Deforming Galois Representations

Yan Yau Cheng

Easter, 2022

Contents

1 Introduction

This essay is about Galois Deformations[1].

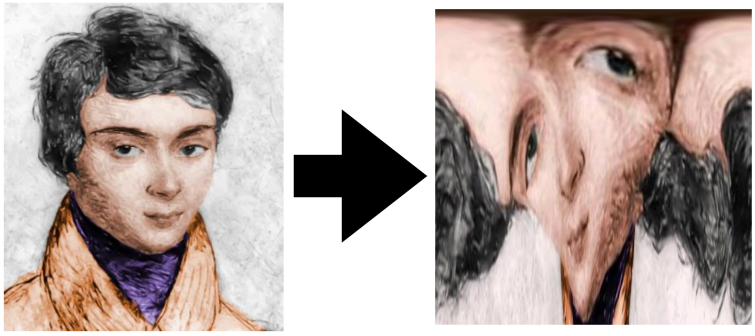


Figure 1: Galois, Deformed

Let k be a finite field, and R be a complete local Noetherian ring with maximal ideal $\mathfrak{m}_R$ and residue field k. Then there is a natural map $\mathrm{GL}_n(R) \to \mathrm{GL}_n(k)$ that is given component-wise by the quotient map $R \to R/\mathfrak{m}_R \cong k$.

Given a topological group Π and a ring R, a representation of Π is a continuous group homomorphism $\Pi \to \mathrm{GL}_n(R)$. Given a representation $\bar{\rho} : \Pi \to \mathrm{GL}_n(k)$, it's natural to ask how it lifts to a representation in $\mathrm{GL}_n(R)$. What representations $\rho : \Pi \to \mathrm{GL}_n(R)$ are there such that after composing with the map $\mathrm{GL}_n(R) \to \mathrm{GL}_n(k)$, gives us $\bar{\rho}$? In other words, we are looking for representations ρ such that the following diagram commutes:

$$\begin{array}{ccc} \Pi & \xrightarrow{\rho} & \mathrm{GL}_n(R) \\ & \searrow^{\bar{\rho}} & \downarrow \\ & & \mathrm{GL}_n(k) \end{array}$$

A deformation is a lift of this form modulo a "strict" equivalence relation, which we will define precisely in the next section.

The first main result of this essay will be to follow Mazur's paper and prove the existence of a *Universal Deformation Ring*. This is a ring $\mathcal{R}$ along with a lift $\boldsymbol{\rho} : \Pi \to \mathrm{GL}_n(\mathcal{R})$ such that for any ring R, all the deformations of $\bar{\rho}$ to $\mathrm{GL}_n(R)$ is given by the composition of $\boldsymbol{\rho}$ and some ring homomorphism $\varphi \in \mathrm{Hom}(\mathcal{R}, R)$. i.e. any lift $\rho : \Pi \to \mathrm{GL}_n(R)$ is given by $\rho = \varphi \circ \boldsymbol{\rho}$ for some $\varphi \in \mathrm{Hom}(\mathcal{R}, R)$.

$$\begin{array}{ccc} & & \mathrm{GL}_n(\mathcal{R}) \\ & \nearrow^{\boldsymbol{\rho}} & \downarrow{\scriptstyle \varphi} \\ \Pi & \xrightarrow{\rho} & \mathrm{GL}_n(R) \\ & \searrow^{\bar{\rho}} & \downarrow \\ & & \mathrm{GL}_n(k) \end{array}$$

These notions will be made formal and explained in detail over the next few sections.

For the remainder of the essay we will try to understand the Universal Deformation Ring better, and compute some explicit examples of $\mathcal{R}$ under certain hypotheses, following the work of Boston.

The majority of the essay will follow the papers [Maz89] and [Bos91], and the lecture notes given in [Gou08] has been a useful reference in the writing on this essay.

[1]Image Credits: `tinyurl.com/2fpjz9ah`

2 Setup

2.1 Some Group Theory

Suppose Π is a profinite group equipped with the profinite topology. We impose a finiteness condition on the group: [Maz89]

Definition. We say that Π satisfies the condition $\mathbf{\Phi}_p$ if for every open subgroup of finite index $\Pi_0 \subseteq \Pi$, there is only a finite number of continuous homomorphisms from Π_0 to $\mathbb{Z}/p\mathbb{Z}$. Where $\mathbb{Z}/p\mathbb{Z}$ is equipped with the discrete topology.

We will assume that Π satisfies condition $\mathbf{\Phi}_p$ throughout the essay.

Later on in the essay we will take Π to be the absolute Galois group of a local field or the maximal extension of a number field unramified outside of a finite set of primes, and we will show that both of these Galois groups indeed satisfy the condition $\mathbf{\Phi}_p$.

Definition. A *pro-p* group is a profinite group G such that every finite quotient G/N is a p-group. We define the *pro-p-completion* of G to be the profinite limit:

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

where N ranges over all normal subgroups where G/N is a finite p-group.

Given a profinite group G and its profinite completion $G^{(p)}$, there is a canonical continuous homomorphism $G \to G^{(p)}$ since there is a natural map $G \to G/N$ for each N in the profinite limit. In light of this the pro-p-completion satisfies the following universal property:

Proposition 1. If G is a profinite group and H is a pro-p group, then any homomorphism $G \to H$ factors uniquely through $G^{(p)}$.

Proof. If H is a pro-p group, this implies that $H = \varprojlim H_i$ and each H_i is a finite p-group.

Consider the map $\phi_i : G \to H_i$, the image of G must be a subgroup of H_i and must be a p-group. This means that this map factors through $G/\operatorname{Ker}\phi_i \cong \operatorname{Im}\phi_i$ which is a p-group.

This gives rise to a map $G^{(p)} \to G/\operatorname{Ker}\phi_i \to H_i$ for each i. Thus by the universal property of inverse limits, there is a unique map $G^{(p)} \to H$ and G factors through this map, concluding our proof. □

2.2 The Category of Complete Local Noetherian Rings

For the rest of this essay we fix k to be a finite field with characteristic p, we now define the category $\mathscr{C}$:

Definition. Let $\operatorname{ob}\mathscr{C}$ be the set of rings R that are complete, local and Noetherian with residue field k. By complete we mean that R is isomorphic to the inverse limit:

$$R = \varprojlim R/\mathfrak{m}_R^s$$

Moreover we define $\operatorname{mor}\mathscr{C}$ to be the local ring morphisms $\phi : R \to S$ that fix the residue field k. In other words, we require that $\phi(\mathfrak{m}_R) \subseteq \mathfrak{m}_S$ and that the induced map $R/\mathfrak{m}_R \to S/\mathfrak{m}_S$ given by $r + \mathfrak{m}_R \mapsto \phi(s) + \mathfrak{m}_S$ is the identity map on k.

Given this definition, we define several related categories:

- Suppose $\Lambda \in \mathscr{C}$, we define $\mathscr{C}_\Lambda$ to be the sub-category of $\mathscr{C}$ where we require that the objects of this category to be additionally Λ-Algebras and that the morphisms should additionally be Λ-algebra homomorphisms.

- We define $\mathscr{C}^0$ to be the full subcategory of local Artinian rings with residue field k. Note that any Artinian local ring is automatically Noetherian and complete so this is indeed a subcategory of $\mathscr{C}$.
- Finally, we define $\mathscr{C}^0_\Lambda$ to be the full subcategory of $\mathscr{C}_\Lambda$ of Artinian rings.

We prove a proposition:

Proposition 2. Every element in $\mathscr{C}$ is an inverse limit of objects in $\mathscr{C}^0$.

Proof. Suppose $R \in \mathscr{C}$, since we know that R is complete, $R = \varprojlim R/\mathfrak{m}^s$. It suffices to show that $R/\mathfrak{m}^s$ is Artinian, which means we need to show that it has dimension zero.

Suppose there is a prime ideal $\mathfrak{m}^s \subseteq \mathfrak{p}$, then since $\mathfrak{p}$ is a prime ideal this implies $\mathfrak{m} \subseteq \mathfrak{p}$ which gives $\mathfrak{m} = \mathfrak{p}$ by the maximality of $\mathfrak{m}$. Since prime ideals of $R/\mathfrak{m}^s$ correspond to prime ideals of R containing $\mathfrak{m}^s$, this implies that $R/\mathfrak{m}^s$ has only 1 prime ideal. Thus $R/\mathfrak{m}^s$ is Artinian.

□

Lemma 3. There is a canonical embedding $k \hookrightarrow R$, also known as the *Teichmüller Lift*.

This implies that there is a way to write elements in R uniquely as the sum of an element of k and an element in $\mathfrak{m}_R$:

$$R = k \oplus \mathfrak{m}_R$$

Proof. Complete local rings satisfy Hensel's lemma, so we can apply Hensel's Lemma to R.

Since $R/\mathfrak{m} = k \cong \mathbb{F}_{p^n}$ contains all $p^n - 1$th roots of unity, we can factor $X^{p^n-1} - 1$ into coprime linear polynomials in $\mathbb{F}_{p^n}$, and this factorisation can be lifted into R by Hensel's Lemma. The Teichmüller lift is simply the lift that identifies roots of the polynomial in k with the roots in R. □

We now define the *Witt vectors*:

Definition. The Witt vectors $W(k)$ for a finite field k is the ring of integers $\mathcal{O}_K$, for $K/\mathbb{Q}_p$ the unique unramified extension of $\mathbb{Q}_p$ with residue field k.

In other words, if $k = \mathbb{F}_{p^n}$ then $W(k) = \mathbb{Z}_p[\mu]$ where μ is a primitive $p^n - 1$th root of unity.

Proposition 4. Every ring $R \in \mathscr{C}$ has a canonical $W(k)$ algebra structure, and so $\mathscr{C} = \mathscr{C}_{W(k)}$. In other words $W(k)$ is an initial object of $\mathscr{C}$.

Proof. There is a unique map from $\mathbb{Z}$ to any ring R. Moreover, since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and R is a complete ring with respect to the $\mathfrak{m}_R$-adic topology, there is a unique map from $\mathbb{Z}_p \to R$ since morphisms in $\mathscr{C}$ must be continuous.

Finally, let $\bar{\mu}$ be the image of μ in $\mathbb{F}_{p^n}$. Since morphisms in the category $\mathscr{C}$ must fix the residue field, μ must be mapped to the Teichmüller lift of $\bar{\mu}$.

Thus there is a unique map from $W(k) = \mathbb{Z}_p[\mu]$ to R, and the map has been described above. □

Proposition 5. Every element of $\mathscr{C}_\Lambda$ is isomorphic to a quotient of a power series ring over Λ.

Proof. Let $R \in \mathscr{C}_\Lambda$ and since R is Noetherian, the maximal ideal is finitely generated. Suppose $\mathfrak{m}_R = (m_1, m_2, \cdots, m_n)$. Consider the map:

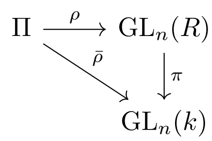
$$\phi : \Lambda[[X_1, X_2, \cdots, X_n]] \to R$$

given by $X_i \mapsto m_i$ and maps Λ to R canonically. This map surjects onto $\mathfrak{m}_R$ since its generators are in the image, and it is well defined because R is complete. Given an element $r \in R$, since the map $\Lambda \to R$ fixes the residue field, there is a $\lambda \in \Lambda$ such that $\phi(\lambda) - r \in \mathfrak{m}_R$. But since ϕ surjects onto $\mathfrak{m}_R$, it follows that it must also surject onto R.

Thus R must be isomorphic to a quotient of $\Lambda[[X_1, X_2, \cdots, X_n]]$, as desired. □

2.3 The Deformation Functor

Let $\bar{\rho} : \Pi \to \mathrm{GL}_n(k)$ be a continuous group homomorphism. For a ring R in the category $\mathscr{C}$, a lift of $\bar{\rho}$ is a map $\rho : \Pi \to \mathrm{GL}_n(R)$ such that upon composing by the map $\pi : \mathrm{GL}_n(R) \to \mathrm{GL}_n(k)$, we get $\bar{\rho}$. In other words we want to look for maps ρ such that the following map commutes:



Now we define the notion of equivalence. Note that we can conjugate ρ by a matrix in $M \in \mathrm{GL}_n(R)$ and obtain another representation $g \mapsto M^{-1}\rho(g)M$. However, after conjugating by M this new representation may not restrict to $\bar{\rho}$ upon projection onto $\mathrm{GL}_n(k)$. So we want to impose a condition on M such that it is the identity upon projecting to $\mathrm{GL}_n(k)$. We make the definition:

Definition (Strict Equivalence)**.** Let

$$\Gamma_n(R) = \mathrm{Ker}\,(\pi : \mathrm{GL}_n(R) \to \mathrm{GL}_n(k))$$

Then we say two lifts $\rho_1, \rho_2 : \Pi \to \mathrm{GL}_n(R)$ are *strictly equivalent* if there is a matrix $M \in \Gamma_n(R)$ such that for all $g \in \Pi$:

$$\rho_1(g) = M^{-1}\rho_2(g)M$$

This is clearly an equivalence relation, so we write $[\rho]$ to denote the strict equivalence class of ρ.

Using this definition, we can now define the notion of a deformation:

Definition (Deformation)**.** A *deformation* of $\bar{\rho}$ to R is a strict equivalence class of representations $[\rho]$ such that $\rho : \Pi \to \mathrm{GL}_n(R)$ is a lift of $\bar{\rho}$.

Given a representation $\bar{\rho}$ and a ring $R \in \mathscr{C}$, we can find all possible deformations of $\bar{\rho}$ to R. Let $\boldsymbol{D}_{\bar{\rho}}(R)$ denote the set of all possible deformations. In other words. Let $E(R)$ be set of all lifts of $\bar{\rho}$ to R, then the set $\boldsymbol{D}_{\bar{\rho}}(R)$ is:

$$\boldsymbol{D}_{\bar{\rho}}(R) = E(R)/\Gamma_n(R)$$

Turns out this is actually a functor:

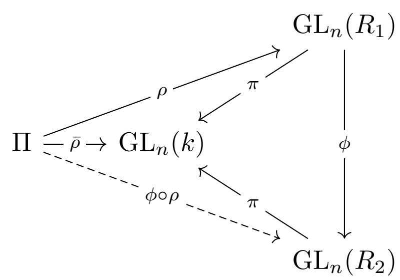
Proposition 6. $\boldsymbol{D}_{\bar{\rho}} : \mathscr{C} \to \mathsf{Set}$ is a functor.

Proof. Suppose that $R_1, R_2 \in \mathscr{C}$ and $\phi : R_1 \to R_2$ is a morphism in $\mathscr{C}$. In other words ϕ is a ring map that induces the identity map on the residue fields of R_1 and R_2.

