrm{Hom}_k(t_R^*, k)$.

Note that $R/(\mathfrak{m}_R^2, \mathfrak{m}_W) = k \oplus t_R^*$. For any $\psi \in \mathrm{Hom}_k(t_R^*, k)$, we extend ψ to $R/\mathfrak{m}_R^2$ by declaring its value on k to be zero. Then we define $\varphi : R \to A$ by $\varphi(r) = \overline{r} + \psi(r)\varepsilon$. Since $\varepsilon^2 = 0$, φ is a W-algebra homomorphism. In particular, $L(\varphi) = \psi$; hence, L is surjective. Since any algebra homomorphism killing $(\mathfrak{m}_R^2, \mathfrak{m}_W)$ is determined by its values on t_R^*, L is injective. ■

Let $\overline{\rho} : G \to \mathbf{GL}_2(k)$ be a representation from G into $\mathbf{GL}_2(k)$ and let $\mathbf{M}_2(k)$ be the set of all 2×2-matrices with entries in k. We let G acts on $\mathbf{M}_2(k)$ by the composed map

$$G \xrightarrow{\overline{\rho}} \mathbf{GL}_2(k) \xrightarrow{\mathrm{Ad}} \mathbf{GL}(\mathbf{M}_2(k)).$$

The k-vector space $\mathbf{M}_2(k)$ with the action of G is usually called the *adjoint representation* of $\overline{\rho}$, and is denoted by $\mathrm{Ad}(\overline{\rho})$.

Proposition 3.5.6. *Suppose that the deformation functor $\mathscr{D} = \mathscr{D}_{\overline{\rho}}$ is represented by an object R in $\underline{\mathbf{CNL}}_W$. Then there is a canonical isomorphism of k-vector space*

$$t_{\mathscr{D}} \xrightarrow{\simeq} \mathrm{H}^1(G, \mathrm{Ad}(\overline{\rho})).$$

Proof. Let $\rho \in t_{\mathscr{D}} = \mathscr{D}(k[\varepsilon])$ be a deformation of $\overline{\rho}$ to $k[\varepsilon]$. Since the maximal ideal (ε) of $k[\varepsilon]$

is principal and of square 0, the map

$$\begin{array}{rcl} \mathbf{M}_2(k) & \xrightarrow{\simeq} & \ker(\mathbf{GL}_2(k[\varepsilon]) \to \mathbf{GL}_2(k)) \\ X & \mapsto & \mathbb{1} + X\varepsilon \end{array}$$

is an isomorphism of groups. Thus, we can lift $\overline{\rho}$ to $k[\varepsilon]$ and can compare ρ and $\overline{\rho}$. This define an element $X(\sigma) \in \mathbf{M}_2(k)$ by

$$\rho(\sigma) = \overline{\rho}(\sigma) + X(\sigma)\overline{\rho}(\sigma)\varepsilon.$$

Moreover, $\sigma \mapsto X(\sigma)$ is a 1-cocycle for the adjoint action:

$$\begin{array}{rcl} \rho(\sigma\tau) & = & \overline{\rho}(\sigma\tau) + X(\sigma\tau)\overline{\rho}(\sigma\tau)\varepsilon \\ \rho(\sigma) & = & \overline{\rho}(\sigma) + X(\sigma)\overline{\rho}(\sigma)\varepsilon \\ \rho(\tau) & = & \overline{\rho}(\tau) + X(\tau)\overline{\rho}(\tau)\varepsilon \\ \rho(\sigma)\rho(\tau) & = & [\overline{\rho}(\sigma) + X(\sigma)\overline{\rho}(\sigma)\varepsilon] \cdot [\overline{\rho}(\sigma)^{-1}\overline{\rho}(\sigma\tau) + X(\tau)\overline{\rho}(\sigma)^{-1}\overline{\rho}(\sigma\tau)\varepsilon] \\ & = & \overline{\rho}(\sigma\tau) + [X(\sigma) + \mathrm{Ad}\,\overline{\rho}(\sigma)X(\tau)]\overline{\rho}(\sigma\tau)\varepsilon. \end{array}$$

Conversely, given an 1-cocycle $X : G \to \mathbf{M}_2(k)$,

$$\rho(\sigma) = \overline{\rho}(\sigma) + X(\sigma)\overline{\rho}(\sigma)\varepsilon$$

defines a deformation of $\overline{\rho}$ over $k[\varepsilon]$, hence a class $\rho \in \mathscr{D}(k[\varepsilon])$.

Furthermore, if X is a coboundary, we have $X(\sigma) = (\mathrm{Ad}\,\overline{\rho}(\sigma) - \mathbb{1})Y$ for some $Y \in \mathbf{M}_2(k)$. We have the following computation

$$\begin{array}{rcl} \rho(\sigma) = \overline{\rho}(\sigma) + X(\sigma)\overline{\rho}(\sigma)\varepsilon & = & \overline{\rho}(\sigma) + (\mathrm{Ad}\,\overline{\rho}(\sigma)Y - Y)\overline{\rho}(\sigma)\varepsilon \\ & = & (\mathbb{1} - Y\varepsilon) \cdot [\overline{\rho}(\sigma) + \overline{\rho}(\sigma)(\mathrm{Ad}\,\overline{\rho}(\sigma)Y)\varepsilon] \\ & = & (\mathbb{1} - Y\varepsilon)\overline{\rho}(\sigma)(\mathbb{1} + Y\varepsilon). \end{array}$$

Hence, We conclude that X is a coboundary if and only if ρ is conjugate to $\overline{\rho}$ for some element in $\ker(\mathbf{GL}_2(k[\varepsilon]) \to \mathbf{GL}_2(k))$. To complete the proof, we note that the zero element of $t_{\mathscr{D}}$ is $\overline{\rho}$

and it is sent to 0 in $\mathrm{H}^1(G, \mathrm{Ad}(\overline{\rho}))$. ■

Corollary 3.5.7. *Suppose that G satisfies the p-finiteness condition Φ_p. If the deformation functor $\mathscr{D} = \mathscr{D}_{\overline{\rho}}$ is represented by an object R in $\underline{\mathbf{CNL}}_W$, then $t_{\mathscr{D}}$ is a finite dimensional k-vector space.*

Proof. Let $G_0 = \ker(\overline{\rho})$. This is an open subgroup of G and the action of G_0 on $\mathrm{Ad}(\overline{\rho})$ is trivial. Note that

$$\begin{aligned} \mathrm{H}^0(G/G_0, \mathrm{H}^1(G_0, \mathrm{Ad}(\overline{\rho}))) = \mathrm{Hom}(G_0, \mathbf{M}_2(k)) &= \mathrm{Hom}(G_0, k) \otimes_k \mathbf{M}_2(k) \\ &= \mathrm{Hom}(\mathrm{Fr}(G_0), k) \otimes_k \mathbf{M}_2(k) \end{aligned}$$

where $\mathrm{Fr}(G)$ is the pro-p-Frattini quotient of G_0. The inflation-restriction sequence yields the left exact sequence

$$0 \longrightarrow \mathrm{H}^1(G/G_0, \mathrm{H}^0(G_0, \mathrm{Ad}(\overline{\rho}))) \longrightarrow \mathrm{H}^1(G, \mathrm{Ad}(\overline{\rho})) \longrightarrow \mathrm{H}^0(G/G_0, \mathrm{H}^1(G_0, \mathrm{Ad}(\overline{\rho}))).$$

The term on the left is finite since G/G_0 and $\mathrm{H}^0(G_0, \mathrm{Ad}(\overline{\rho}))$ are finite. The term on the right is finite because of the p-finiteness condition Φ_p for G. Hence, this lemma is proved. ■

Chapter 4

The Existence of the Universal Deformation

Diese beklagen, daß man heute zu viel abstrakte Mathematik lernen muß, bevor man sinnvoll arbeiten kann. Diese Entwicklung ist zwar zu bedauern, doch darf man nicht übersehen, daßsie uns andererseits mächtige Hilfsmittel in die Hand gibt, und es erlaubt, komplizierte Sachverhalte einfach und klar darzustellen. Wer diese Methoden ablehnt, wird bei seinen Forschungen meist an der Oberfläche bleiben müssen.