We first need to define $\boldsymbol{D}_{\bar{\rho}}(\phi) : \boldsymbol{D}_{\bar{\rho}}(R_1) \to \boldsymbol{D}_{\bar{\rho}}(R_2)$. For $[\rho] \in \boldsymbol{D}_{\bar{\rho}}(R_1)$, we define:

$$\boldsymbol{D}_{\bar{\rho}}(\phi)([\rho]) := [\phi \circ \rho]$$

We check that this is well defined. First of all, since ϕ induces the identity map on the residue fields, the following diagram commutes:



So $\phi \circ \rho$ is indeed a lift of $\bar{\rho}$, and so $[\phi \circ \rho] \in \boldsymbol{D}_{\bar{\rho}}(R_2)$. Moreover, suppose $[\rho] = [\rho']$, then there is some $M \in \Gamma_n(R_1)$ such that $\rho(g) = M^{-1}\rho'(g)M$. Note that again by the fact that ϕ induces the identity on residue fields, that $\phi(M) \in \Gamma_n(R_2)$. Thus we have that:

$$\phi(\rho(g)) = \phi(M)^{-1}\phi(\rho'(g))\phi(M)$$

Which implies $[\phi \circ \rho] = [\phi \circ \rho']$, and so $\boldsymbol{D}_{\bar{\rho}}(\phi)$ is well defined.

Finally we check that $\boldsymbol{D}_{\bar{\rho}}$ is actually a functor. However, this follows immediately from the definition given since $\boldsymbol{D}_{\bar{\rho}}(\phi \circ \psi)(\rho) = (\phi \circ \psi) \circ \rho = \phi \circ (\psi \circ \rho) = \boldsymbol{D}_{\bar{\rho}}(\phi)\boldsymbol{D}_{\bar{\rho}}(\psi)\rho$. □

We can similarly define $\boldsymbol{D}_{\bar{\rho},\Lambda}$ for the restriction of $\boldsymbol{D}_{\bar{\rho}}$ to the subcategory $\mathscr{C}_\Lambda$. Since the representation $\bar{\rho}$ is often fixed, if the context is clear this may be dropped from the notation, so we write $\boldsymbol{D}$ and $\boldsymbol{D}_\Lambda$ instead.

2.3.1 The Deformation Functor is Continuous

Next we want to show that the functor $\boldsymbol{D}_{\bar{\rho}}$ is uniquely determined by where it sends elements of $\mathscr{C}^0$. To do that we first define the notion of a *continuous functor* on $\mathscr{C}$.

Suppose $\mathscr{F}$ is a functor on $\mathscr{C}$ and $R \in \mathscr{C}$ has maximal ideal $\mathfrak{m}$. Then the quotient map $R \to R/\mathfrak{m}^k$ induces a map $\mathscr{F}(R) \to \mathscr{F}(R/\mathfrak{m}^k)$ for each k. Thus these maps factor into a unique map:

$$\mathscr{F}(R) \to \varprojlim \mathscr{F}(R/\mathfrak{m}^k)$$

Note that since R is complete, $R \cong \varprojlim R/\mathfrak{m}^k$. We say that the functor $\mathscr{F}$ is continuous if the the functor commutes with the action of profinite limit:

Definition. Suppose $\mathscr{F}$ is a functor on $\mathscr{C}$. Then $\mathscr{F}$ is *continuous* if the natural morphism

$$\mathscr{F}(R) \to \varprojlim \mathscr{F}(R/\mathfrak{m}^k)$$

is in fact an isomorphism.

We now prove a lemma:

Lemma 7. The functor $\boldsymbol{D}_{\bar{\rho}}$ is continuous.

This proof will largely follow the structure of the proof of Lemma 2.3 in [Gou08]. The difficulty of the proof lies in the fact that the functor maps to equivalence classes of homomorphisms, rather than the homomorphisms themselves.

Proof. We quote without proof the two following identities which can be easily checked:

$$\mathrm{GL}_n(R) = \varprojlim \mathrm{GL}_n(R/\mathfrak{m}^k)$$
$$\Gamma_n(R) = \varprojlim \Gamma_n(R/\mathfrak{m}^k)$$

Additionally, since the quotient map $R/\mathfrak{m}^{k+1} \to R/\mathfrak{m}^k$ is surjective, it follows that the maps $\mathrm{GL}_n(R/\mathfrak{m}^{k+1}) \to \mathrm{GL}_n(R/\mathfrak{m}^k)$ and $\Gamma_n(R/\mathfrak{m}^{k+1}) \to \Gamma_n(R/\mathfrak{m}^k)$ are also surjective, since those maps are defined entry-wise.

The natural map $\boldsymbol{D}_{\bar{\rho}}(R) \to \varprojlim \boldsymbol{D}_{\bar{\rho}}(R/\mathfrak{m}^k)$ sends the strict equivalence class of a representation $\rho : \Pi \to \mathrm{GL}_n(R)$ to a sequence of classes of representations $\left\{[\rho_k : \Pi \to \mathrm{GL}_n(R/\mathfrak{m}^k)]\right\}_{k\in\mathbb{Z}^+}$ where ρ_k is obtained by composing ρ with the quotient map $R \to R/\mathfrak{m}^k$.

We first show that this map is surjective. Suppose that $\{[\rho_k]\}_{k\in\mathbb{Z}^+}$ be an inverse sequence of representations, so ρ_{k+1} composed with the quotient map $\mathrm{GL}_n(R/\mathfrak{m}^{k+1}) \to \mathrm{GL}_n(R/\mathfrak{m}^k)$ is strictly equivalent to ρ_k. This means that there is some $M_k \in \Gamma_n(R/\mathfrak{m}^k)$ such that:

$$\rho_k = M_k^{-1}(\rho_{k+1} \mod \mathfrak{m}^k)M_k$$

We can pick a lift $M_{k+1} \in \Gamma_n(R/\mathfrak{m}^{k+1})$ of M_k, and since we are working in the strict equivalence class of representations, $[\rho_{k+1}] = [M_{k+1}^{-1}\rho_{k+1}M_{k+1}]$. Without loss of generality we can replace ρ_{k+1} with $M_{k+1}^{-1}\rho_{k+1}M_{k+1}$ instead, and in doing so we obtain that $\rho_k = \rho_{k+1} \mod \mathfrak{m}^k$. Inductively we can choose representatives ρ_k of $[\rho_k]$ such that the sequence $\{\rho_k\}_k$ is compatible with quotient maps. Since we know that $\mathrm{GL}_n(R) = \varprojlim \mathrm{GL}_n(R/\mathfrak{m}^k)$, then by the universal property of inverse limits there is a unique map ρ that is compatible with all these maps. Thus $[\rho]$ maps to this sequence, and the map is surjective.

Next we show that the map is injective. Suppose $[\rho], [\rho'] \in \boldsymbol{D}_{\bar{\rho}}(R)$ and $\rho_k = \rho \mod \mathfrak{m}^k$, and $\rho'_k = \rho' \mod \mathfrak{m}^k$. Then we want to show that if ρ_k is strictly equivalent to ρ'_k for every k, then ρ is strictly equivalent to ρ'.

If ρ_k is strictly equivalent to ρ'_k then there exists $M_k \in \Gamma_n(R/\mathfrak{m}^k)$ such that $\rho_k = M_k^{-1}\rho'_k M_k$. We can pick M_k inductively such that $M_k = M_{k+1} \mod \mathfrak{m}^k$, so using the fact that $\Gamma_n(R) = \varprojlim \Gamma_n(R/\mathfrak{m}^k)$, there is a $M \in \Gamma_n(R)$ that restricts to every M_k upon taking mod $\mathfrak{m}^k$, and thus $\rho = M^{-1}\rho' M$ and so the map is injective.

So the natural map is indeed bijective, which implies $\boldsymbol{D}$ is continuous. □

This lemma is important because $R/\mathfrak{m}^k$ are objects of $\mathscr{C}^0$, and the lemma shows that if we know the values of the functor $\boldsymbol{D}_{\bar{\rho}}$ on $\mathscr{C}^0$, then we know the functor on all of $\mathscr{C}$.

Note also that although the above proof was about the functor $\boldsymbol{D}_\rho$, the exact same proof will also show that $\boldsymbol{D}_{\rho,\Lambda}$ is continuous.

2.4 Representability

For $R \in \mathscr{C}$, define the set-valued functor $\boldsymbol{h}_R(-) = \mathrm{Mor}_{\mathscr{C}}(R, -)$. A functor $\mathscr{F} : \mathscr{C} \to \mathsf{Set}$ is *representable* if it is naturally isomorphic to the functor $\boldsymbol{h}_{\mathcal{R}}$ for some $\mathcal{R}$.

Since we defined the set-valued functor $\boldsymbol{D}_{\bar{\rho}}$ in the previous section, it is a natural question to ask whether this functor is representable. If it is representable, then there exists some ring $\mathcal{R}_{\bar{\rho}}$ such that for every $R \in \mathscr{C}$:

$$\boldsymbol{D}_{\bar{\rho}}(R) = \mathrm{Mor}_{\mathscr{C}}(\mathcal{R}_{\bar{\rho}}, R)$$

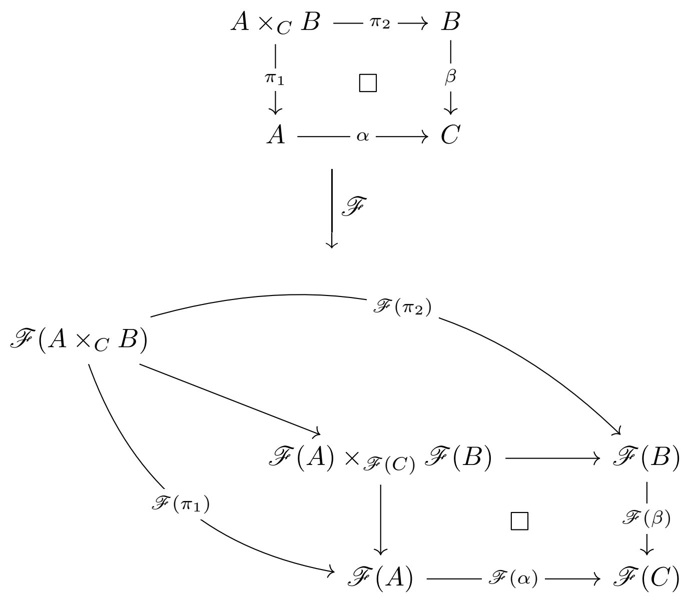
Suppose $R = \mathcal{R}_{\bar{\rho}}$, and let the identity map on $\mathcal{R}_{\bar{\rho}}$ correspond to a deformation $\boldsymbol{\rho} : \Pi \to \mathrm{GL}_n(\mathcal{R}_{\bar{\rho}})$.

Since this is a natural transformation of functors, any deformation ρ of $\bar{\rho}$ to a ring R must correspond to a morphism $\varphi : \mathcal{R}_{\bar{\rho}} \to R$, where $\rho = \varphi \circ \boldsymbol{\rho}$. In other words, every deformation of $\bar{\rho}$ comes from the composition of a ring morphism $\mathcal{R} \to R$ and the deformation $\boldsymbol{\rho}$.

Since every deformation can be obtained from the deformation $\boldsymbol{\rho}$, we call this the *Universal Deformation*, additionally we call $\mathcal{R}_{\bar{\rho}}$ the *Universal Deformation Ring* of $\bar{\rho}$.

The main result of section 3 will be to show that a Universal Deformation indeed exists. In this subsection we show some necessary conditions for a general set-valued functor on the category $\mathscr{C}$ to be representable.

Suppose $\mathscr{F}$ is a functor and let $\alpha : A \to C$ and $\beta : B \to C$ be morphisms in an arbitrary category $\mathcal{C}$. If the fibre product $A \times_C B$ exists, there there is a natural map from $\mathscr{F}(A \times_C B) \to \mathscr{F}(A) \times_{\mathscr{F}(C)} \mathscr{F}(B)$ by the universal property of fibre products in Set, as seen in the below diagram.



Definition. If this map is a bijection and $\mathscr{F}(A \times_C B) = \mathscr{F}(A) \times_{\mathscr{F}(C)} \mathscr{F}(B)$ for every A, B, C, then we say that $\mathscr{F}$ satisfies the *Mayer Vietoris Property.*

Proposition 8. If $\mathscr{F}$ is a representable functor, then it satisfies the Mayer-Vietoris Property.

Proof. If $\mathscr{F}$ is representable, then there exists an object $D \in \mathscr{C}$ such that $\mathscr{F} = \mathrm{Mor}(D, -)$

Then it suffices to prove that:

$$\mathrm{Mor}(D, A \times_C B) = \mathrm{Mor}(D, A) \times_{\mathrm{Mor}(D,C)} \mathrm{Mor}(D, B)$$

However, this is tautological with the universal property of the fibre product. An object in $\mathrm{Mor}(D, A) \times_{\mathrm{Mor}(D,C)} \mathrm{Mor}(D, B)$ is a pair of morphisms from D to A and B that agree on C, but by the universal property of fibre products these maps must uniquely factor through $A \times_C B$. Thus the two sets are equal. $\square$

We have proved that the Mayer Vietoris Property is a necessary condition for a functor to be representable, but it is not very useful in the category $\mathscr{C}$. This is because fibre products need not exist because the fibre product of Noetherian Rings need not be Noetherian.

Consider the map $k[[X, Y]] \to k[[X]]$ given by $Y \mapsto 0$ and the inclusion $k \hookrightarrow k[[X]]$. These are all objects and maps in the category $\mathscr{C}$, however their fibre product is the ring $k + k[[X, Y]]Y$, which is not Noetherian because the ideal $I = (XY, X^2Y, X^3Y, \cdots) \subseteq k + k[[X, Y]]Y$ is not finitely generated. Thus the fibre product is not in the category $\mathscr{C}$.

However, hope is not lost, as it turns out fibre products exist in $\mathscr{C}^0$:

Proposition 9. Fibre products exist in the category $\mathscr{C}^0_\Lambda$.

Proof. Suppose $\alpha : A \to C$, $\beta : B \to C$ be morphisms of objects in $\mathscr{C}^0_\Lambda$. We wish to show that the ring $D := A \times_C B$ is local Artinian with residue field k. Note D is the subring of $A \times B$ consisting of elements (a, b) where $\alpha(a) = \beta(b)$. Let π_A, π_B, π_C be the projection maps from D to A, B, C respectively.

Then consider the ideal $\mathcal{I} = \pi_A^{-1}(\mathfrak{m}_A) = \pi_B^{-1}(\mathfrak{m}_B) = \pi_C^{-1}(\mathfrak{m}_C)$. This is the preimage of a prime ideal and is thus prime. On the other hand, any $x \in D \setminus \mathcal{I}$ will map to units x_A, x_B under the projections π_A, π_B and they agree upon mapping to C. Then the pair (x_A^{-1}, x_B^{-1}) also agrees upon mapping to C, and thus defines an element in D which is inverse to x. So any element in $D \setminus \mathcal{I}$ is a unit, and thus this ideal $\mathcal{I}$ is indeed maximal, and D is local.