Gred Faltings

Let $\mathcal{G}$ be $\mathbf{GL}_1$ or $\mathbf{GL}_2$. We will give rigidity conditions of the representation $\overline{\rho} : G \to \mathcal{G}(k)$ and verify those conditions of Schlessinger's criteria for our fixed deformation functor $\mathscr{D}$ of $\overline{\rho}$ in this chapter. In the process, we shall see where these assumptions are needed.

§ 4.1. Verification of condition (H1)

The verification of Schlessinger criteria ***(H1)*** will not require any assumption.

For any representation $\rho : G \to \mathcal{G}(A)$ and for any $g \in \mathcal{G}(A)$, we write ${}^{g}\rho$ for the representation given by $({}^{g}\rho)(\sigma) = g \cdot \rho(\sigma) \cdot g^{-1}$.

Consider the cartesian square

$$\begin{array}{ccc} A_3 & \xrightarrow{\beta_2} & A_2 \\ {\scriptstyle\beta_1}\downarrow & & \downarrow{\scriptstyle\alpha_2} \\ A_1 & \xrightarrow[\alpha_1]{} & A_0 \end{array}$$

and the corresponding map

$$\mathscr{D}(A_3) \to \mathscr{D}(A_1) \times_{\mathscr{D}(A_0)} \mathscr{D}(A_2). \tag{3.1}$$

Assume that α_1 is surjective. We must show that (3.1) is surjective. Let $(\pi(\rho_1), \pi(\rho_2)) \in \mathscr{D}(A_1) \times \mathscr{D}(A_2)$ such that $\mathscr{D}(\alpha_1)(\pi(\rho_1)) = \mathscr{D}(\alpha_2)(\pi(\rho_2))$, where the map π is defined as in **§3.2**. In other words, we are given two continuous representations

$$\rho_i : G \to \mathcal{G}(A_i) \quad i = 1, 2,$$

such that there exists $g_0 \in \varphi_{A_0}^{-1}(Z_{\overline{\rho}})$ such that for all $\sigma \in G$

$$\rho_{20}(\sigma) = {}^{g_0}\rho_{10}(\sigma)$$

where

$$\rho_{i0} = \alpha_i \circ \rho_i : G \to \mathcal{G}(A_0)$$

is the push-forward of ρ_i to A_0.

Recall that in algebraic geometry and in commutative algebra, a ring homomorphism $f : A \to B$ is said to be *formally smooth* if it satisfies the following *infinitesimal lifting property*: Suppose B is given the structure of an A-algebra via the map f. Given a commutative A-algebra C, and a nilpotent ideal J of C, any A-algebra homomorphism $B \to C/J$ may be lifted to an A-algebra homomorphism $B \to C$. That is to say, the canonical map

$$\mathrm{Hom}_A(B, C) \to \mathrm{Hom}_A(B, C/J)$$

is surjective. Formally smooth maps were introduced by Alexander Grothendieck in Éléments de Géométrie Algébrique [10], IV, *Définition* **(19.3.1)**. There are also several equivalent definitions of smoothness to be found in EGA IV. The fact that *f is smooth if and only if f is locally of finite type and formally smooth* is proved in EGA IV, *Corollaire* **(19.5.4)**.

Since $\mathcal{G}$ is smooth and α_1 is surjective, the map $\mathcal{G}(A_1) \to \mathcal{G}(A_0)$ is surjective by the formal smoothness of $\mathcal{G}$. Hence $g_0 = \alpha_1(g_1)$ for some $g_1 \in \mathcal{G}(A_1)$ and $g_1 \in \varphi_{A_1}^{-1}(Z_{\overline{\rho}})$, since $\varphi_{A_1} =$

$\varphi_{A_0} \circ \alpha_1$. Letting $\rho_1' = {}^{g_1}\rho_1$, then we have $\rho_{10}' = \rho_{20}$. Therefore, ρ_1' and ρ_2 have the same image in $\mathcal{G}(A_0)$, and $\rho_3 = (\rho_1', \rho_2)$ takes values in $\mathcal{G}(A_1) \times_{\mathcal{G}(A_0)} \mathcal{G}(A_2) = \mathcal{G}(A_3)$; moreover, $\pi(\rho_3) \in \mathscr{D}(A_3)$ and $\mathscr{D}(\beta_i)(\pi(\rho_3)) = \pi(\rho_i)$.

§ 4.2. *Verification of condition (H2)*

We will study the injectivity properties as stated in conditions ***(H2)*** and ***(H4)***.

If $\pi(\rho_3)$ and $\pi(\rho_3')$ have the same image, this means we are given two representations

$$\rho_3, \rho_3' : G \to \mathcal{G}(A_3)$$

such that $\rho_{3i} \overset{H_i}{\sim} \rho_{3i}'$ for $i = 1, 2$, with $H_i = \varphi_{A_i}^{-1}(Z_{\overline{\rho}})$. That is, there exist $g_i \in H_i$ for $i = 1, 2$, such that $\rho_{3i}' = {}^{g_i}\rho_{3i}$. Pushing these equalities to A_0, we obtain $\rho_{30}' = {}^{g_{10}}\rho_{30} = {}^{g_{20}}\rho_{30}$.

Consider the condition ***(H2)***, namely, if $A_1 \to A_0$ is the quotient map $k[\varepsilon] \to k$. In this case,

$$g_{10}^{-1} g_{20} \in Z_{\overline{\rho}}.$$

Note that the centralizer $Z_{\overline{\rho}}$ of $\overline{\rho}$ is contained in the center $Z_{\overline{\mathcal{G}}}$ of $\overline{\mathcal{G}}$, where $\overline{\mathcal{G}} = \mathcal{G}(k)$; note also that the center $Z_{\mathcal{G}}$ of $\mathcal{G}$ is $\mathbf{GL}_1$ which is formally smooth over W.

Since $\mathbf{GL}_1$ is smooth and $\alpha_1 : A_1 \to A_0$ is surjective, the map $\mathcal{G}(A_1) \to \mathcal{G}(A_0)$ is surjective by the formal smoothness of $\mathbf{GL}_1$. Therefore, we can lift $z_0 = g_{10}^{-1} g_{20}$ to $z_1 \in Z_{\mathcal{G}}(A_1)$ and $g_1' = g_1 z_1$ satisfies $g_{10}' = g_{20}$. Hence, we define $g_3 = (g_1', g_2) \in \mathcal{G}(A_1) \times_{\mathcal{G}(A_0)} \mathcal{G}(A_2) = \mathcal{G}(A_3)$. We thus have $g_3 \in \varphi_{A_3}^{-1}(Z_{\overline{\rho}})$ and $\rho_3' = {}^{g_3}\rho_3$ as desired, and this shows that ***(H2)*** is true.