The map $D \to A \to A/\mathfrak{m}_A \cong k$ is surjective and has kernel containing $\mathcal{I}$, but since $\mathcal{I}$ is maximal and the map is non-zero the kernel is equal to $\mathcal{I}$. This means that $D/\mathcal{I} \cong k$ and so D has residue field k.

To see that D is Artinian, we show that it has finite length as a Λ-module. Since A and B are Artinian, they have finite length as Λ-modules. Then $A \times B$ is a finite length Λ-module which implies $D \subseteq A \times B$

also has finite length as a Λ-module. Thus D is an Artinian Λ-Algebra, and we conclude that D is in $\mathscr{C}^0_\Lambda$. □

Because fibre products exist in $\mathscr{C}^0$, it makes a lot more sense to work in this category instead, but in order to do this we need a result that tells us whether $\mathscr{F}$ is representable on $\mathscr{C}$ by only looking at $\mathscr{C}^0$. To do this we define the concept of *pro-representability*:

Definition. Let $\mathscr{F}$ be a functor on $\mathscr{C}^0$, we say that $\mathscr{F}$ is *pro-representable* if there exists an object $\mathcal{R}$ in the larger category $\mathscr{C}$ such that for $S \in \mathscr{C}^0$:

$$\mathscr{F}(S) = \mathrm{Mor}_{\mathscr{C}}(\mathcal{R}, S)$$

In general pro-representability on $\mathscr{C}^0$ does not imply representability on $\mathscr{C}$, but if our functor is continuous then they are in fact equivalent statements:

Lemma 10. Suppose $\mathscr{F}$ is a continuous functor on $\mathscr{C}$. Then $\mathscr{F}$ is pro-representable on $\mathscr{C}^0$ if and only if $\mathscr{F}$ is representable on $\mathscr{C}$.

Proof. The reverse direction is clear, so it suffices to only show that a pro-representable functor is also representable.

Suppose $\mathscr{F}$ is pro-representable and represented by $\mathcal{R} \in \mathscr{C}$, and R is an object in $\mathscr{C}$. Since $\mathscr{F}$ is continuous we know that:

$$\mathscr{F}(R) = \varprojlim \mathscr{F}(R/\mathfrak{m}^s) = \varprojlim \mathrm{Mor}(\mathcal{R}, R/\mathfrak{m}^s)$$

But by the universal property of inverse limits, the maps $\mathcal{R} \to R/\mathfrak{m}^s$ must all factor uniquely through a map $\mathcal{R} \to R$. This means that any element in the set $\varprojlim \mathrm{Mor}(\mathcal{R}, R/\mathfrak{m}^s)$ corresponds uniquely to a morphism $\mathrm{Mor}(\mathcal{R}, R)$ and vice versa, thus $\mathscr{F}(R) = \mathrm{Mor}(\mathcal{R}, R)$ and $\mathscr{F}$ is representable. □

2.5 Some Galois Theory

Given an infinite field extension L/K, the Galois group $\mathrm{Gal}(L/K)$ is defined to be the inverse limit $\varprojlim \mathrm{Gal}(L'/K)$ as L' ranges all finite subextensions $L/L'/K$. The Galois group is equipped with the profinite topology.

In particular, given a field K, we write $G_K = \mathrm{Gal}(\bar{K}/K)$ for the *absolute Galois group* of K.

Moreover, if K is a number field and S is a set of primes in K including the primes at infinity, then let K_S denote the maximal extension of K that is unramified outside of the set of primes S. We write $G_{K,S} = \mathrm{Gal}(K_S/K)$.

Proposition 11. Let K be a finite extension of $\mathbb{Q}_p$. Then G_K satisfies the $\mathbf{\Phi}_p$ condition.

Proof. By a theorem in Local Fields, there are only finitely many extensions of K of any given degree. So in particular there are only finitely many extensions L/K of degree p.

For any non-trivial continuous homomorphism $\phi : G_K \to \mathbb{Z}/p\mathbb{Z}$, $\mathrm{Ker}\,\phi$ has index p, which means that field fixed by $\mathrm{Ker}\,\phi$ has degree p over K. Given a fixed $\mathrm{Ker}\,\phi$, there are exactly $p-1$ nontrivial homomorphisms from $G_K/\mathrm{Ker}\,\phi \to \mathbb{Z}/p\mathbb{Z}$, so each degree p extension of K corresponds to exactly $p-1$ nontrivial homomorphisms. Since there are only finitely many degree p extensions, this proves that there are only finitely many continuous homomorphisms $G_K \to \mathbb{Z}/p\mathbb{Z}$ and thus G_K satisfies $\mathbf{\Phi}_p$. □

Proposition 12. Suppose the set S contains all primes lying above p. Then $G_{K,S}$ satisfies the $\mathbf{\Phi}_p$ condition. [Tia14]

Proof. This follows from the Hermite-Minkowski Theorem, which states that there are only finitely many number fields with bounded discriminant.

Suppose L/K is a degree p extension that is unramfied outside S. Then for $q \notin S$, L_q/K_q is unramified and thus has discriminant $d_{L_q/K_q} = 1$.

If $q \in S$, then L_q/K_q is a field extension degree p. There are only finitely many local field extensions of a fixed degree, and let d_q be the maximal discriminant out of all extensions of degree p.

Let $d = \prod_{q \in S} d_q$. Then note that by the identity:

$$d_{L/K} = \prod_q d_{L_q/K_q}$$

It follows that if L/K is a degree p extension that is unramified outside of S, it must have discriminant less than d. Thus by the Hermite-Minkowski theorem, there are only finitely many such extensions.

Thus we have shown that there are finitely many extensions of K that are of degree p and unramified outside of S, so by the same argument as the previous proof, there are only finitely many continuous homomorphisms $G_{K,S} \to \mathbb{Z}/p\mathbb{Z}$ and thus condition $\mathbf{\Phi}_p$ is satisfied. □

While most of this essay will focus on when Π is an arbitrary profinite group that satisfies the Φ_p condition, the above two propositions show that all discussion regarding general Π will apply when we consider the above Galois groups

2.6 Galois Cohomology

We define the notion of a group cohomology, and a Galois cohomology is simply the group cohomology of a Galois group. Let G be a group, and M a G-module.

Let M^G denote the G-invariant elements of M, i.e. $M^G = \{m \in M | \forall g \in G : gm = m\}$.

We can think of the map $M \mapsto M^G$ as a functor $\mathsf{Mod}_G \to \mathsf{AbGrp}$ from G-modules to abelian groups. This functor is isomorphic to the functor $\mathrm{Hom}_G(\mathbb{Z}, -)$. Where $\mathbb{Z}$ is given the trivial G module structure. Any G-module homomorphism $\mathbb{Z} \to M$ is uniquely determined by the image of 1 and since $g1 = 1$ is G-invariant it follows that the image of 1 must also be G-invariant. Giving $\mathrm{Hom}_G(\mathbb{Z}, M)$ the structure of a group by pointwise addition, we find that $M^G \cong \mathrm{Hom}_G(\mathbb{Z}, M)$

Since the Hom functor is left exact, it follows that $(-)^G$ is also a left exact functor. The group cohomology $H^*(G, M)$ measures the failure of this functor to be right exact.

Definition (Group Cohomology)**.** We pick an injective resolution of M:

$$0 \to M \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \cdots$$

And upon applying the functor $(-)^G$ we obtain a chain complex which is no longer neccesarily exact:

$$0 \to (I^0)^G \xrightarrow{d^0} (I^1)^G \xrightarrow{d^1} (I^2)^G \xrightarrow{d^2} \cdots$$

As with usual cohomology, we define the cohomology groups to be the kernel of the differential maps quotiented by the image:

$$H^i(G, M) := \frac{\mathrm{Ker}\, d^i}{\mathrm{Im}\, d^{i-1}}$$

Noting that the functors $(-)^G$ and $\mathrm{Hom}_G(\mathbb{Z}, -)$ are isomorphic, one can think of the group cohomology as the Ext cohomology over G-modules:

$$H^*(G, M) = \mathrm{Ext}^*_G(\mathbb{Z}, M)$$

2.6.1 Explicit Description of Cochains, Cocycles, Coboundaries

From properties of Ext we can deduce that for any G-module M, we have that $H^0(G, M) = M^G$.

For higher cohomologies, we can also explicitly describe the cochains, cocycles, and coboundaries for the rth cohomology. This description also follows from properties of Ext and is taken from [Mil20].

The cochains $C^r(G, M)$ correspond to the set:

$$C^r(G, M) = \{\text{set maps } G^r \to M\}$$

We define the differential map $d^r : C^r(G, M) \to C^{r+1}(G, M)$. Suppose $\phi : G^r \to M$ is an element of $C^r(G, M)$. Then we have that:

$$\begin{aligned}(d^r\phi)(g_1, g_2, \cdots, g_{r+1}) =& g_1\phi(g_2, \cdots, g_{r+1}) \\ &+ \sum_{j=1}^{r} (-1)^j \phi(g_1, \cdots, g_j g_{j+1}, \cdots, g_{r+1}) \\ &+ (-1)^{r+1}\phi(g_1, \cdots, g_r)\end{aligned}$$

Where an element of G written outside of ϕ is to be interpreted as the group action of G on M, and the sum in the middle essentially concatenates consecutive terms.

Define the set of *cocycles* to be $Z^r(G, M) = \operatorname{Ker} d^r$ and the set of *coboundaries* $B^r(G, M) = \operatorname{Im} d^{r-1}$. Then we have that the group cohomology is in fact isomorphic to:

$$H^r(G, M) = \frac{\operatorname{Ker} d^r}{\operatorname{Im} d^{r-1}} = \frac{Z^r(G, M)}{B^r(G, M)}$$

In particular we write down the first and second cocyles and coboundaries explicitly, for $r = 1$ we have the sets:

$$\begin{aligned}Z^1(G, M) &= \{\phi : G \to M | \phi(gh) = \phi(g) + g\phi(h)\} \\ B^1(G, M) &= \{\phi : g \mapsto gm - m | m \in M\}\end{aligned}$$

For $r = 2$ we have that the cocycles $Z^2(G, M)$ are given by cochains $\phi : G^2 \to M$ such that:

$$g_1\phi(g_2, g_3) = \phi(g_1 g_2, g_3) - \phi(g_1, g_2 g_3) + \phi(g_1, g_2)$$

And the coboundaries $B^2(G, M)$ are given by maps that look like:

$$(g_1, g_2) \mapsto g_1\varphi(g_2) - \varphi(g_1 g_2) + \varphi(g_1)$$

For any arbitrary map $\varphi \in C^1(G, M)$.

2.7 The Tangent Space

Suppose $R \in \mathscr{C}_\Lambda$ is a Λ-algebra. We define the *Zariski Cotangent Space* to be:

$$t_R^* = \mathfrak{m}_R/(\mathfrak{m}_R^2, \mathfrak{m}_\Lambda)$$

where $(\mathfrak{m}_R^2, \mathfrak{m}_\Lambda)$ is the ideal generated by $\mathfrak{m}_R^2$ and by the image of $\mathfrak{m}_\Lambda$ in R. Noting that t_R^* has a $\Lambda/\mathfrak{m}_\Lambda \cong k$-module structure, the Zariski cotangent space is in fact a k-vector space. We define the *Zariski tangent space* to be the dual of the cotangent space:

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

Notice a morphism $A \to B$ in the category $\mathscr{C}_\Lambda$ induces a map of tangent spaces $f^* : t_B \to t_A$. Moreover, if f is surjective then it induces a surjection between the maximal ideals of A and B, and thus a surjection $f_* : t_A^* \twoheadrightarrow t_B^*$. This in turn implies that the dual map f^* is injective.

We define the ring of dual numbers to be $k[\varepsilon] \cong k[X]/(X^2)$.

Lemma 13. For a ring $R \in \mathscr{C}_\Lambda$, there is a natural bijection of sets:

$$t_R \cong \mathrm{Hom}_\Lambda(R, k[\varepsilon])$$

Where Hom_Λ refers to a homomorphism in the category $\mathscr{C}_\Lambda$.

Proof. Suppose $\phi \in \mathrm{Hom}_\Lambda(R, k[\varepsilon])$, then for $r \in R$, we have $\phi(r) = \bar{r} + \varphi(r)\varepsilon$. Where $\bar{r} \in k$ is the reduction of r modulo $\mathfrak{m}$ and $\varphi : R \to k$ is a map of Λ-modules since it should commute with addition and scalar multiplication.

By considering R as a Λ-module, we can canonically write $R \cong k \oplus \mathfrak{m}_R$ from lemma 3. But ϕ sends k to itself, so φ is uniquely determined by where it sends $\mathfrak{m}_R$.

Since $\phi(m) = \varphi(m)\varepsilon$ for any $m \in \mathfrak{m}_R$, it follows from $\varepsilon^2 = 0$ that $\phi(\mathfrak{m}_R^2) = 0$, and so $\varphi(\mathfrak{m}_R^2) = 0$. Additionally, since R is a Λ algebra and the map $\Lambda \to k[\varepsilon]$ sends $\mathfrak{m}_\Lambda$ to zero it follows that $\varphi(\mathfrak{m}_\Lambda) = 0$ as well.

Thus the φ factors through the quotient by $(\mathfrak{m}_R^2, \mathfrak{m}_\Lambda)$ and gives a map $\mathfrak{m}_R/(\mathfrak{m}_R^2, \mathfrak{m}_\Lambda) \to k$. This is a map of $\Lambda/\mathfrak{m}_\Lambda$-modules, which are k vector spaces. Conversely, any such map determines a unique φ, and thus the sets are in bijection. □

Corollary 14. If $\mathscr{F}$ is a representable functor represented by the ring R, then the tangent space of the ring representing $\mathscr{F}$, t_R is in bijection with the $\mathscr{F}(k[\varepsilon]) = \mathrm{Hom}_\Lambda(R, k[\varepsilon])$.

We have shown that $\mathscr{F}(k[\varepsilon])$ has a k-vector space structure if $\mathscr{F}$ is representable. But we can in fact give $\mathscr{F}(k[\varepsilon])$ a vector space structure as long as it satisfies a special case of the Mayer Vietoris property:

Proposition 15. Consider the fibre product $k[\varepsilon] \times_k k[\varepsilon]$ given by the maps $k[\varepsilon] \to k$ which send ε to zero. Suppose the natural map $\mathscr{F}(k[\varepsilon] \times_{\mathscr{F}(k)} k[\varepsilon]) \to \mathscr{F}(k[\varepsilon]) \times_{\mathscr{F}(k)} \mathscr{F}(k[\varepsilon])$ is a bijection, and that $\mathscr{F}(k)$ contains a single element. Then there is a natural k-vector space structure.

Proof. The key to this proof is to first define a notion of addition and scalar multiplication on $k[\varepsilon]$, and then use the functoriality of $\mathscr{F}$ to define addition and scalar multiplication on $\mathscr{F}(k[\varepsilon])$. Note that since $\mathscr{F}(k)$ consists of a single element, fibred products over $\mathscr{F}(k)$ is the same as the direct product. Thus:

$$\mathscr{F}(k[\varepsilon]) \times_{\mathscr{F}(k)} \mathscr{F}(k[\varepsilon]) \cong \mathscr{F}(k[\varepsilon]) \times \mathscr{F}(k[\varepsilon])$$

Elements of $k[\varepsilon] \times_k k[\varepsilon]$ are pairs of elements $(x_1 + y_1\varepsilon, x_2 + y_2\varepsilon)$ such that they agree upon restricting to k, so we must have that $x_1 = x_2$. Consider the map $\mathfrak{p} : k[\varepsilon] \times_k k[\varepsilon] \to k[\varepsilon]$ given by:

$$\mathfrak{p} : (x + y_1\varepsilon, x + y_2\varepsilon) \mapsto x + (y_1 + y_2)\varepsilon$$

One can check that this is a well-defined Λ-algebra morphism.

Since we assumed that there is a bijection $\mathscr{F}(k[\varepsilon]) \times \mathscr{F}(k[\varepsilon]) \cong \mathscr{F}(k[\varepsilon] \times_k k[\varepsilon])$, we identify the two sets and apply $\mathscr{F}(\mathfrak{p})$ in order to define addition on the set $\mathscr{F}(k[\varepsilon])$:

$$(a, b) \in \mathscr{F}(k[\varepsilon]) \times_k \mathscr{F}(k[\varepsilon]) \cong \mathscr{F}(k[\varepsilon] \times_k k[\varepsilon]) \xrightarrow{\mathscr{F}(\mathfrak{p})} \mathscr{F}(k[\varepsilon]) \ni a + b$$

To define scalar multiplication we note that the map $\mathfrak{t}_\lambda : k[\varepsilon] \to k[\varepsilon]$ given by:

$$x + y\varepsilon \mapsto x + \lambda y\varepsilon$$

is also a morphism of Λ-algebras for any $\lambda \in k$. Then we simply can define multiplication by a scalar in $\mathscr{F}(k[\varepsilon])$ to be the application of the functor $\mathscr{F}(\mathfrak{t}_\lambda)$. In other words, for $a \in \mathscr{F}(k[\varepsilon])$:

$$\lambda \cdot a = \mathscr{F}(\mathfrak{t}_\lambda)(a)$$

We now check that addition and scalar multiplication distributes as they should in a vector space, but again by functoriality it simply suffices to check this on $k[\varepsilon]$.

For example $x + y_1\varepsilon, x + y_2\varepsilon \in k[\varepsilon]$, then:

$$\begin{aligned} \mathfrak{t}_\lambda(\mathfrak{p}(x + y_1\varepsilon, x + y_2\varepsilon)) &= \mathfrak{t}_\lambda(x + (y_1 + y_2)\varepsilon) \\ &= x + \lambda(y_1 + y_2)\varepsilon \\ &= \mathfrak{p}(x + \lambda y_1\varepsilon, x + \lambda y_2\varepsilon) \\ &= \mathfrak{p}(\mathfrak{t}_\lambda(x + y_1\varepsilon), \mathfrak{t}_\lambda(x + y_2\varepsilon)) \end{aligned}$$

Thus scalar multiplication distributes over the addition of vectors. The other vector space axioms can be checked similarly. Thus we have given $\mathscr{F}(k[\varepsilon])$ a vector space structure.

□

3 Universal Deformation Rings

3.1 Statement of Main result

Suppose $\rho : \Pi \to \mathrm{GL}_n(A)$ for $A \in \mathscr{C}_\Lambda$ is a lift of the representation $\bar{\rho}$. Note that A^n can be given the stricture of a Π-module through the action ρ. i.e. $g * M = \rho(g)M$ for $M \in A^n$.

We now define $C_A(\rho)$ to be the set of Π-module endomorphisms of A^n. Clearly any such endomorphism is also a linear map $A^n \to A^n$, and thus an element of $M_n(A)$. However this linear map $P \in M_n(A)$ must also commute with the action of Π in order for it to be Π-module homomorphism. Thus:

Definition.

$$C_A(\rho) := \mathrm{Hom}_\Pi(A^n, A^n) = \{P \in M_n(A) | \forall g \in \Pi : P\rho(g) = \rho(g)P\}$$

This is the set of all elements of $M_n(A)$ which commute with $\rho(g)$ for all g.

In particular, we are interested in the case where $C_k(\bar{\rho}) = k$. In other words, this means that the only matrices that commute with $\bar{\rho}$ are the scalar matrices. This may seem like an arbitrary condition, but turns out *absolutely irreducible* representations satisfy this property.

Definition (Absolutely irreducible representations)**.** A representation $\rho : G \to \mathrm{GL}_n(k)$ is *irreducible* if it has no G-invariant subspace.

It is *absolutely irreducible* if for every field extension k'/k, the representation $\rho \otimes k' : G \to \mathrm{GL}_n(k')$ is irreducible.

Proposition 16. If $\bar{\rho} : \Pi \to \mathrm{GL}_n(k)$ is absolutely irreducible representation, then $C_k(\bar{\rho}) = k$.

Proof. Let $\bar{k}$ be the algebraic closure of k and consider the representation $\bar{\rho} \otimes \bar{k} : \Pi \to \mathrm{GL}_n(\bar{k})$. By our assumption, this is an irreducible representation.

By Schur's lemma from representation theory we know that the only Π-endomorphisms of an irreducible representation are the scaling maps. So in other words we know that $C_{\bar{k}}(\bar{\rho} \otimes \bar{k}) = \bar{k}$.

However, any element of $C_k(\bar{\rho})$ will extend to a Π-endomorphism over $\bar{k}$, i.e. an element in $C_{\bar{k}}(\bar{\rho} \otimes \bar{k}) = \bar{k}$. Thus elements in $C_k(\bar{\rho})$ can only be scalar matrices. Since all scalar matrices commute with $\bar{\rho}$, we conclude that $C_k(\bar{\rho}) = k$. □

We are now ready to state the main theorem of this section:

Theorem 17 (Existence of Universal Deformation Ring)**.** Suppose that Π is a profinite group satisfying condition $\mathbf{\Phi}_p$ and $\bar{\rho} : \Pi \to \mathrm{GL}_n(k)$ is a representation such that $C_k(\bar{\rho}) = k$.

Then there exists a ring $\mathcal{R} = \mathcal{R}(\Pi, k, \bar{\rho})$ in $\mathscr{C}_\Lambda$ and a deformation $\boldsymbol{\rho} : \Pi \to \mathrm{GL}_n(\mathcal{R})$ of $\bar{\rho}$ such that every other deformation $\rho : \Pi \to A$ is given uniquely by a morphism $\mathcal{R} \to A$.

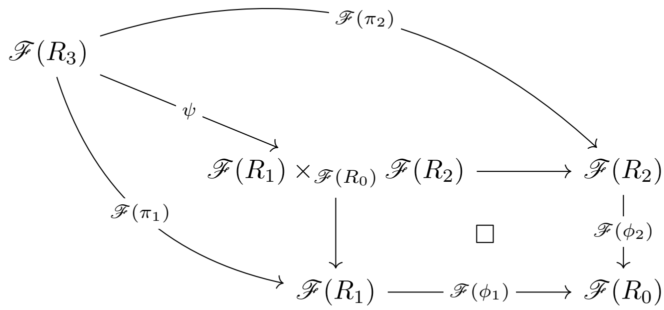
The rest of this section will be working towards a proof of this result.

3.2 Schlessinger's Criteria

The Schlessinger's Criteria are a series of conditions that specify when a functor $\mathscr{F} : \mathscr{C}_\Lambda^0 \to \mathsf{Set}$ is pro-representable. We first define the notion of a small homomorphism:

Definition. A homomorphism $\phi : R \to S$ is *small* if it is surjective and $\mathrm{Ker}(\phi)$ is principal and annihilated by $\mathfrak{m}_R$.

Now suppose we have rings $R_0, R_1, R_2 \in \mathscr{C}_\Lambda^0$, and morphisms $\phi_1 : R_1 \to R_0; \phi_2 : R_2 \to R_0$. Then let $R_3 := R_1 \times_{R_0} R_2$. For a functor $\mathscr{F}$ there is a natural map $\mathscr{F}(R_3) \to \mathscr{F}(R_1) \times_{\mathscr{F}(R_0)} \mathscr{F}(R_2)$, from the universal property of fibre product, illustrated in the below diagram. We label this map ψ.



We now state the Schlessinger Criteria:

Definition. The following are the Schlessinger Criteria:

H1. If the map $R_2 \to R_0$ is small, then ψ is surjective.

H2. If $R_0 = k$ and $R_2 = k[\varepsilon]$, then ψ is bijective.

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

H4. If $R_1 = R_2$, and $\phi_1 = \phi_2$ are small maps from R_1, R_2 to R_0, then ψ is bijective.

Note that the statement of **H3** makes sense if condition **H2** is true, since the statement **H2** implies that the assumptions in proposition 15 are true, and thus $\mathscr{F}(k[\varepsilon])$ can indeed be given a vector space structure.

It turns out these 4 criteria are sufficient to ensure that $\mathscr{F}$ is pro-representable:

Theorem 18 (Schlessinger)**.** Let $\mathscr{F}$ be functor on $\mathscr{C}_\Lambda^0$ such that $\mathscr{F}(k)$ has 1 element. Then if $\mathscr{F}$ satisfies the Schlessinger Criteria **H1-H4** then $\mathscr{F}$ is pro-representable.

The proof of this theorem is omitted and but can be found at [Sch68]. This theorem implies that we simply need to show that the functor $\boldsymbol{D}_\Lambda$ satisfies the 4 Schlessinger Criteria in order to prove Theorem 17.

3.3 Universal Deformation Rings Exist!

We now prove the main result of this section: that a universal deformation ring indeed exists. We show that $\boldsymbol{D}_\Lambda$ is representable by showing that it satisfies the 4 Schlessinger Criteria. This entire subsection will closely follow the proof that was given in [Gou08]

As with the previous section, we let $R_0, R_1, R_2 \in \mathscr{C}_\Lambda^0$ and $R_3 = R_1 \times_{R_0} R_2$. For each i, we define $E_i = E(R_i)$ to be the set of lifts (before taking equivalence classes) of $\bar{\rho}$ to R_i. Then we can write:

$$\boldsymbol{D}_\Lambda(R_i) = E_i/\Gamma_n(R_i)$$

In this case, our map ψ can be written in the form:

$$\psi : E_3/\Gamma_n(R_3) \to E_1/\Gamma_n(R_1) \times_{E_0/\Gamma_n(R_0)} E_2/\Gamma_n(R_2)$$

We define a set:

Definition. Suppose $\phi_i \in E_i$ be a lift of $\bar{\rho}$ to R_i. Then we define:

$$G_i(\phi_i) = \{M \in \Gamma_n(R_i) | M \text{ commutes with the image of } \phi_i\}$$

This is very similar to the definition $C_{R_i}(\phi_i)$, but we only take matrices in $\Gamma_n(R_i)$ rather than all of $M_n(R_i)$, so $C_{R_i}(\phi_i)$ is a ring while $G_i(\phi_i)$ is a group.

We now prove a series of lemmas:

Lemma 19. $\boldsymbol{D}_\Lambda$ satisfies property **H1**: *If the map $R_2 \to R_0$ is small, then ψ is surjective.*

Proof. An element of $\boldsymbol{D}_\Lambda(R_1) \times_{\boldsymbol{D}_\Lambda(R_0)} \boldsymbol{D}_\Lambda(R_2)$ is simply a pair of deformations $([\phi_1], [\phi_2])$ that agree upon mapping to R_0. To show that ψ is surjective, we need to find an element $[\phi] \in \boldsymbol{D}_\Lambda(R_3)$ that restricts to $[\phi_1]$ and $[\phi_2]$.

Since $[\phi_1]$ and $[\phi_2]$ agree upon mapping to R_0, there is some $\overline{M} \in \Gamma_n(R_0)$ such that conjugating the image of ϕ_2 by $\overline{M}$ gives the image of ϕ_1. However, since small maps are surjective and $R_2 \to R_0$ is a small map, this implies that there is a lift $M \in \Gamma_n(R_2)$ of $\overline{M}$ such that $M^{-1}\phi_2 M$ and ϕ_1 map to the same element in E_0.

This in turn implies that ϕ_1 and $M^{-1}\phi_2 M$ specify an element $\phi_3 \in E_3$, and $[\phi_3]$ maps to the pair $([\phi_1], [\phi_2])$, so this shows that ψ is indeed surjective.

□

It should be noted that the only property of $R_2 \to R_1$ being small that was used was the fact that the map is surjective. We now prove a lemma that gives us a sufficient condition for ψ to be injective:

Lemma 20. Let $\phi_2 \in E_2$ and $\phi_0 \in E_0$ be its image after composing with $R_2 \to R_0$. Suppose the map $G_2(\phi_2) \to G_0(\phi_0)$ is surjective for all $\phi_2 \in E_2$. Then the map ψ is injective.

Where the map $G_2(\phi_2) \to G_0(\phi_0)$ stated in the lemma is simply the restriction of the $\Gamma_n(R_2) \to \Gamma_n(R_0)$ map.

Proof. Suppose $[\phi], [\varphi] \in \boldsymbol{D}_\Lambda(R_3)$ are deformations of $\bar{\rho}$ such that they have the same image under $\psi : \boldsymbol{D}_\Lambda(R_3) \to \boldsymbol{D}_\Lambda(R_1) \times_{\boldsymbol{D}_\Lambda(R_0)} \boldsymbol{D}_\Lambda(R_2)$. Suppose $\phi_i, \varphi_i \in E_i$ are the lifts to R_i that are induced by ϕ, φ. Then $[\phi], [\varphi]$ having the same image under ψ implies that ϕ_i is strictly equivalent to φ_i for $i = 1, 2$.

Let $M_i \in \Gamma_n(R_i)$ be the matrices such that $\phi_i = M_i^{-1}\varphi_i M_i$ for $i = 1, 2$. Since these maps should agree upon mapping down to E_0, we have:

$$\phi_0 = \overline{M_1}^{-1}\varphi_0\overline{M_1} = \overline{M_2}^{-1}\varphi_0\overline{M_2}$$

where $\overline{M_i}$ is the image of M_i upon mapping to $\Gamma_n(R_0)$. Note that the above equality implies $\overline{M_2 M_1}^{-1}\varphi_0 = \varphi_0\overline{M_2 M_1}^{-1}$.