§ 4.3. *Verification of condition (H3)*

Let $G_0 = \ker(\overline{\rho})$. We let $\widehat{\mathcal{G}}$ be the formal group of $\mathcal{G}$ defined by

$$\widehat{\mathcal{G}}(A) := \ker\left(\varphi : \mathcal{G}(A) \to \mathcal{G}(k)\right).$$

Suppose that ρ is a lift of $\overline{\rho}$ to $k[\varepsilon]$. If $x \in G_0$, we have $\overline{\rho}(x) = \mathbb{1}$, and hence $\rho(x) \in \widehat{\mathcal{G}}(k[\varepsilon])$.

Hence, ρ determines a map from G_0 to $\widehat{\mathcal{G}}(k[\varepsilon])$. Two lifts that determine the same map must be identical.

We see that the formal group

$$\widehat{\mathcal{G}}(k[\varepsilon]) = \{\mathbb{1} + X\varepsilon \mid X \in \mathbf{M}_2(k)\}$$

is a p-elementary abelian group and that G_0 is an open subgroup of G. By the p-finiteness condition Φ_p, there are only finitely many maps from G_0 into $\widehat{\mathcal{G}}(k[\varepsilon])$. Hence, $\mathscr{D}(k[\varepsilon])$ is a finite set. We also have shown that $\mathscr{D}(k[\varepsilon])$ itself is a k-vector space in **§3.5**, and therefore we are done!

***Remark* 4.3.1.** This proof relies on the facts that k is a finite field and that the profinite group G satisfies the p-finiteness condition Φ_p.

§ 4.4. *Verification of condition (H4)*

Let $\widehat{Z}_{\mathcal{G}}$ be the formal group of $Z_{\mathcal{G}}$, that is, $\widehat{Z}_{\mathcal{G}} = \ker(Z_{\mathcal{G}}(A) \to Z_{\mathcal{G}}(k))$.

Lemma 4.4.1. *If $Z_{\overline{\rho}} = k$, then for any object A in $\underline{\mathbf{CNL}}_W^0$ and $\pi(\rho) \in \mathscr{D}(A)$ we have $Z_\rho \cap \widehat{\mathcal{G}}(A) \subseteq \widehat{Z}_{\mathcal{G}}(A)$.*

Proof. We denote the deformation of $\overline{\rho}$ to C by ρ_C for any object C in $\underline{\mathbf{CNL}}_W^0$. We let

$$Z_{\rho_C}(C) = \{P \in \mathrm{Lie}(\mathcal{G})(C) \mid P\rho_C(\sigma)P^{-1} = \rho_C(\sigma) \text{ for all } \sigma \in G\},$$

where $\mathrm{Lie}(\mathcal{G})(C) = \mathbf{M}_1(C)$ or $\mathbf{M}_2(C)$ respectively.

Since the map $A \to k$ is surjective, it factors as a sequence of small extensions. Since $Z_{\overline{\rho}} = k$, this lemma will follow by induction from the following claim:

Claim: If $A \to B$ is small and if $Z_{\rho_B}(B) \cap \widehat{\mathcal{G}}(B) \subseteq \widehat{Z}_{\mathcal{G}}(B)$, then we have

$$Z_{\rho_A}(A) \cap \widehat{\mathcal{G}}(A) \subseteq \widehat{Z}_{\mathcal{G}}(A).$$

Let $z \in Z_{\rho_A}(A) \cap \widehat{\mathcal{G}}(A)$. Let $\overline{x}$ be the image of z in $Z_{\rho_B}(B) \cap \widehat{\mathcal{G}}(B)$. By our hypothesis, $\overline{x} \in \widehat{Z}_{\mathcal{G}}(B)$. Let $x \in \widehat{Z}_{\mathcal{G}}(A)$ be a lift of $\overline{x}$. Suppose that $z \mapsto \overline{x}$. Then we can write $z = x \cdot (\mathbb{1} + tY)$ where t is a generator of the kernel $A \to B$ and $Y \in \mathrm{Lie}(\mathcal{G})(A)$.

Since z commutes with the image of ρ_A, we must have for every $\sigma \in G$,

$$(x\mathbb{1} + txY)\rho_A(\sigma) = \rho_A(\sigma)(x\mathbb{1} + txY).$$

This gives

$$Y\rho_A(\sigma) = \rho_A(\sigma)Y.$$

Reducing modulo the maximal ideal $\mathfrak{m}_A$ and using the fact $Z_{\overline{\rho}} = k$, we see that Y is of the form $Y = a\mathbb{1} + Y_1$ where $a \in A$ and the entries of Y_1 belong to $\mathfrak{m}_A$. Since $A \to B$ is small, we have $t\mathfrak{m}_A = 0$; it follows that $z = x \cdot (ta + 1)\mathbb{1} \in \widehat{Z}_{\mathcal{G}}(A)$. ■

Suppose that $Z_{\overline{\rho}} = k$. We will now verify the condition ***(H4)*** of Schlessinger's criteria. Consider a diagram in $\underline{\mathbf{CNL}}_W^0$

$$\begin{array}{ccc} A_3 & \xrightarrow{\beta_1} & A_1 \\ {\scriptstyle\beta_1}\downarrow & & \downarrow{\scriptstyle\alpha_1} \\ A_1 & \xrightarrow[\alpha_1]{} & A_0 \end{array}$$

and assume that $\alpha_1 : A_1 \to A_0$ is surjective. Given $\pi(\rho_3), \pi(\rho_3)' \in \mathscr{D}(A_3)$ with same images in $\mathscr{D}(A_1) \times_{\mathscr{D}(A_0)} \mathscr{D}(A_1)$. In other words, we are given two representations $\rho_3 = (\rho_1, \rho_2) : G \to \mathcal{G}(A_3)$ and $\rho_3' = (\rho_1', \rho_2') : G \to \mathcal{G}(A_3)$ such that for $i = 1, 2$ there exists $g_i \in \widehat{\mathcal{G}}(A_1)$ we have $\rho_i' = {}^{g_i}\rho_i$. Let $\rho_{30} = \alpha_1 \circ \rho_1 = \alpha_1 \circ \rho_2$ and similarly for ρ_{30}'. Composing with α_1, we obtain

$$\rho_{30}' = {}^{g_{10}}\rho_{30} = {}^{g_{20}}\rho_{30}$$

hence $z_0 = g_{10}^{-1}g_{20} \in Z_{\rho_{30}} \cap \widehat{\mathcal{G}}(A_0)$. From the previous lemma, $Z_{\rho_{30}} \cap \widehat{\mathcal{G}}(A_0)$ consists of the scalar matrices in $\widehat{\mathcal{G}}(A_0)$ if $\mathcal{G} = \mathbf{GL}_1$ or $\mathbf{GL}_2$.