This means $\overline{M_2 M_1}^{-1}$ commutes with the image of φ_0, so $\overline{M_2 M_1}^{-1} \in G_0(\varphi_0)$.

Now we use the fact that the map $G_2(\varphi_2) \to G_0(\varphi_0)$ is surjective to find some $N \in G_2(\varphi_2)$ such that N maps to $\overline{M_2 M_1}^{-1}$. Let $N_2 = N^{-1}M_2$, then note that since N commutes with φ_2 we have:

$$\phi_2 = M_2^{-1}\varphi_2 M_2 = M_2^{-1}N\varphi_2 N^{-1}M_2 = N_2^{-1}\varphi_2 N_2$$

Moreover N_2 reduces to $\overline{M_1}$ upon mapping to $\Gamma_n(R_0)$. This means $(M_1, N_2) \in \Gamma_n(R_1) \times \Gamma_n(R_2)$ in fact specifies an element of $\Gamma_n(R_3)$. Call this element $M \in \Gamma_n(R_3)$. Then this element in fact satisfies $\phi = M^{-1}\varphi M$. This implies that $[\phi] = [\varphi]$, and so the map ψ is indeed injective.

□

We now prove that **H2** is satisfied, but this is a simple corollary of Lemma 20.

Lemma 21. $\boldsymbol{D}_\Lambda$ satisfies property **H2**: *If $R_0 = k$ and $R_2 = k[\varepsilon]$, then ψ is bijective.*

Proof. Note that the map $k[\varepsilon] \to k$ is small, so by the **H1** we know that ψ is surjective.

On the other hand, in order to show that ψ is injective, from Lemma 20 it suffices to show that the map $G_2(\phi_2) \to G_0(\phi_0)$ is surjective for all $\phi_2 \in E_2$.

Since we know that $R_0 = k$, by definition $\Gamma_n(R_0)$ must contain only the identity matrix. Since $G_0(\phi_0)$ is a subgroup of $\Gamma_n(R_0)$ it must also be the group with 1 element. Thus any map $G_2(\phi_2) \to G_0(\phi_0) \cong \mathbf{1}$ must be surjective. This concludes the proof.

□

Now we move onto **H3**. We first prove a lemma about $\Gamma_n(k[\varepsilon])$.

Lemma 22. The group $\Gamma_n(k[\varepsilon])$ is finite, and p-elementary abelian (every non-identity element has order p, or the group has exponent p).

A direct corollary of this lemma is that by the structure theorem on finitely generated abelian groups, $\Gamma_n(k[\varepsilon])$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^N$ for some integer N.

Proof. If $M \in \Gamma_n(k[\varepsilon])$ it must reduce to the identity matrix after reducing to $\mathrm{GL}_n(k)$, then as a matrix it must be of the form $M = I_n + N\varepsilon$, where $N \in M_n(k)$.

Note that each entry in the matrix N must be in k which is a finite field of characteristic p. This means that there are precisely $|k|^{n^2}$ possible matrices N, and this number is also the size of $\Gamma_n(k[\varepsilon])$. So we have shown that $\Gamma_n(k[\varepsilon])$ is a finite p-group.

To show that the group is abelian and has exponent p, we use the fact that $\varepsilon^2 = 0$. Suppose $I + N_1\varepsilon, I + N_2\varepsilon \in \Gamma_n(k[\varepsilon])$, then we have:

$$(I + N_1\varepsilon)(I + N_2\varepsilon) = I + N_1\varepsilon + N_2\varepsilon = (I + N_2\varepsilon)(I + N_1\varepsilon)$$

$$(I + N_1\varepsilon)^p = I + pN_1\varepsilon + \varepsilon^2(\cdots) = I$$

So $\Gamma_n(k[\varepsilon])$ is abelian, and every element has order dividing p, which means all non-identity elements have order exactly p. □

Equipped with this lemma, we prove the third Schlessinger Criteria. Note that the $\boldsymbol{\Phi}_p$ condition is used in the proof of **H3**.

Lemma 23. $\boldsymbol{D}_\Lambda$ satisfies property **H3**: *The vector space $t_{\boldsymbol{D}_\Lambda} = \boldsymbol{D}_\Lambda(k[\varepsilon])$ is finite dimensional.*

Proof. Define $\Pi_0 = \mathrm{Ker}(\bar{\rho} : \Pi \to \mathrm{GL}_n(k))$, and let $\rho : \Pi \to \mathrm{GL}_n(k[\varepsilon])$ be a lift. Then by definition $\rho(\Pi_0)$ must map to the identity upon composing with the projection $k[\varepsilon] \to k$, so $\rho(\Pi_0) \subseteq \Gamma_n(k[\varepsilon])$.

Now note that Π_0 is an open subgroup of Π and has index dividing $\mathrm{GL}_n(k)$ which is finite. So using condition $\boldsymbol{\Phi}_p$ we know that there are only a finite number of continuous homomorphisms $\Pi_0 \to \mathbb{Z}/p\mathbb{Z}$.

This in turn implies that there are only a finite number of homomorphisms $\Pi_0 \to \Gamma_n(k[\varepsilon]) \cong (\mathbb{Z}/p\mathbb{Z})^N$ by the previous lemma.

Fix a set $S = \{\pi_1, \cdots, \pi_r\}$ of coset representatives of Π/Π_0. Note that this set is finite because Π_0 has finite index. Then since $\mathrm{GL}_n(k[\varepsilon])$ is also a finite set, there are only finitely many set maps $S \to \mathrm{GL}_n(k[\varepsilon])$.

Note that any homomorphism $\Pi \to \mathrm{GL}_n(k[\varepsilon])$ is uniquely determined by where it sends Π_0 and the coset representatives S. (While not every pair of maps from Π_0 and S will give a well-defined group homomorphism, every homomorphism will uniquely come from such a pair of maps). Since there are a finite number of homomorphisms from Π_0 and a finite number of set maps from S, it follows that there can only be a finite number of lifts $\rho : \Pi \to \mathrm{GL}_n(k[\varepsilon])$.

Thus $\boldsymbol{D}_\Lambda(k[\varepsilon])$ is a quotient of the set of lifts which is still a finite set. This implies that it is indeed finite dimensional as a k-vector space.

□

The first 3 Schlessinger Criteria are true in general, but in order to prove **H4** we need to impose the additional condition on $\bar{\rho}$ that $C_k(\bar{\rho}) \cong k$, i.e. the matrices that commute with $\bar{\rho}$ are only the scalar matrices. We first prove two lemmas, the first is about small morphisms, and the second is about the $C_k(\bar{\rho}) \cong k$ condition.

Lemma 24. If $A, B \in \mathscr{C}^0_\Lambda$ and $A \to B$ is a surjective homomorphism, then the homomorphism can be factored into a chain

$$A = A_0 \to A_1 \to \cdots \to A_N = B$$

where each A_i is in $\mathscr{C}^0_\Lambda$ and each morphism $A_i \to A_{i+1}$ is a small map.

Proof. Recall that a homomorphism $R \to S$ is small if it is surjective and has a principal kernel that is annihilated by the maximal ideal of the domain $\mathfrak{m}_R$. Suppose $\phi : A \to B$ is a surjective map and let $\operatorname{Ker}\phi = I$.

Note that since A is Artinian and local, so its maximal ideal is the only prime ideal, so its maximal ideal $\mathfrak{m}_A$ an nilradical co-incide, and thus $\mathfrak{m}_A$ is nilpotent (the nilradical is nilpotent in Noetherian rings). Suppose $\mathfrak{m}_A^s = 0$, then consider the chain:

$$A = A/(0) = A/I\mathfrak{m}_A^s \to A/I\mathfrak{m}_A^{s-1} \to \cdots \to A/I\mathfrak{m}_A \to A/I = B$$

Where the map $A/I\mathfrak{m}_A^r \to A/I\mathfrak{m}_A^{r-1}$ is the natural quotient map with kernel $\mathfrak{m}_A^{r-1}$, which is annihilated by $\mathfrak{m}_A$, the maximal ideal of $A/I\mathfrak{m}_A^r$.

So now we can assume without loss of generality that $\operatorname{Ker}\phi = (a_1, a_2, \cdots, a_r)$ is annihilated by the maximal ideal $\mathfrak{m}_A$. Consider the sequence:

$$A \to A/(a_1) \to A/(a_1, a_2) \to \cdots \to A/(a_1, a_2, \cdots, a_r) = B$$

Each map has a kernel of the form (a_i) which is principal, and annihilated by the maximal ideal of the domain. This finishes the proof.

□

Lemma 25. Suppose $C_k(\bar{\rho}) = k$. Then for any deformation ρ of $\bar{\rho}$ to an Artinian ring $A \in \mathscr{C}^0_\Lambda$, we have $C_A(\rho) = A$. i.e. The only matrices in $C_A(\rho)$ are the scalar matrices.

In particular, this implies that the for any i, $G_i(\phi_i)$ consists of only scalar matrices in $\Gamma_n(R_i)$

Proof. Since the quotient map $A \to A/\mathfrak{m}_A \cong k$ is surjective, by lemma 24 we can split this into a chain of small morphisms and induct. i.e. It suffices to prove that if $\phi : A \to B$ is a small morphism and $C_B(\rho_B) = B$, then we must have $C_A(\rho_A) = A$.

Suppose $Q \in C_A(\rho_A)$. Then Q commutes with the image of ρ_A. Upon composing with the map $A \to B$ we find that the image of Q must also commute with the image of ρ_B, thus the image of Q must be in $C_B(\rho_B)$, i.e it must be a scalar.

Let $Q \mapsto b \in B$. However, since $A \to B$ is a surjection, there is a scalar $a \in A$ that maps to b. Then since Q can be written as $a + M'$ where M' maps to the 0 matrix. We know that $A \to B$ is a small morphism, so it has principal kernel, say (t). Then $M' = tM$ for some $M \in M_n(A)$.

So since $Q = a + tM$ commutes with ρ_A, for each $g \in \Pi$ we have $(a + tM)\rho_A(g) = \rho_A(g)(a + tM)$

This simplifies to $\rho_A(g)M = M\rho_A(g)$. By composing with the reduction $A \to k$, we know that the image of M must commute with $\bar{\rho}$ and thus is in $C_k(\bar{\rho}) = k$.

This implies that $M = r + M''$, where $r \in A$ is a scalar and M'' is a matrix with entries in the maximal ideal $\mathfrak{m}_A$. Noting that the ideal t is annihilated by the maximal ideal, we know that $tM'' = 0$ and thus $Q = a + t(r + M'') = a + tr$ is a scalar, as desired. □

Finally, we show that **H4** is true under our assumption:

Lemma 26. If $C_k(\rho) = k$, then **H4** is true: If $R_1 = R_2$, and $\phi_1 = \phi_2$ are small maps from R_1, R_2 to R_0, then ψ is bijective.

Proof. From **H1** we know that ψ is surjective, so it suffices to show injectivity. To do so, we wish to show that $G_2(\phi_2) \to G_1(\phi_1)$ is surjective so we can apply lemma 20.

From the previous lemma, we know that $G_i(\phi_i)$ consists of only scalars. In particular $G_i(\phi_i) \subseteq \Gamma_n(R_i)$ are the scalars that map to the identity upon quotienting by the maximal ideal, so $G_i(\phi_i)$ is precisely the set $1 + \mathfrak{m}_{R_i}$.

We know that the map $R_2 \to R_0$ is surjective because it is small, and since the morphisms in $\mathscr{C}_\Lambda$ fixes the residue field of the rings, this surjective map restricts to $G_2(\phi_2) = 1 + \mathfrak{m}_{R_2} \twoheadrightarrow 1 + \mathfrak{m}_{R_0} = G_0(\phi_0)$. Thus we conclude that ψ is injective and thus bijective.

□

Finally we can prove Theorem 17:

Proof of Theorem 17. The theorem follows immediately from Lemmas 19, 21, 23, and 26. □

4 Universal Deformation Rings in 1 dimension

In this section we study the case where $n = 1$ and we have a residual representation $\bar{\rho} : \Pi \to \mathrm{GL}_1(k) \cong k^\times$. Note that the group $\mathrm{GL}_n(R)$ is always abelian at $n = 1$, and since strict equivalence is defined up to conjugation, and conjugation in an abelian group is trivial, a deformation and a lift are the same thing in the 1-dimensional case.

Let $\Gamma = \Pi^{ab,(p)}$ be the abelianisation of the pro-p completion of Π, then if G is any abelian pro-p group, any homomorphism $\Pi \to G$ must uniquely factor through the projection $\gamma : \Pi \to \Gamma$, by the universal property of the abelianisation and pro-p completion of a group.

For a $\Lambda \in \mathscr{C}$, we define the notion of a *completed group ring*:

Definition. We define the *completed group ring* $\Lambda[[\Gamma]]$ to be the inverse limit of group rings $\Lambda[\Gamma/H]$ as H ranges over open normal subgroups of finite index of Γ:

$$\Lambda[[\Gamma]] = \varprojlim \Lambda[\Gamma/H]$$

It is true that $\Lambda[[\Gamma]]$ is an element of $\mathscr{C}_\Lambda$, we will show that $\bar{\rho}$ is in fact represented by this ring.

By lemma 3 there is a Teichmüller lift $k^\times \to \Lambda^\times$, so we can lift the representation $\bar{\rho}$ to Λ by composing with the Teichmuller lift, obtaining a representation $\rho_0 : \Pi \to \mathrm{GL}_1(\Lambda) \cong \Lambda^\times$.

Theorem 27. The universal deformation ring for $\bar{\rho}$ is $\mathcal{R} = \Lambda[[\Gamma]]$ and the universal deformation is given by:

$$\boldsymbol{\rho}(g) = \rho_0(g)[\gamma(g)]$$

Proof. Let Γ be generated as a group by elements $g_1, \cdots, g_r$. Then as a result there is a surjective ring homomorphism $\Lambda[[X_1, \cdots, X_r]] \to \Lambda[[\Gamma]]$

Now suppose $\rho : \Pi \to A^\times$ is a lift of $\bar{\rho}$ to $A \in \mathscr{C}_\Lambda$. Then consider the map $\psi(g) = \rho(g)/\rho_0(g)$, since the maps ρ, ρ_0 agree when restricted to $k^\times$, this means that ψ takes values in $1 + \mathfrak{m}_A$.

The group $1 + \mathfrak{m}_A = \varprojlim \left(1 + \mathfrak{m}_A^i/\mathfrak{m}_A^{i+1}\right)$ is an abelian pro-p group, so the map $\psi : \Pi \to 1 + \mathfrak{m}_A$ factors through the abelianised pro-p quotient Γ, this gives a map $f_\rho : \Gamma \to 1 + \mathfrak{m}_A$.

$$\begin{array}{ccc} \Pi & \xrightarrow{\gamma} & \Gamma \\ & \searrow^{\psi} & \downarrow f_\rho \\ & & 1 + \mathfrak{m}_A \end{array}$$

The map f_ρ extends to a homomorphism of Λ-algebras $f_\rho : \Lambda[[\Gamma]] \to A$. Note that this implies that $\rho = f_\rho \circ \boldsymbol{\rho}$.