We have $\alpha_1 : \widehat{Z}_{\mathcal{G}}(A_1) \to \widehat{Z}_{\mathcal{G}}(A_0)$ is surjective by the formal smoothness. Hence there exists $z_1 \in \widehat{Z}_{\mathcal{G}}(A_1)$ mapping to z_0 such that by putting $g_1' = z_1 g_1 = g_1 z_1 \in \widehat{\mathcal{G}}(A_1)$, we have

$$g_3 = (g_1', g_2) \in \widehat{\mathcal{G}}(A_3)$$

and

$$\rho_3' = (\rho_1', \rho_2') = ({}^{g_1'}\rho_1, {}^{g_2}\rho_2) = {}^{g_3}\rho_3.$$

That is, $\pi(\rho_3)' = \pi(\rho_3)$, and the condition ***(H4)*** is true.

§ 4.5. *The main theorem*

The upshot is:

Theorem 4.5.1 (Mazur [20], Ramakrishna [23]). *Let $\mathcal{G}$ be $\mathbf{GL}_1$ or $\mathbf{GL}_2$. Suppose that G is a profinite group satisfying the p-finiteness condition Φ_p and $\overline{\rho} : G \to \mathcal{G}(k)$ is a continuous representation such that $Z_{\overline{\rho}} = k$. Then there exists a ring R in $\underline{\mathbf{CNL}}_W$ and a deformation ρ^{u} of $\overline{\rho}$ to R,*

$$\rho^{\mathrm{u}} : G \to \mathcal{G}(R)$$

such that any deformation of $\overline{\rho}$ to a complete noetherian local W-algebra A is obtained from ρ^{u} via a unique morphism $R \to A$.

§ 4.6. *Absolutely irreducible representations*

The hypothesis that $Z_{\overline{\rho}} = k$ plays an important role in the main theorem. It is of great significance to ask which representations have this property.

Definition 4.6.1. (1) A representation $\overline{\rho} : G \to \mathcal{G}(k)$ is said to be *reducible* if the representation space has a proper subspace that is invariant under the action of G.

(2) It is said to be *irreducible* if no such subspace exists.

(3) We say that $\overline{\rho}$ is *absolutely irreducible* if there is no extension k'/k such that $\overline{\rho} \otimes_k k'$ is reducible.

Example 4.6.2. The irreducible two-dimensional representation of the symmetric group S_3 of order 6 over $\mathbb{Q}$ is absolutely irreducible.

Example 4.6.3. The representation of the circle group by rotations in the plane is irreducible over $\mathbb{R}$, but is not absolutely irreducible. After extending to $\mathbb{C}$, it splits into two irreducible components. This is to be expected, since the circle group is commutative and it is known that all irreducible representations of commutative groups over an algebraically closed field are one-dimensional.

The following theorem can be found in any standard textbook on group representation theory. For example, see Chapter 1 of Serre's book [26].

Theorem 4.6.4 (Schur's Lemma). *If the representation $\overline{\rho} : G \to \mathcal{G}(k)$ is absolutely irreducible, then $Z_{\overline{\rho}} = k$.*

Hence, absolutely irreducible representations have universal deformations. However, there is important other case where $\overline{\rho}$ is not irreducible but still satisfies $Z_{\overline{\rho}} = k$.

Proposition 4.6.5. *Let k be any field, and let V be any representation of G with a G-stable filtration $V_1 \subset V_2 \subset \cdots \subset V_n = V$ such that:*

(a) V_{i+1}/V_i is one-dimensional with G acting by χ_i;

(b) The χ_i are distinct;

(c) The extension $V_i/V_{i-1} \to V_{i+1}/V_{i-1} \to V_{i+1}/V_i$ is non-split for all i.

Then $Z_{\overline{\rho}} = k$.

Proof. Let $M \in Z_{\overline{\rho}}$. We claim that M is a scalar. We first note that V_1 is the unique one-dimensional subspace on which G acts via χ_1. For if V_1' were another, we could build a Jordan-Holder series $V_1 \subset V_1 \cup V_1' \subset \cdots$ and thus χ_1 would appear at least twice in the Jordan-Holder decomposition which cannot happen since χ_i are distinct.

It follows then that M preserves V_1 and by induction preserves the whole flag. Let M act on V_1 by multiplication by a. We will show that $M = a\mathbb{1}$. Consider $M - a\mathbb{1} : V \to V$. This element $M - a\mathbb{1}$ is also in $Z_{\overline{\rho}}$. Since $M - a\mathbb{1}\mid_{V_1} = 0$, it factors as a morphism

$$T : V/V_1 \to V.$$

By induction, the induced map $V/V_1 \to V/V_1$ is G-invariant which is multiplication by a scalar b. If $b \neq 0$, then $T|_{V_2}$ would give a splitting of the extension where $i = 1$ and so we can assume $b = 0$.

Thus, T is actually a G-invariant map $V/V_1 \to V$. If $T = 0$, then we are done, else let V_i be the first subspace on which it is non-trivial. Then $T : V_i/V_{i-1} \to V_1$ is a G-module isomorphism, contradiction. ■

§ 4.7. *Example: the case* $\mathbf{GL}_1$

For $\mathcal{G} = \mathbf{GL}_1$ and $\overline{\rho} : G \to k^\times$, we see that the assumptions $Z_{\overline{\rho}} = k$ and the center of $\mathbf{GL}_1$ is formally smooth over W are trivially fulfilled. We will compute $R = R^{\mathrm{u}}$ and ρ^u in this section.

Consider the deformation ρ of $\overline{\rho}$ to A, i.e., a character

$$\rho : G \to A^\times.$$

Since $A \in \mathrm{Obj}(\underline{\mathbf{CNL}}_W)$, the reduction morphism $A \to k$ has a multiplicative lifting $\omega_A : k^\times \to A^\times$ called the Teichmüller lifting which is functorial: if $A \xrightarrow{\alpha} B \to k$, then $\alpha \circ \omega_A = \omega_B$.

Write $\rho(\sigma) = \omega \circ \overline{\rho}(\sigma) \cdot \langle \rho \rangle(\sigma)$ with $\langle \rho \rangle(\sigma) \equiv 1 \pmod{\mathfrak{m}}$. Since $1 + \mathfrak{m}$ is pro-p abelian, the character $\langle \rho \rangle$ factors through the maximal p-abelian quotient $G^{p,\mathrm{ab}}$ of G. We define $\psi_\rho : W[\![G^{p,\mathrm{ab}}]\!] \to A$ as the unique local W-algebra homomorphism such that for all $\sigma \in G^{p,\mathrm{ab}}$

$$\psi_\rho([\sigma]) = \langle \rho \rangle(\sigma)$$

where $[\sigma]$ denotes the corresponding element of σ in the group ring $W[\![G^{p,\mathrm{ab}}]\!]$.

Proposition 4.7.1. *For $\mathcal{G} = \mathbf{GL}_1$, the universal pair $(R^{\mathrm{u}}, \rho^{\mathrm{u}})$ is given by*

$$R^{\mathrm{u}} = W[\![G^{p,\mathrm{ab}}]\!]$$

and

$$\begin{array}{rcl}\rho^{\mathrm{u}} : G & \to & W[\![G^{p,\mathrm{ab}}]\!] \\ \sigma & \mapsto & \omega(\overline{\rho}(\sigma)) \cdot [\sigma^{p,\mathrm{ab}}]\end{array}$$

where $\sigma \mapsto \sigma^{p,\mathrm{ab}}$ is the projection $G \to G^{p,\mathrm{ab}}$.