Thus this implies that every representation ρ that lifts $\bar{\rho}$ is given by the composition of $\boldsymbol{\rho}$ with f_ρ. So $\Lambda[[\Gamma]]$ and $\boldsymbol{\rho}$ are the universal deformation ring and universal deformation of $\bar{\rho}$ respectively.

□

5 Universal Deformation Rings in Higher Dimensions

5.1 Tangent Space Revisited

We first define the adjoint representation of a residual representation $\bar{\rho}$:

Definition. Let Π act on the set of matrices $M_n(k)$ via conjugation by $\bar{\rho}$. i.e. for any matrix $M \in M_n(k)$:

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

Viewing $M_n(k)$ as a n^2 dimensional k vector space, this gives a representation of Π. Call this the *Adjoint Representation* of $\bar{\rho}$ and denote this by $\mathrm{Ad}(\bar{\rho})$. Representations of Π can be viewed as Π-modules, so $\mathrm{Ad}(\bar{\rho})$ is a Π-module.

We will now show that the tangent space of $\boldsymbol{D}$ is in fact isomorphic to the first group cohomology of the adjoint representation:

Proposition 28. Let $t_{\boldsymbol{D}} = \mathrm{Hom}_\Lambda(\mathcal{R}, k[\varepsilon])$ denote the tangent space of the functor $\boldsymbol{D}_\Lambda$. then we have an isomorphism:

$$t_{\boldsymbol{D}} \cong H^1(\Pi, \mathrm{Ad}(\bar{\rho}))$$

Proof. Let ρ be a deformation of $\bar{\rho}$ to the ring of dual numbers $k[\varepsilon]$. Then if $g \in \Pi$ and $\bar{\rho}(g) = A_g \in \mathrm{GL}_n(k)$, we must have that $\rho(g) = A_g + M_g\varepsilon$ for some $M_g \in M_n(k)$, noting that A is invertible we can write this as:

$$\rho(g) = (I + N_g\varepsilon)A_g$$

Noting that ρ should be a homomorphism of groups, we have that:

$$\begin{aligned}(I + N_{gh}\varepsilon)A &= (I + N_g\varepsilon)A_g(I + N_h\varepsilon)A_h \\ &= (I + N_gA_g\varepsilon + A_gN_h\varepsilon)A_h \\ &= (I + N_g\varepsilon + A_gN_hA_g^{-1}\varepsilon)A_{gh}\end{aligned}$$

Consider the map $\phi : \Pi \to M_n(k)$ given by $g \mapsto N_g$, then viewing M_n as the Π-module $\mathrm{Ad}(\bar{\rho})$. We have that ϕ satisfies:

$$\phi(gh) = \phi(g) + g \cdot \phi(h)$$

This is precisely the condition needed for a map $\Pi \to \mathrm{Ad}(\bar{\rho})$ to be a 1-cocyle, so ϕ is a cocycle.

On the other hand, suppose ρ' is another representation that is strictly equivalent to ρ. Then there exists $I + T\varepsilon \in \Gamma_n(k[\varepsilon])$ such that (note that $(I + T\varepsilon)(I - T\varepsilon) = I$):

$$\begin{aligned}\rho'(g) &= (I + T\varepsilon)\rho(g)(I + T\varepsilon)^{-1} \\ &= (I + T\varepsilon)(I + N_g\varepsilon)A_g(I - T\varepsilon) \\ &= A_g + TA_g\varepsilon + N_gA_g\varepsilon - A_gT\varepsilon \\ &= (I + T\varepsilon + N_g\varepsilon - A_gTA_g^{-1}\varepsilon)A_g\end{aligned}$$

So the cocycle associated to ρ' is the map $g \to N_g + T - A_gTA_g^{-1}$

The difference between these two cocycles is the map $g \to T - A_gTA_g^{-1} = T - g \cdot T$, which is precisely a coboundary.

Noting that there any lift ρ uniquely determines a cocycle ϕ and vice versa, we have proved that the set of deformations is of $\bar{\rho}$ is isomorphic to the first cohomology group $H^1(\Pi, \mathrm{Ad}(\bar{\rho})$.

We conclude the proof by noting that by Corollary 14, the tangent space is isomorphic to $\boldsymbol{D}(k[\varepsilon])$. ☐

We have a corollary:

Corollary 29. Let $d_1 = \dim H^1(\Pi, \mathrm{Ad}(\bar{\rho}))$. Then there is a surjection $\Lambda[[X_1, X_2, \cdots, X_{d_1}]] \twoheadrightarrow \mathcal{R}$. In order words, the universal deformation ring $\mathcal{R}$ is isomorphic to a quotient of the power series ring over Λ in d_1 variables.

Proof. By the previous proposition, we know that d_1 is the dimension of the tangent space $\boldsymbol{D}_\Lambda$. But the tangent space and cotangent space have the same dimension, so we have that:

$$d_1 = \dim_k t^*_{\mathcal{R}} = \dim_k \mathfrak{m}_R/(\mathfrak{m}_R^2, \mathfrak{m}_\Lambda)$$

Suppose $\mathfrak{m}_{\mathcal{R}} = (m_1, \cdots, m_n)$ be a minimal representation of $\mathfrak{m}_{\mathcal{R}}$ (i.e. one requiring minimal m_i's). Then the m_i must be linearly independent and they must not be in $\mathfrak{m}_{\mathcal{R}}^2$.

Then $\mathfrak{m}_{\mathcal{R}}/\mathfrak{m}_{\mathcal{R}}^2$ is a free Λ-module generated by exactly the elements $m_1, \cdots, m_n$. Quotienting by $\mathfrak{m}_\Lambda$ shows that $\mathfrak{m}_R/(\mathfrak{m}_R^2, \mathfrak{m}_\Lambda)$ is a k-vector space freely generated by $m_1, \cdots, m_n$. Then n is the dimension of $\mathfrak{m}_R/(\mathfrak{m}_R^2, \mathfrak{m}_\Lambda)$, and so $n = t_1$.

Using the construction from proposition 5, we obtain a surjection from $\Lambda[[X_1, X_2, \cdots, X_{d_1}]] \twoheadrightarrow \mathcal{R}$ as desired.

□

5.2 Obstruction Classes

We now define the notion of an obstruction class. Suppose $\phi : R_1 \to R_0$ is a surjective morphism of elements in $\mathscr{C}_\Lambda$ such that the kernel $\operatorname{Ker}\phi$ is annihilated by $\mathfrak{m}_{R_1}$. (This is similar to the condition of a small morphism but we do not require the kernel to be principal and the rings need not be Artinian.)

Let $\rho : \Pi \to \mathrm{GL}_n(R_0)$ be a lift of $\bar{\rho}$. We want to find possible deformations $\Pi \to \mathrm{GL}_n(R_1)$ that also lift ρ. Suppose $\gamma : \Pi \to GL_n(R_1)$ is a set-map that lifts ρ. The *obstruction* measures how far away this set map is from being a homomorphism of groups.

Since γ restricts to ρ upon mapping $R_1 \to R_0$, it follows that γ must have form:

$$\gamma(g) = \rho(g) + M_g$$

for $M_g \in M_n(\operatorname{Ker}\phi)$. If γ is a group homomorphism, then $\gamma(gh) = \gamma(g)\gamma(h)$. Define the function:

$$c(g,h) = \gamma(gh)\gamma(h)^{-1}\gamma(g)^{-1}$$

Then γ is a homomorphism if and only if $c(g,h) \equiv I$. However, since we know that γ is a homomorphism upon taking modulo $\operatorname{Ker}\phi$, we can write $c(g,h) = I + d(g,h)$, where $d(g,h) \in M_n(\operatorname{Ker}\phi)$, and γ is a homomorphism if and only if $d \equiv 0$.

Note that $\operatorname{Ker}\phi$ is annihilated by $\mathfrak{m}_{R_1}$, so we can view it as an $R_1/\mathfrak{m}_{R_1}$-module, i.e a k vector space. Thus if we let Π act on $M_n(\operatorname{Ker}\phi)$ by conjugation of $\bar{\rho}$, then it can be viewed as the G-module $\mathrm{Ad}(\bar{\rho}) \otimes_k \operatorname{Ker}\phi$.

Lemma 30. *$d(g,h) \in Z^2(\Pi, \mathrm{Ad}(\bar{\rho}) \otimes \operatorname{Ker}\phi)$ is a 2-cocycle. Moreover, for any other set-valued function γ' lifting ρ to R_1, the induced cocycle d' differs from d by a 2-coboundary in $B^2(\Pi, \mathrm{Ad}(\bar{\rho}) \otimes \operatorname{Ker}\phi)$.*

Thus, there exists a lift of ρ of R_1 if and only if the cohomology class given by $d(g,h)$ is trivial. We call $\mathcal{O}(\rho)$ the Obstruction class of ρ relative to $R_1 \to R_0$.

Proof. We first try to simplify the expression of d. Note that since $\operatorname{Ker}\phi \subseteq \mathfrak{m}_{R_1}$, it is annihilated by itself and so $M_g M_h = 0$ for any $g, h \in \Pi$. Noting this, a quick calculation shows that if $\gamma(g) = \rho(g) + M_g$ then

$$\gamma(g)^{-1} = \rho(g)^{-1} - \rho(g)^{-1} M_g \rho(g)^{-1}$$

Substituting this into $d(g,h) = \gamma(gh)\gamma(h)^{-1}\gamma(g)^{-1} - I$ and using the fact that ρ is still a group homomorphism, we obtain the expression:

$$\begin{aligned} d(g,h) &= (\rho(gh) + M_{gh})(\rho(h)^{-1} - \rho(h)^{-1}M_h\rho(h)^{-1})(\rho(g)^{-1} - \rho(g)^{-1}M_g\rho(g)^{-1}) - I \\ &= M_{gh}\rho(h)^{-1}\rho(g)^{-1} - \rho(gh)\rho(h)^{-1}M_h\rho(h)^{-1}\rho(g)^{-1} - \rho(gh)\rho(h)^{-1}\rho(g)^{-1}M_g\rho(g)^{-1} \\ &= M_{gh}\rho(gh)^{-1} - \rho(g)M_h\rho(gh)^{-1} - M_g\rho(g)^{-1} \end{aligned}$$

Note that since $d \in M_n(\operatorname{Ker}\phi)$ is annihilated by $\mathfrak{m}_{R_1}$, the conjugation action by $\bar{\rho}(g)$ is simply the same as the conjugation action by $\rho(g)$. Thus:

$$\begin{aligned} g_1 \cdot d(g_2, g_3) &= \rho(g_1)(M_{g_2g_3}\rho(g_2g_3)^{-1} - \rho(g_2)M_{g_3}\rho(g_2g_3)^{-1} - M_{g_2}\rho(g_2)^{-1})\rho(g_1)^{-1} \\ &= \rho(g_1)M_{g_2g_3}\rho(g_1g_2g_3)^{-1} - \rho(g_1g_2)M_{g_3}\rho(g_1g_2g_3)^{-1} - \rho(g_1)M_{g_2}\rho(g_1g_2)^{-1} \end{aligned}$$

On the other hand:

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

Thus comparing terms, we have that $g_1 \cdot d(g_2, g_3) = d(g_1g_2, g_3) - d(g_1, g_2g_3) + d(g_1, g_2)$, and so d defines a 2-cocyle.

On the other hand, suppose γ' is a different lift of ρ, then $\gamma(g) = \rho(g) + M'_g$ for a different $M'_g \in M_n(\operatorname{Ker}\phi)$. Then letting $N_g = M_g - M'_g$, we have that:

$$\begin{aligned}
d(g, h) - d'(g, h) &= N_{gh}\rho(gh)^{-1} - \rho(g)N_h\rho(gh)^{-1} - N_g\rho(g)^{-1}\\
&= g\psi(h) - \psi(gh) + \psi(g)
\end{aligned}$$

Where we define $\psi \in C^1(G, \operatorname{Ad}(\bar{\rho}) \otimes \operatorname{Ker}\phi)$ by $g \mapsto N_g\rho(g)^{-1}$. Thus the map d changes by a co-boundary when you change the lift γ.

Thus, d gives a cohomology class in $\mathcal{O}(\rho) \in H^2(\Pi, \operatorname{Ad}(\bar{\rho}) \otimes \operatorname{Ker}\phi) \cong H^2(\Pi, \operatorname{Ad}(\bar{\rho})) \otimes \operatorname{Ker}\phi$, and a lift of ρ exists if and only if $\mathcal{O}(\rho) = 0$. As desired. □

In general these obstruction classes are hard to calculate, but a special case is if the second homology $H^2(\Pi, \operatorname{Ad}(\bar{\rho}))$ is trivial, in which case the obstruction class must be zero and so a lift exists. In this case it is in fact very easy to compute the deformation ring:

Theorem 31. Let $d_i = \dim H^i(\Pi, \operatorname{Ad}(\bar{\rho}))$, and suppose that $C_k(\bar{\rho}) = k$ and $\mathcal{R} = \mathcal{R}(\Pi, k, \bar{\rho})$ is the universal deformation ring representing $\boldsymbol{D}_\Lambda$. Then we have:

$$\operatorname{Krull}\dim(\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R}) \geq d_1 - d_2$$

Moreover, if $d_2 = 0$ (i.e. the second cohomology is trivial), then the above inequality is in fact an equality, and

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

Proof. From corollary 29 we know that there is a surjective homomorphism $\Lambda[[X_1, X_2, \cdots, X_{d_1}]] \twoheadrightarrow \mathcal{R}$, and this homomorphism induces an isomorphism of tangent spaces. Define F to be the ring $\Lambda[[X_1, X_2, \cdots, X_{d_1}]]/\mathfrak{m}_\Lambda = k[[X_1, X_2, \cdots, X_{d_1}]]$ and let J be the kernel of the morphism $F = k[[X_1, X_2, \cdots, X_{d_1}]] \twoheadrightarrow \mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R}$, then we have an exact sequence:

$$0 \to J \to F \to \mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R} \to 0$$

Since $\mathfrak{m}_F J \subseteq J$, we can further quotient to get the exact sequence of k-vector spaces:

$$0 \to J/\mathfrak{m}_F J \to F/\mathfrak{m}_F J \to \mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R} \to 0$$

Let $d = \dim_k J/\mathfrak{m}_F J$ be the dimension of $\dim_k J/\mathfrak{m}_F J$ as a vector space. Fix a basis of this vector space and let $j_1, j_2, \cdots, j_d \in J$ be a lift of the basis to J, then if $\mathcal{I}$ is the ideal in F generated by the j_i's, then we have that $J = \mathcal{I} + \mathfrak{m}_F J$. By Nakayama's lemma, $\mathcal{I} = J$ and so J is generated by the d elements $j_1, \cdots, j_d$.

Since $\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R} \cong F/J$, and $F = k[[X_1, \cdots, X_{d_1}]]$ has krull dimension d_1. By a theorem in commutative algebra, quotienting by an ideal of d elements decreases the Krull dimension by at most d. Thus we have

$$\operatorname{Krull}\dim(\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R}) \geq d_1 - d = d_1 - \dim_k(J/\mathfrak{m}_F J)$$

Thus it suffices to prove that $d_2 \geq \dim_k(J/\mathfrak{m}_F J)$.

Let $\boldsymbol{\rho}_p$ be the composition of the universal deformation with the quotient map $\mathcal{R} \to \mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R}$, by the universal property of quotients, deformations to any Λ-algebra that where $\mathfrak{m}_\Lambda$ is sent to zero factors uniquely though $\boldsymbol{\rho}_p$, or in other words $\boldsymbol{\rho}_p$ is universal amongst k-algebras.

We consider the obstruction of lifting $\boldsymbol{\rho}_p$ to $F/\mathfrak{m}_F J$, which is the cohomology class $\mathcal{O}(\boldsymbol{\rho}_p) \in H^2(\Pi, \mathrm{Ad}(\bar{\rho}))\otimes J/\mathfrak{m}_F J$. We define the k-linear map:

$$\alpha : \mathrm{Hom}_k(J/\mathfrak{m}_F J, k) \to H^2(\Pi, \mathrm{Ad}(\bar{\rho})) \otimes J/\mathfrak{m}_F J$$

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

So it suffices to prove that the map α is injective. Suppose $f \in \operatorname{Ker}\alpha$ be non-zero, and $A = (F/\mathfrak{m}_F J)/\operatorname{Ker} f$ be the quotient of $F/\mathfrak{m}_F J$ by the kernel of f, and also define $I = (J/\mathfrak{m}_F J)/\operatorname{Ker} f = \operatorname{Im} f = k$. Then we get the exact sequence:

$$0 \to I \to A \to \mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R} \to 0$$

This still induces an isomorphism of tangent spaces, but since we quotiented by the kernel of f, the obstruction class of lifting $\boldsymbol{\rho}_p$ to A is now trivial.

Thus we must have a lift of $\boldsymbol{\rho}_p$ to the ring A. Since A is a k-algebra, by the universal property of $\boldsymbol{\rho}_p$ this lift must be induced by a homomophism $\mathcal{R} \to A$ that factors through $\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R}$, so we get a lift induced by a homomorphism $\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R} \to A$. Thus by the split-exact sequence lemma the above exact sequence splits, and $A \cong \mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R} \oplus I$. However, I being nonzero contradicts the fact that the tangent spaces of A and $\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R}$ are isomorphic. Thus the image of f cannot be non-zero. i.e. $\operatorname{Ker}\alpha = 0$, thus proving $d_2 \geq \dim_k(J/\mathfrak{m}_F J)$ and $\operatorname{Krull}\dim(\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R}) \geq d_1 - d_2$.

Finally, if $d_2 = 0$, this means that J has at most 0 generators. This in turn implies that the kernel of the map $\Lambda[[X_1, \cdots, X_{d_1}]] \to \mathcal{R}$ has kernel 0, which implies

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

□

Before we continue we need more group theory:

5.3 More Group Theory

This section will be a miscellaneous collection of group theoretical results which we will need in the next subsection.

Lemma 32. $\Gamma_n(R)$ is a pro-p group for any $R \in \mathscr{C}$.

Proof. Using the fact that $\Gamma_n(R)$ can be written as the profinite limit:

$$\Gamma_n(R) = \varprojlim \Gamma_n(R/\mathfrak{m}_R^r)$$

It suffices to show that $\Gamma_n(R/\mathfrak{m}_R^r)$ is a p-group for each k. We induct on r.

When $k = 1$ we know that $\Gamma_n(R/\mathfrak{m}_R) = \{I\}$ is a p-group. Now suppose $\Gamma_n(R/\mathfrak{m}_R^{r-1})$ is a p-group and consider the transition map:

$$\Gamma_n(R/\mathfrak{m}_R^r) \to \Gamma_n(R/\mathfrak{m}_R^{r-1})$$

This map is surjective and by our induction hypothesis the image is a p-group. It suffices to show that kernel of the map is also a p-group. Any element in the kernel must reduce to the identity matrix upon taking mod $\mathfrak{m}_R^{r-1}$, thus must have form $I + M$ for $M \in M_n(\mathfrak{m}_R^r/\mathfrak{m}_R^{r-1})$. So there is a bijection between the kernel of the map to the set $M_n(\mathfrak{m}_R^r/\mathfrak{m}_R^{r-1})$. Since $\mathfrak{m}_R^r/\mathfrak{m}_R^{r-1}$ is a finite dimensional k-vector space, it follows that $M_n(\mathfrak{m}_R^r/\mathfrak{m}_R^{r-1})$ has order a power of p, so the map has kernel a p-group. □

We state without proof the following theorems:

Theorem 33 (Schur-Zassenhaus [Rob96])**.** Let G be a profinite group with a normal pro-p Sylow subgroup P such that P has finite index in G and is topologically finitely generated (i.e. P has a dense open subgroup that is finitely generated). Let $\pi : G \to G/P$ be the quotient map. Then there exists a subgroup $A \leq G$ such that π induces an isomorphism $A \cong G/P$. Furthermore any other $A' \leq G$ satisfying this property is conjugate to A by an element of P.

In particular, this also implies that $G = P \rtimes A$ is the semidirect product of A and P.

Theorem 34 (Burnside's Basis Theorem)**.** Let G and P be as the previous theorem. Let $\bar{P}$ be the maximal p-elementary abelian quotient of P (i.e. the maximal quotient of P such that $\bar{P}$ is abelian and every element has order p). Note that $\bar{P}$ is a $\mathbb{F}_p$-vector space.

If $x_1, \cdots, x_d \in P$ and their images under $P \to \bar{P}$ generate $\bar{P}$ as a vector space, then the elements $x_1, \cdots, x_d$ generate a dense subgroup of P.

Lemma 35. Let P be a pro-p group and $\bar{P}$ the maximal p-elementary abelian quotient. Given two A-actions $A \to \operatorname{Aut} P$ that restrict to the same map $A \to \operatorname{Aut} \bar{P}$ upon quotienting, the semidirect products of P and A induced by these two actions are isomorphic.

We now prove:

Proposition 36 ([Bos91])**.** Let $G, A, P, \bar{P}$ be as the above theorems. Since $P, \bar{P}$ is normal, let A act on P and $\bar{P}$ by conjugation, making them into A-modules.

If $\bar{V}$ is a $\mathbb{F}_p[A]$-submodule of $\bar{P}$ (i.e. $\bar{V}$ is a vector subspace of $\bar{P}$ that is closed the A-action), then there exists an A-invariant subgroup V of P with $\dim_{\mathbb{F}_p} \bar{V}$ generators which maps onto $\bar{V}$ via the map $\pi : G \to G/P$.

Proof. We first prove the case in which P is a free pro-p group. So P is the pro-p completion of the free group.

Let $\mathcal{F}$ be the free pro-p group with $\dim \bar{V}$ generators, with the generators of $\mathcal{F}$ abstractly identified with a basis of $\bar{V}$, so that there is a surjection $\mathcal{F} \to V$. Since there is an A action $A \to \operatorname{Aut}(\bar{V})$, we can lift this to an A-action on $\mathcal{F}$.

Let $\bar{U}$ be a $\mathbb{F}_p[A]$-module complement of $\bar{V}$ in $\bar{P}$, and let $\mathcal{G}$ be the free pro-p group with $\dim \bar{U}$ generators. We repeat the same construction as above to obtain an A-action on $\mathcal{G}$.

Then since there is an A-action on the both $\mathcal{F}$ and $\mathcal{G}$, there is an A-action on the free product $\mathcal{F} * \mathcal{G}$. Since P is also a free pro-p group by assumption, $\mathcal{F} * \mathcal{G} \cong P$. By our construction the maximal p-elementary abelian quotient of $\mathcal{F} * \mathcal{G}$ is $\bar{P}$ and the A-action on this quotient is the same as the A-action on $\bar{P}$ given by quotienting P. This implies that the semidirect product of $\mathcal{F} * \mathcal{G}$ and A is isomorphic to the semidirect product of P and A by lemma 35. Then taking V to be the image of $\mathcal{F}$ under this isomorphism, V is A-invariant with the correct number of generators, and it maps onto $\bar{V}$ as desired.

Now suppose P is a general pro-p group. Let $\mathcal{F} \to P$ be a surjective homomorphism from a free pro-p group $\mathcal{F}$ with $\dim \bar{P}$ generators. Let R be the kernel of the surjection and denote by $\operatorname{Aut}_R \mathcal{F}$ the the automorphisms of $\mathcal{F}$ that fix R.

We will show the map $\operatorname{Aut}_R \mathcal{F} \to \operatorname{Aut} P$ induced by $\phi : \mathcal{F} \twoheadrightarrow P$ is surjective. Fix a generating set $g_1, \cdots, g_r$ of P. Let $f_1, \cdots, f_r$ be a generating set of $\mathcal{F}$ that maps to this generating set of P under ϕ. For any automorphism $\alpha : P \to P$, let $e_1, \cdots, e_r$ be the images of $g_1, \cdots, g_r$ via α, and $h_1, \cdots, h_r$ be lifts of e_i via ϕ. Then the map $\mathcal{F} \to \mathcal{F}$ given by $f_i \mapsto h_i$ is surjective, since the elements h_i are independent in the vector space $\bar{P}$ by Burnside's basis theorem. This map induces an isomorphism on the maximal p-elementary abelian quotient $\bar{\mathcal{F}}$. Thus by Burnside's basis theorem, this is also an isomorphism on $\mathcal{F}$. R is fixed under this map since it maps to zero in P, so this is an element of $\operatorname{Aut}_R \mathcal{F}$ that restricts to α, so the map is surjective.

In particular, for an A-action $A \to \operatorname{Aut} P$, we can lift this to an A-action $A \to \operatorname{Aut}_R \mathcal{F}$. By our first case, $\mathcal{F}$ contains a closed subgroup J that is free on the generators of $\bar{V} \leq \bar{P}$, and is invariant by this A-action. Then the image of J in P gives us our desired $\bar{V}$. □

Definition. Suppose $H \leq \mathrm{GL}_n(k)$ be a subgroup whose order is coprime to p. Then any $k[H]$-module decomposes into a direct sum of irreducible $k[H]$-modules by Maschke's theorem.

Give $M_n(k)$ a $k[H]$-module structure through conjugation by elements in H, and call this module M. Let V be another $k[H]$-module, then V is *prime-to-adjoint* if V and M have no irreducible sub-representations in common.

5.4 More Galois Theory

For this section assume $p > 2$. Let $K/\mathbb{Q}$ be be a number field and let $H = \mathrm{Gal}(K/\mathbb{Q})$. Let S_0 be a finite set of primes in $\mathbb{Q}$ containing p and the infinity, and let S be the set of primes in K that lie above S_0. Let L be the maximal pro-p extension of K that is unramified outside S, and let $P = \mathrm{Gal}(L/K)$.

Let r_2 be the number of complex places of K, and for $\mathbb{F}$ a field, define the function:

$$\delta(\mathbb{F}) = \begin{cases} 0 & \mathbb{F} \text{ contains a primitive } p\text{-th root of unity} \\ 1 & \text{otherwise} \end{cases}$$

Let K_v be the completion of K at the place v. Define Z_S to be the set of nonzero elements $x \in K$ such that the fractional ideal (x) is a pth power when factored into prime ideals (this makes sense because prime ideal factorisation in number fields is unique) and x is a p-th power in each completion K_v for $v \in S$.

In particular, Z_S contains $(K^\times)^p$, the set of all p-th powers in K. Note that the sets Z_S and $(K^\times)^p$ are stable under the Galois action by $H = \mathrm{Gal}(K/\mathbb{Q})$ since images of p-th powers under field automorphisms are still p-th powers. Thus we can think of the sets Z_S and $(K^\times)^p$ as $\mathbb{F}_p[H]$-modules, and let B_S denote the quotient $\mathbb{F}_p[H]$-module $Z_S/(K^\times)^p$, which is in particular also a $\mathbb{F}_p$-vector spaces.

We now quote the following theorem:

Theorem 37 ([Koc70])**.** Let $d(P)$ and $r(P)$ denote the generator rank and relation rank (i.e. the minimal number of generators and relations needed to define P as a pro-p group) of P, then the following two identities hold:

$$\begin{aligned} r(P) &= \left(\sum_{v \in S} \delta(K_v) \right) - \delta(K) + \dim_{\mathbb{F}_p} B_s \\ d(P) &= r_2 + 1 + r(P) \end{aligned}$$

In particular, this implies that P is topologically finitely generated (it has a dense open subgroup that is finitely generated).

We further make the following definitions. Let $\bar{E} = K^\times/(K^\times)^p$ denote the units in K modulo pth powers, and define $\bar{E}_v = K_v^\times/(K_v^\times)^p$ similarly. We quote a result from global class field theory:

Theorem 38. Suppose the class number of K is not divisible by p, then we have the following exact sequence of $\mathbb{F}_p[H]$-modules: [Bos91]

$$0 \to B_S \to \bar{E} \to \bigoplus_{v \in S} \bar{E}_v \to \bar{P} \to 0$$

For each prime $l \in \mathbb{Q}$, let $H_l \leq H$ the decomposition subgroup at a prime lying above l (i.e. H_l is the subgroup of H that fixes the prime ideal $\mathfrak{l}$, for $\mathfrak{l}$ an ideal of K that lies above l. This group is unique up to conjugation.). Furthermore let H_∞ be the subgroup of H generated by a complex conjugation. Finally let $\mu_p(K)$ be the group of pth roots of unity in K. Then we state this following theorem:

Theorem 39 ([BM89])**.** As $\mathbb{F}_p[H]$-modules, if the order of H is not divisible by p, then we have the following isomorphisms:

$$\begin{aligned} \bigoplus_{v \in S} \bar{E}_v &\cong \mathbb{F}_p[H] \oplus \left(\bigoplus_{l \in S_0} \mathrm{Ind}_{H_l}^H \mu_p(K_l) \right) \\ \bar{E} \oplus \mathbb{F}_p &\cong \mu_p(K) \oplus \mathrm{Ind}_{H_\infty}^H \mathbb{F}_p \end{aligned}$$

Where Ind refers to the induced representation. And K_l refers to the field K_{v_l}, for any choice of $v_l \in S$ which lies above l. The choice of v_l does not matter because the induced module will be isomorphic regardless of choice.