Proof. By the p-finiteness condition Φ_p, we know that $G^{p,\mathrm{ab}}$ is finitely generated as a $\mathbb{Z}_p$-module. If r is the number of generators, then $W[\![G^{p,\mathrm{ab}}]\!]$ is a quotient of the power series ring $W[\![t_1, \ldots, t_r]\!]$ and, therefore, is a complete noetherian local W-algebra.

Take any deformation ρ of $\overline{\rho}$ to A, i.e., $\rho : G \to A^{\times}$, we get a local W-algebra homomorphism $\psi_\rho : W[\![G^{p,\mathrm{ab}}]\!] \to A$ uniquely determined by the condition

$$\psi_\rho([\sigma]) = \langle \rho \rangle(\sigma).$$

But we have

$$\begin{array}{rcl}\psi_\rho(\rho^{\mathrm{u}}(\sigma)) & = & \psi_\rho(\omega(\overline{\rho}(\sigma)) \cdot [\sigma^{p,\mathrm{ab}}]) \\ & = & \omega(\overline{\rho}(\sigma))\psi_\rho([\sigma^{p,\mathrm{ab}}]) \\ & = & \omega(\overline{\rho}(\sigma))\langle \rho \rangle(\sigma) \\ & = & \rho(\sigma),\end{array}$$

that is, $\psi_\rho \circ \rho^{\mathrm{u}} = \rho$. Thus $W[\![G^{p,\mathrm{ab}}]\!]$ is the universal deformation ring and ρ^{u} defined above is the universal deformation of ρ. ■

***Remark* 4.7.2.** If we fix an topological group isomorphism $G^{p,\mathrm{ab}} \simeq H \times \mathbb{Z}_p^r$ where H is a finite group, we obtain a local W-algebra isomorphism

$$W[\![G^{p,\mathrm{ab}}]\!] \simeq W[\![t_1, \ldots, t_r]\!][H].$$

That is, the universal deformation ring is the group algebra of a finite group over an Iwasawa algebra, ring of formal power series in r variables over W.

Appendix A

Categories and Functors

It is my experience that proofs involving matrices can be shortened by 50% if one throws the matrices out.

Emil Artin, *Geometric Algebra*

The language of categories and functors is a particularly convenient way to think about the deformation theory. We will introduce the concept of categories to serve as a useful tool and to provide a general context for dealing with a number of different mathematical situations in this master thesis. The more details and materials are contained in the book of Mac Lane [19].

§ A.1. Categories

Definition A.1.1. A *category* $\mathfrak{C}$ is defined by the following two data:

- a collection of objects of $\mathfrak{C}$, denoted by $\mathrm{Obj}(\mathfrak{C})$;
- For any A and B in $\mathrm{Obj}(\mathfrak{C})$, there is a *set* $\mathrm{Hom}_{\mathfrak{C}}(A, B)$ and referred to as the set of morphisms from A into B.

satisfying the following rules:

(a) For any A, B and C in $\mathrm{Obj}(\mathfrak{C})$, there is a rule of composition for morphisms, i.e., a mapping: $\mathrm{Hom}_{\mathfrak{C}}(A, B) \times \mathrm{Hom}_{\mathfrak{C}}(B, C) \to \mathrm{Hom}_{\mathfrak{C}}(A, C) : (f, g) \mapsto g \circ f$;

(b) *(Associativity).* For any three morphisms: $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, we have $h \circ (g \circ f) = (h \circ g) \circ f$;

(c) For each A in $\mathrm{Obj}(\mathfrak{C})$, there is an element $1_A \in \mathrm{Hom}_{\mathfrak{C}}(A, A)$ such that $1_A \circ f = f$ and $g \circ 1_A = g$ for all $f : B \to A$ and $g : A \to B$.

We list some examples of categories which are frequently used in this master thesis:

Example A.1.2. The collection of all sets forms a category which we denote by $\underline{\mathbf{Sets}}$. For $A, B \in \mathrm{Obj}(\underline{\mathbf{Sets}})$, the set $\mathrm{Hom}_{\underline{\mathbf{Sets}}}(A, B)$ is nothing but the set of all mappings from A into B; the composition of morphisms is the usual composition of mappings.

Example A.1.3. The collection of all abelian groups forms a category which we denote by $\underline{\mathbf{Ab}}$. For $A, B \in \mathrm{Obj}(\underline{\mathbf{Sets}})$, the set $\mathrm{Hom}_{\underline{\mathbf{Ab}}}(A, B)$ is the set of all group homomorphisms from A into B.

Example A.1.4. Let $\mathcal{O}$ be a discrete valuation ring of characteristic 0 with the maximal ideal $\mathfrak{m}$. Suppose that $k = \mathcal{O}/\mathfrak{m}$ has characteristic $p > 0$. The collection of all complete noetherian local $\mathcal{O}$-algebras A with $\phi : A/\mathfrak{m}_A \xrightarrow{\simeq} k$ forms a category which we denote by $\underline{\mathbf{CNL}_{\mathcal{O}}}$. For any A, $B \in \mathrm{Obj}(\underline{\mathbf{CNL}_{\mathcal{O}}})$, the set $\mathrm{Hom}_{\underline{\mathbf{CNL}_{\mathcal{O}}}}(A, B)$ is the set of all local $\mathcal{O}$-algebra homomorphisms commute with the ϕ's.

Example A.1.5. Let G be a profinite group. We define $\underline{\mathbf{Mod}_G}$ to be the category consisting of discrete G-modules with continuous G-action and continuous G-linear maps.

Example A.1.6. If $\mathfrak{C}$ is a category, then we can get another category $\mathfrak{C}^{\mathrm{opp}}$ by keeping the objects, but putting $\mathrm{Hom}_{\mathfrak{C}^{\mathrm{opp}}}(A, B) = \mathrm{Hom}_{\mathfrak{C}}(B, A)$. It is a easy to verify that $\mathfrak{C}^{\mathrm{opp}}$ is a category. It is called the *dual category of* $\mathfrak{C}^{\mathrm{opp}}$.

Definition A.1.7. (1) A category $\mathfrak{C}'$ is a *subcategory* of $\mathfrak{C}$ if the following two conditions are satisfied:

(a) Each object of $\mathfrak{C}'$ is an object of $\mathfrak{C}$ and $\mathrm{Hom}_{\mathfrak{C}'}(A, B) \subseteq \mathrm{Hom}_{\mathfrak{C}}(A, B)$;

(b) The composition of morphisms is the same in $\mathfrak{C}$ and in $\mathfrak{C}'$.

(2) A subcategory $\mathfrak{C}'$ is called a *full* subcategory of $\mathfrak{C}$ if $\mathrm{Hom}_{\mathfrak{C}'}(A, B) = \mathrm{Hom}_{\mathfrak{C}}(A, B)$ for any two objects A, B in $\mathfrak{C}'$.

Example A.1.8. Let $\underline{\mathbf{Rel}}$ be the category whose objects are sets and whose morphisms $A \to B$ are relations $R \subseteq A \times B$. Two relations $R \subseteq A \times B$ and $S \subseteq B \times C$ may be composed via

$$S \circ R = \{(a,c) \mid \text{ there exists } b \in B, (a,b) \in R \text{ and } (b,c) \in S\}.$$

Category $\underline{\mathbf{Rel}}$ has the category of sets $\underline{\mathbf{Sets}}$ as a subcategory, where the morphism $f : A \to B$ in $\underline{\mathbf{Sets}}$ corresponds to the functional relation $F \subseteq A \times B$ defined by: $(a,b) \in F$ if and only if $f(a) = b$.

Example A.1.9. The collection of all artinian local rings in $\underline{\mathbf{CNL}}_{\mathcal{O}}$ forms a full subcategory which is denoted by $\underline{\mathbf{CNL}}^0_{\mathcal{O}}$. Notice that the maximal ideal of an artinian local ring is always nilpotent and hence such rings are complete and noetherian. The objects of $\underline{\mathbf{CNL}}_{\mathcal{O}}$ are pro-objects of $\underline{\mathbf{CNL}}^0_{\mathcal{O}}$, that is, that any object of $\underline{\mathbf{CNL}}_{\mathcal{O}}$ is a projective limit of objects of $\underline{\mathbf{CNL}}^0_{\mathcal{O}}$.

§ A.2. Functors

Definition A.2.1. Let $\mathfrak{C}$ and $\mathfrak{D}$ be two categories. A *covariant* (resp. *contravariant) functor* $\mathscr{F} : \mathfrak{C} \to \mathfrak{D}$ is a rule associating an object $\mathscr{F}(A)$ of $\mathfrak{D}$ and a morphism $\mathscr{F}(f) \in \mathrm{Hom}_{\mathfrak{D}}(\mathscr{F}(A), \mathscr{F}(B))$ (resp. $\mathscr{F}(f) \in \mathrm{Hom}_{\mathfrak{D}}(\mathscr{F}(B), \mathscr{F}(A))$) to each object A of $\mathfrak{C}$ and each morphism $f \in \mathrm{Hom}_{\mathfrak{C}}(A, B)$ satisfying

$$\mathscr{F}(f \circ g) = \mathscr{F}(f) \circ \mathscr{F}(g) \qquad (\text{ resp. } \mathscr{F}(f \circ g) = \mathscr{F}(g) \circ \mathscr{F}(f))$$

and

$$\mathscr{F}(1_A) = 1_{\mathscr{F}(A)}.$$

Example A.2.2. Let G be a profinite group. The association of the G-invariant submodule to each object in the category:

$$M \mapsto \mathrm{H}^0(G, M) = M^G := \{m \in M \mid gm = m \text{ for all } g \in G\}$$

is a covariant functor from $\underline{\mathbf{Mod}}_G$ into $\underline{\mathbf{Ab}}$, called the *fixed module* functor. Each G-linear homomorphism $\phi : M \to N$ induces $\phi^G : M^G \to N^G$ by G-linearity.

Example A.2.3. The category of covariant functors $\underline{\mathbf{Fun}}(\mathfrak{C}, \mathfrak{D})$ from the category $\mathfrak{C}$ to the category $\mathfrak{D}$ is defined by letting the objects be the covariant functors from $\mathfrak{C}$ to $\mathfrak{D}$, and for two such functors $\mathscr{F}$ and $\mathscr{G}$ we let

$$\mathrm{Hom}_{\underline{\mathbf{Fun}}(\mathfrak{C},\mathfrak{D})}(\mathscr{F}, \mathscr{G})$$

be collections $\{\Psi_A\}_{A \in \mathrm{Obj}(\mathfrak{C})}$ of morphisms $\Psi_A : \mathscr{F}(A) \to \mathscr{G}(A)$, such that whenever $f \in \mathrm{Hom}_{\mathfrak{C}}(A, B)$, then the following diagram commutes:

$$\begin{tikzcd}
\mathscr{F}(A) \arrow[r, "\Psi_A"] \arrow[d, "\mathscr{F}(\varphi)"'] & \mathscr{G}(A) \arrow[d, "\mathscr{G}(\varphi)"] \\
\mathscr{F}(B) \arrow[r, "\Psi_B"'] & \mathscr{G}(B)
\end{tikzcd}$$

The morphisms of functors are often called *natural transformations*. The commutative diagram above is then called the *naturality condition*. If, for every object A in $\mathfrak{C}$, the morphism Ψ_A is an isomorphism in $\mathfrak{D}$, then Ψ is said to be a *natural isomorphism* or sometimes *isomorphism of functors*. Two functors $\mathscr{F}$ and $\mathscr{G}$ are called *naturally isomorphic* or simply *isomorphic* if there exists a natural isomorphism $\mathscr{F}$ to $\mathscr{G}$.

§ A.3. Representability

Let $\mathfrak{C}$ be a category, and let $A \in \mathrm{Obj}(\mathfrak{C})$. We define a contravariant functor $\mathbf{h}_A : \mathfrak{C} \to \underline{\mathbf{Sets}}$ by $\mathbf{h}_A(B) = \mathrm{Hom}_{\mathfrak{C}}(B, A)$ for any object B in $\mathfrak{C}$. For a morphisms $f : B_1 \to B_2$, we let

$$\mathbf{h}_A(f) : \mathrm{Hom}_{\mathfrak{C}}(B_2, A) \to \mathrm{Hom}_{\mathfrak{C}}(B_1, A)$$

by $g \mapsto g \circ f$. We extend a notation from algebraic geometry, and refer to the functor $\mathbf{h}_A$ as *the functor of points of the object A*. We also refer to the set $\mathbf{h}_A(B) = \mathrm{Hom}_{\mathfrak{C}}(B, A)$ as the set of B-valued points of the object A in $\mathfrak{C}$.

Definition A.3.1. A contravariant functor $\mathscr{F} : \mathfrak{C} \to \underline{\mathbf{Sets}}$ is said to be *representable* by the object A of $\mathfrak{C}$ if there is an isomorphism of functors $\Psi : \mathbf{h}_A \to \mathscr{F}$.

Fact A.3.2. *Two objects A and B in the category $\mathfrak{C}$ are isomorphic if and only if the functors $\mathbf{h}_A$ and $\mathbf{h}_B$ are isomorphic.*

Given a contravariant functor $\mathscr{F} : \mathfrak{C} \to \underline{\mathbf{Sets}}$. Let A be an object in $\mathfrak{C}$, and let $\xi \in \mathscr{F}(A)$. For any object B of $\mathfrak{C}$, we then define a mapping as follows:

$$\begin{aligned} \Phi_B : \mathbf{h}_A(B) &\to \mathscr{F}(B) \\ f &\mapsto \mathscr{F}(f)(\xi). \end{aligned}$$

This is a morphism of contravariant functors $\Phi : \mathbf{h}_A \to \mathscr{F}$.

Fact A.3.3 (Yoneda's Lemma). *The functor $\mathscr{F}$ is representable by the object A if and only if there exists an element $\xi \in \mathscr{F}(A)$ such that the corresponding Φ is an isomorphism of contravariant functors. This is the case if and only if all Φ_B are bijective.*

Definition A.3.4. We say that the object A represents the functor $\mathscr{F}$ and that the element $\xi \in \mathscr{F}(A)$ is the *universal element*.

This language is tied to the following *universal mapping property*: For all elements $\eta \in \mathscr{F}(B)$, there exists a unique morphism $f : B \to A$ such that

$$\mathscr{F}(f)(\xi) = \eta.$$

***Remark* A.3.5.** For the covariant case, we define $\mathbf{h}^A : \mathfrak{C} \to \underline{\mathbf{Sets}}$ by setting $\mathbf{h}^A(B) = \mathrm{Hom}_{\mathfrak{C}}(A, B)$ for any object B in $\mathfrak{C}$, which is a covariant functor. We then similarly get the notion of a representable covariant functor $\mathfrak{C} \to \underline{\mathbf{Sets}}$. Of course this amounts to applying the contravariant case to the dual category $\mathfrak{C}^{\mathrm{opp}}$.

Appendix B

Cohomology for Profinite groups

Algebraic geometry seems to have acquired the reputation of being esoteric, exclusive, and very abstract, with adherents who are secretly plotting to take over all the rest of mathematics. In one respect this last point is accurate.

David Mumford

In this appendix, we recall the construction of group cohomology theory and study the basic properties. The bible for this subject is Serre [27], in conjunction with [25] or [3]. Haberland [11] is also an excellent reference.

§ B.1. G-modules

We fix a profinite group G.

Definition B.1.1. (1) An *abstract G-module* M is an abelian group M together with an action $G \times M \to M : (g, m) \mapsto gm$ such that $1m = m$, $(gh)m = g(hm)$ and $g(m+n) = gm + gn$ for all $g, h \in G$, $m, n \in M$.

(2) A *topological G-module* M is an abelian Hausdorff topological group M endowed with the structure of an abstract G-module such that the action $G \times M \to M$ is continuous.

(3) By a *discrete G-module* M, we mean that M is a topological G-module such that the action $G \times M \to M$ is continuous for the discrete topology on M.

For a closed subgroup $H \subset G$, we denote the subgroup of H-invariant elements in M by M^H, i.e.,

$$M^H = \{m \in M \mid hm = m \text{ for all } h \in H\}.$$

Fact B.1.2. *Let G be a profinite group and let M be an abstract G-module. Then the following statements are equivalent:*

(i) M is a discrete G-module;

(ii) For every $m \in M$, the subgroup $G_m := \{g \in G \mid gm = m\}$ is open;

(iii) $M = \bigcup M^U$, where U runs through the open subgroups of G.

In this master thesis, we are mainly concerned with discrete modules, and so the term G-module, without the word "topological" or "abstract", will always mean a discrete module.

§ B.2. Cohomology for profinite groups

We fix a profinite group G. Let G acts on G^n by left multiplication. The cohomology for G arises from the diagram

$$\cdots \;\substack{\longrightarrow\\ \longrightarrow\\ \longrightarrow\\ \longrightarrow}\; G \times G \times G \;\substack{\longrightarrow\\ \longrightarrow\\ \longrightarrow}\; G \times G \rightrightarrows G,$$

the arrows being the projections $d_i : G^{n+1} \to G^n$ for each $i = 0, \ldots, n$ given by $d_i(\sigma_0, \ldots, \sigma_{i-1}, \widehat{\sigma_i}, \sigma_{i+1}, \ldots, \sigma_n)$, where by $\widehat{\sigma_i}$ we indicate that we have omitted σ_i from the $(n+1)$-tuple $(\sigma_0, \ldots, \sigma_n)$.

We assume that all G-modules to be discrete. For every G-module M, we form the abelian group $X^n = X^n(G, M) = \mathrm{Map}(G^{n+1}, M)$ of all continuous maps $x : G^{n+1} \to M$. X^n is a G-module by $(\sigma x)(\sigma_0, \ldots, \sigma_n) = \sigma x(\sigma^{-1}\sigma_0, \ldots \sigma^{-1}\sigma_n)$. The maps $d_i : G^{n+1} \to G^n$ induce G-module homomorphisms $d_i^* : X^{n-1} \to X^n$, and we form the alternating sum

$$\partial^n = \sum_{i=0}^{n} (-1)^i d_i^* : X^{n-1} \to X^n.$$

Fact B.2.1. *The sequence*

$$0 \longrightarrow M \xrightarrow{\partial^0} X^0 \xrightarrow{\partial^1} X^1 \xrightarrow{\partial^2} X^2 \xrightarrow{\partial^3} \cdots$$

is exact.

We apply the functor "fixed module", and set for $n \geq 0$

$$\mathrm{C}^n(G, M) = X^n(G, M)^G.$$

$\mathrm{C}^n(G, M)$ consists of the continuous functions $x : G^{n+1} \to M$ such that $x(\sigma\sigma_0, \ldots, \sigma\sigma_n) = \sigma x(\sigma_0, \ldots, \sigma_n)$ for all $\sigma \in G$. These functions are called the *n-cochains* of G with coefficients in M.

From the FACT B.2.1, we obtained a sequence

$$\mathrm{C}^0(G, M) \xrightarrow{\partial^1} \mathrm{C}^1(G, M) \xrightarrow{\partial^2} \mathrm{C}^2(G, M) \xrightarrow{\partial^3} \cdots,$$

which is no longer exact in general; but it is still a complex, i.e., $\partial^{n+1} \circ \partial^n = 0$. We now set

$$\begin{aligned} \mathrm{Z}^n(G, M) &= \ker(\mathrm{C}^n(G, M) \xrightarrow{\partial^{n+1}} \mathrm{C}^{n+1}(G, M)), \\ \mathrm{B}^n(G, M) &= \mathrm{im}(\mathrm{C}^{n-1}(G, M) \xrightarrow{\partial^n} \mathrm{C}^n(G, M)), \end{aligned}$$

and $\mathrm{B}^0(G, A) = 0$. Since $\partial^{n+1} \circ \partial^n = 0$, we have $\mathrm{B}^n(G, M) \subset \mathrm{Z}^n(G, M)$. The elements of $\mathrm{Z}^n(G, M)$ and $\mathrm{B}^n(G, M)$ are called the *n-cocycles* and *n-coboundaries* respectively.

DEFINITION B.2.2. For each $n \geq 0$, the quotient group

$$\mathrm{H}^n(G, M) = \mathrm{Z}^n(G, M)/\mathrm{B}^n(G, M)$$

is called the *n-dimensional cohomology group* of G with coefficients in M.

FACT B.2.3. *If G is a finite group and M is a finite G-module, then $\mathrm{H}^n(G, M)$ is a finite module for each $n \geq 0$.*

FACT B.2.4. *For $n = 0, 1$, and 2, the groups $\mathrm{H}^n(G, M)$ admit the following interpretations:*

(i) For $n = 0$, we have $\mathrm{H}^0(G, M) = M^G$;

(ii) For $n = 1$, we have

$$\mathrm{H}^1(G, M) = \frac{\{x : G \to M \mid x(\sigma\tau) = \sigma x(\tau) + x(\sigma)\ \forall \sigma, \tau \in G\}}{\{x : \sigma \mapsto (\sigma - 1)m \mid m \in M\}};$$

(iii) For n=2, we have

$$\mathrm{H}^2(G,M) \\ = \frac{\{x : G^2 \to M \mid x(\sigma\tau,\rho) + x(\sigma,\tau) = x(\sigma,\tau\rho) + \sigma x(\tau,\rho)\ \forall \sigma,\tau,\rho \in G\}}{\{x : G^2 \to M \mid x(\sigma,\tau) = y(\sigma) - y(\sigma\tau) + \sigma y(\tau)\}},$$

with arbitrary $y : G \to M \in \mathrm{C}^1(G,M)$.

Let $\{I, \leq\}$ be a directed set. Let $\{T_i\}_{i\in I}$ be a family of objects indexed by I and $f_{ij} : T_i \to T_j$ be a homomorphism for all $i \leq j$ with the following properties:

(a) f_{ii} is the identity of T_i, and

(b) $f_{ik} = f_{jk} \circ f_{ij}$ for all $i \leq j \leq k$.

The triple $\mathcal{I} = \{I, T_i, f_{ij}\}$ is called a *directed system*. The underlying set of the *direct limit*, T, of the direct system $\mathcal{I} = \{I, T_i, f_{ij}\}$ is defined as the disjoint union of the T_i's modulo a certain equivalence relation $\sim$:

$$\varinjlim_{I} T_i = \bigsqcup_{i\in I} T_i \Big/ \sim .$$

Here, if $t_i \in T_i$ and $t_j \in T_j$, $t_i \sim t_j$ if there is some $k \in I$ such that $f_{ik}(t_i) = f_{jk}(t_j)$.

Let U, V runs through the open normal subgroups of G. If $V \subseteq U$, then the projections $G^{n+1} \to (G/V)^{n+1} \to (G/U)^{n+1}$ induce homomorphisms

$$C^n(G/U, M^U) \to C^n(G/V, M^V) \to C^n(G,M),$$

which commute with the operators ∂^{n+1}. We thus obtain homomorphisms

$$\mathrm{H}^n(G/U, M^U) \to \mathrm{H}^n(G/V, M^V) \to \mathrm{H}^n(G,M).$$

The groups $\mathrm{H}^n(G/U, M^U)$ form a direct system and we have a canonical homomorphism $\varinjlim_U \mathrm{H}^n(G/U, M^U) \to \mathrm{H}^n(G,M)$.

Fact B.2.5. *The above homomorphism is an isomorphism:*

$$\varinjlim_{U} \mathrm{H}^n(G/U, M^U) \xrightarrow{\simeq} \mathrm{H}^n(G, M).$$

Fact B.2.6 (The inflation-restriction exact sequence)**.** *Let U be a closed normal subgroup of G, and suppose that $\mathrm{H}^m(G, M) = 0$ for all $m = 1, 2, \ldots, n-1$. Then the following sequence is exact:*

$$\begin{aligned} 0 &\longrightarrow \mathrm{H}^n(G/U, M^U) \longrightarrow \mathrm{H}^n(G, M) \longrightarrow \mathrm{H}^0(G/U, \mathrm{H}^n(U, M)) \\ &\longrightarrow \mathrm{H}^{n+1}(G/U, M^U). \end{aligned}$$

Bibliography

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[3] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory (2nd edition)*, London, United Kingdom, London Mathematical Society, 2010, Reprint of the 1967 original. MR 911121 (88h:11073)

[4] L. Clozel, M. Harris, and R. Taylor, *Automorphy for some l-adic lifts of automorphic mod l Galois representations*, Publ. Math. Inst. Hautes Études Sci. (2008), no. 108, 1–181, With Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras.

[5] B. Conrad, F. Diamond, and R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), no. 3, 521–567.

[6] B. de Smit and H. W. Lenstra, Jr. , *Explicit construction of universal deformation rings*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, 1997, pp. 313–326.

[7] F. Diamond, *On deformation rings and Hecke rings*, Ann. of Math. (2) **144** (1996), no. 1, 137–166.

[8] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 41–78.

[9] A. Grothendieck, *Technique de descente et théorèmes d'existence en géométrie algébrique. II. Le théorème d'existence en théorie formelle des modules*, Séminaire Bourbaki, vol. **5**, Société Mathématique de France, 1995, pp. 369–390.

[10] A. Grothendieck and J. Dieudonné, *Eléments de Géométrie Algébrique*, Publ. Math. IHES, **4** (1960), **8** (1961), **11** (1961), **17** (1963), **20** (1964), **24** (1965), **28** (1966), **32** (1967).

[11] K. Haberlan, *Galois Cohomology of Algebraic Number Fields*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1978, With two appendices by Helmut Koch and Thomas Zink.

[12] M. Harris, N. Shepherd-Barron, and R. Taylor, *A family of Calabi-Yau varieties and potential automorphy*, Ann. of Math. (2) **171** (2010), no. 2, 779–813.

[13] H. Hida, *Galois representations into* $\mathbf{GL}_2(\mathbb{Z}_p[\![X]\!])$ *attached to ordinary cusp forms*, Invent. Math. **85** (1986), no. 3, 545–613.

[14] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504.

[15] ———, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586.

[16] M. Kisin, *The Fontaine-Mazur conjecture for* $\mathbf{GL}_2$, J. Amer. Math. Soc. **22** (2009), no. 3, 641–690.

[17] ———, *Lecture Notes on Deformations of Galois Representations*, Clay Mathematics Institute 2009 Summer School on Galois Representations (University of Hawaii at Manoa, Honolulu, Hawaii), June 15 - July 10 2009.

[18] ———, *Moduli of finite flat group schemes and modularity*, Ann. of Math. (2) **170** (2009), no. 3, 1085–1180.

[19] S. Mac Lane, *Categories for the working mathematician*, 2nd ed., Graduate Texts in Mathematics, vol. **5**, Springer-Verlag, 1998.

[20] B. Mazur, *Deforming of Galois Representations*, Galois Groups over $\mathbb{Q}$ (Y. Ihara, K. Ribet, and J.-P. Serre, eds.), Mathematical Sciences Research Institute Publications, no. **16**, Springer-Verlag, 1987, pp. 385–437.

[21] ———, *An introduction to the deformation theory of Galois representations*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer-Verlag, New York, 1997, pp. 243–311.

[22] J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, vol. **322**, Springer-Verlag, 1999.

[23] R. Ramakrishna, *On a variation of Mazur's deformation functor*, Compositio Math. **87** (1993), 269–286.

[24] M. Schlessinger, *Functors of Artin rings*, Trans. A.M.S. **130** (1968), 208–222.

[25] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. **67**, Springer-Verlag, 1979.

[26] ———, *Linear representations of finite groups*, Graduate Texts in Mathematics, vol. **42**, Springer-Verlag, New York, 1996.

[27] ———, *Galois cohomology*, Springer Monographs in Mathematics, Springer-Verlag, 1997.

[28] R. Taylor, *Automorphy for some l-adic lifts of automorphic mod l Galois representations. II*, Publ. Math. Inst. Hautes Études Sci. (208), no. 108, 183–239.

[29] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), no. 3, 553–572.

[30] J. Tilouine, *Deformations of Galois representations and Hecke algebras*, Published for The Mehta Research Institute of Mathematics and Mathematical Physics, Allahabad, 1996.

[31] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. **141** (1995), no. 3, 443–551.

Index