We also state without proof:

Theorem 40 ([Bos91])**.** For $R \in \mathscr{C}$, let X be a finitely generated subgroup of $\Gamma_n(R)$, and let A be a subgroup of $\mathrm{GL}_n(R)$ that fixes X under conjugation. Then if the maximal p-elementary quotient $\bar{X}$ is prime-to-adjoint as a $\mathbb{F}_p[A]$ module, then X is trivial.

5.5 Dimension bounds for Galois Groups over Number Fields

We return to deformations of representations, and finally, we specialise Π to be a Galois Group. Fix a number field K and S a finite set of primes that contains all primes above p and primes at infinity. Define also $S_\infty \subseteq S$ to be the set of primes at infinity. Let $\Pi = G_{K,S}$, and for a prime v of K, we write K_v to be the completion of K with respect to v.

We first state without a proof a corollary of the global Euler characteristic formula, and a reference of this can be found in section I.5 in [Mil06]:

Theorem 41. Let M be a $G_{K,S}$-module and $d = [K : \mathbb{Q}]$, then:

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

In particular if $M = \mathrm{Ad}(\bar{\rho})$ we have that:

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

An immediate corollary is the following:

Corollary 42.

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

Proof. This follows from Theorem 31 and the fact that $H^0(\Pi, \mathrm{Ad}(\bar{\rho})) = \mathrm{Ad}(\bar{\rho})^\Pi$ is the elements of M_n that commute with the image of Π. This is precisely $C_k(\bar{\rho}) = k$, so $d_0 = 1$. Substituting and rearranging gives:

$$\mathrm{Krull}\dim(\mathcal{R}/\mathfrak{m}_\Lambda \mathcal{R}) \geq d_1 - d_2 = 1 + dn^2 - \sum_{v \in S_\infty} \dim H^0(G_{K_v}, \mathrm{Ad}(\bar{\rho}))$$

□

5.6 Tame Representations

This section mostly follows the exposition given in [Bos91].

Let $K = \mathbb{Q}$ and $\Pi = G_{\mathbb{Q},S} = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$. Suppose we have an absolutely irreducible residual representation $\bar{\rho} : \Pi \to \mathrm{GL}_n(k)$. We define $\Pi_0 = \mathrm{Ker}(\bar{\rho})$, and let $K = \mathbb{Q}^{\Pi_0}$ be the field fixed by Π_0. Let S_1 be the set of primes of K that lie above primes in S.

If $\boldsymbol{\rho} : \Pi \to \mathrm{GL}_n(\mathcal{R})$ is the universal deformation of $\bar{\rho}$, then note that since Π_0 maps to the identity under $\bar{\rho}$, the image of Π_0 under the lift $\boldsymbol{\rho}$ must restrict to the identity. In other words:

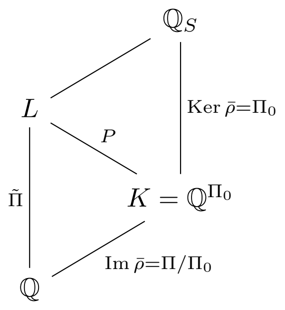
$$\boldsymbol{\rho}(\Pi_0) \subseteq \Gamma_n(\mathcal{R})$$

and $\boldsymbol{\rho}$ gives induces a homomorphism $\Pi_0 \to \Gamma_n(\mathcal{R})$ by restriction.

By the universal property of pro-p quotients, the map $\Pi_0 \to \Gamma_n(\mathcal{R})$ must factor through a pro-p quotient of Π_0.

Let L be the maximal pro-p extension of K that is unramified outside of the set of primes S_1, and define $P = \mathrm{Gal}(L/K)$ (i.e. L is the maximal extension of K such that the P is pro-p). By the definition of L we have that P is the maximal pro-p-quotient of Π_0 then map $\boldsymbol{\rho}|_{\Pi_0} : \Pi_0 \to \Gamma_n(\mathcal{R})$ factors through P uniquely. Looking at our original map, this implies that $\boldsymbol{\rho} : \Pi \to \mathrm{GL}_n(\mathcal{R})$ must uniquely factor through $\tilde{\Pi} = \mathrm{Gal}(L/\mathbb{Q})$.

We have the following diagram indicating inclusion of fields with corresponding Galois groups labelled on the edges:



Since we have shown that the universal deformation $\boldsymbol{\rho}$ factors through the group $\tilde{\Pi}$, also called the *p-completion* Π *relative to* $\bar{\rho}$. This implies that in order to study the deformations of $\bar{\rho} : \Pi \to \mathrm{GL}_n(k)$, it is in fact enough to restrict this residual representation to the group $\tilde{\Pi}$ and only consider $\bar{\rho} : \tilde{\Pi} \to \mathrm{GL}_n(k)$. By our construction we know that $\tilde{\Pi}/P \cong \mathrm{Im}(\bar{\rho})$.

We now define the notion of a *tame represenation.*

Definition. A residual representation $\bar{\rho} : \Pi \to \mathrm{GL}_n(k)$ is *tame* if the order of $\mathrm{Im}(p)$ is not divisible by p.

Write $H = \mathrm{Im}(\bar{\rho}) = \tilde{\Pi}/P$ and suppose $\bar{\rho}$ is a tame representation. In this case P is a maximal pro-p subgroup of $\tilde{\Pi}$, i.e. it is a Sylow pro-p subgroup. Thus we can apply theorem 33 (the Schur-Zassenhaus theorem) and obtain that there is a subgroup $A \leq \tilde{\Pi}$ that is isomorphic to H, and $\tilde{\Pi} = P \rtimes A$.

We know that $\Gamma_n(W(k))$ is a pro-p group from lemma 32. Let $G \leq \mathrm{GL}_n(W(k))$ be the preimage of $\mathrm{Im}(\bar{\rho})$ under the projection map $\mathrm{GL}_n(W(k)) \to \mathrm{GL}_n(k)$, and consider the projection map restricted to G, i.e the map $G \to \mathrm{Im}(\bar{\rho})$. This map is surjective and has kernel a subgroup of $\Gamma_n(W(k))$ which is pro-p. Since the image of the map is not divisible by p, it means that the this kernel is a Sylow pro-p subgroup of G. This means we can apply theorem 33 again and G contains a subgroup H_1 isomorphic to $H = \mathrm{Im}(\bar{\rho})$.

Since $G \leq \mathrm{GL}_n(W(k))$, this means that $\mathrm{GL}_n(W(k))$ contains a subgroup H_1 that is isomorphic to H. Since $\bar{\rho}$ has image H, there is clearly a lift ρ_1 lifting $\bar{\rho}$ to $W(k)$ simply by identifying $H = \mathrm{Im}(\bar{\rho})$ with the subgroup H_1 of $\mathrm{GL}_n(W(k))$.

Thus we have a lift:

$$\rho_1 : \tilde{\Pi} \to \mathrm{GL}_n(W(k))$$

That induces an inclusion $\sigma : A \hookrightarrow \mathrm{GL}_n(W(k))$, sending A to H_1.

Proposition 43. Any other lift of $\bar{\rho}$ to $W(k)$ is strictly equivalent to ρ_1, and σ is also unique up to conjugation by $\Gamma_n(W(k))$.

Proof. Suppose $\rho_1' : \tilde{\Pi} \to \mathrm{GL}_n(W(k))$ is another lift of $\bar{\rho}$. Then we have a map $\mathrm{Im}(\rho_1') \to \mathrm{Im}(\bar{\rho})$ via restricting the domain of the map $\mathrm{GL}_n(W(k)) \to \mathrm{GL}_n(k)$, and moreover $\mathrm{Im}(\rho_1') \leq G$. This map has kernel a subgroup of $\Gamma_n(W(k))$ and is thus a p group, and again, since the image of the map has order not divisible by p, the kernel of this image is a Sylow pro-p subgroup of $\mathrm{Im}(\rho_1') \leq G$. Applying the Schur-Zassenhaus theorem again there must be a subgroup of $\mathrm{Im}(\rho_1')$ isomorphic to H. This is also a subgroup of G, and Schur-Zassenhaus states any two such groups must be conjugate by an element of the Sylow pro-p subgroup of G. Thus the restriction of A in ρ_1 and ρ_1' differ by a conjugation by an element in $\Gamma_n(W(k))$. Since all homomorphisms also need to be continuous, this means that ρ_1 and ρ_1' must also differ by a conjugation in $\Gamma_n(W(k))$ and they are thus strictly equivalent lifts. $\square$

Since we know that $\mathscr{C} = \mathscr{C}_{W(k)}$, every ring $R \in \mathscr{C}$ has a canonical $W(k)$ algebra structure given by a homomorphism $W(k) \to R$. Thus by composing σ by this map, we have a homomorphism $\sigma_R : A \to \mathrm{GL}_n(R)$.

From earlier this section we know that every deformation of $\bar{\rho} : \tilde{\Pi} \to \mathrm{GL}_n(k)$ to R induces a homomorphism from $P = \operatorname{Ker} \bar{\rho} \to \Gamma_n(R)$. Note that A acts on P via conjugation since P is a normal subgroup of $\tilde{\Pi}$. On the other hand, A acts on $\Gamma_n(R)$ through conjugation by σ_R. So both P and $\Gamma_n(R)$ have A-actions, it makes sense to ask which continuous homomorphisms $P \to \Gamma_n(R)$ commute with this A action. We define the set-valued functor $\boldsymbol{E}_{\bar{\rho}} : \mathscr{C} \to \mathsf{Sets}$ to be precisely these homomorphisms:

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

Since $\tilde{\Pi} = P \rtimes A$, any deformation $\tilde{\Pi} \to \mathrm{GL}_n(R)$ is determined by where it sends P and A, as long as the map from P to $\mathrm{GL}_n(R)$ respects the A action on P.

In other words, given an element of $\boldsymbol{E}_{\bar{\rho}}$, this combined with the map σ_R specifies a lift $\tilde{\Pi} \to \mathrm{GL}_n(R)$. Thus there is a natural morphism of functors $\boldsymbol{E}_{\bar{\rho}} \to \boldsymbol{D}_{\bar{\rho}}$. We now state a theorem from [Bos91]:

Theorem 44. If $C_k(\bar{\rho}) = k$, then the natural morphism $\boldsymbol{E}_{\bar{\rho}} \to \boldsymbol{D}_{\bar{\rho}}$ is in fact an isomorphism.

Proof. We wish to show that for an arbitrary $R \in \mathscr{C}$, the induced map $\boldsymbol{E}_{\bar{\rho}}(R) \to \boldsymbol{D}_{\bar{\rho}}(R)$ is a bijection.

We first show that the map is surjective. Let $[\rho] \in \boldsymbol{D}_{\bar{\rho}}(R)$ be a deformation of $\bar{\rho}$. Then ρ restricts to a map $A \to \mathrm{GL}_n(R)$. By the above proposition, this map is conjugate to the map σ_R. So without loss of generality, pick a representative ρ of the strict equivalence class $[\rho]$ such that the induced map $A \to \mathrm{GL}_n(R)$ is precisely the map σ_R. But in this case, since the induced map is σ_R, by restricting ρ to the subgroup P, we have a map that is compatible with the A-action on P and $\Gamma_n(R)$. Thus $\rho|_P$ is precisely an element in $\boldsymbol{E}_{\bar{\rho}}(R)$, and this exactly maps to the strict equivalence class $[\rho]$.

Now we show that this is an injective map. Suppose $\phi_1, \phi_2 \in \boldsymbol{E}_{\bar{\rho}}(R)$ and induce lifts $\psi_1, \psi_2 \in \boldsymbol{D}_{\bar{\rho}}(R)$. Both ψ_1 and ψ_2 will induce the map $\sigma : A \to \mathrm{GL}_n(W(k))$ on A, this means that the element that ψ_1 and ψ_2 are conjugate through a matrix in $\Gamma_n(R)$ that fixes A under conjugation. In other words, it must commute with the image of A.

On the other hand, the homomorphisms $P \to \Gamma_n(R)$ commute with the A-action, and so since $C_k(\bar{\rho}) = k$ consists of only scalar matrices, the maps ψ_1 and ψ_2 must be conjugate by a scalar matrix. This means that $\psi_1 = \psi_2$, and by restricting the maps to P, we have that $\phi_1 = \phi_2$. ∎

This is useful because if we can find a ring that represents $\boldsymbol{E}_{\bar{\rho}}$, then this ring must also represent $\boldsymbol{D}_{\bar{\rho}}$.

Theorem 45. The functor $\boldsymbol{E}_{\bar{\rho}}$ is representable.

Proof. Pick generators $x_1, x_2, \cdots x_d$ of P, then the image of x_r in $\Gamma_n(R)$ has the form $I + M_r$ for $M_r \in M_n(\mathfrak{m}_R)$. Let M_r have entries $M = (m_{ij}^{(r)})_{1 \le i,j \le n}$.

Let $\mathcal{F}$ be the pro-p completion of the free group with generators $x_1, x_2, \cdots, x_d$. Then there exists a surjection $\mathcal{F} \to P$ with kernel N, In this case, there is a bijective correspondence between homomorphisms $P \to \Gamma_n(R)$ and homomorphisms $\mathcal{F} \to \Gamma_n(R)$ where N is contained in the kernel.

Consider the power series ring in dn^2 variables $W(k)[[T_{ij}^{(r)}]]_{1 \le r \le d; 1 \le i,j \le n} = W(k)[[T_{11}^{(1)}, \cdots, T_{nn}^{(d)}]]$. We define a homomorphism $\mathcal{F} \to \Gamma_n(W(k)[[T_{ij}^{(r)}]])$ which sends:

$$x_r \mapsto I + (T_{ij}^{(r)})$$

Requiring that N is in the kernel is simply imposing a number of linear equations on $T_{ij}^{(r)}$, and similarly the requirement that the A-actions commute with $P \to \Gamma_n(R)$ is also just imposing a number of linear conditions. Let $\mathcal{I}$ be the ideal generated by these conditions and define $\mathcal{R} = W(k)[[T_{ij}^{(r)}]]/\mathcal{I}$.

These conditions give rise to a homomorphism $\mathcal{F} \to \Gamma_n(\mathcal{R})$ which has kernel N, and thus gives a homomorphism $P \to \Gamma_n(\mathcal{R})$ which respects the A-action. This is universal, since any other function $P \to \Gamma_n(R)$ would uniquely factor through a map $\mathcal{F} \to \mathcal{R}$, and thus uniquely give a ring map $\mathcal{R} \to R$. Thus the ring $\mathcal{R}$ represents the functor $\boldsymbol{E}_{\bar{\rho}}$. ∎

Since the functors $\boldsymbol{E}_{\bar{\rho}}$ and $\boldsymbol{D}_{\bar{\rho}}$ are isomorphic, this implies that the their tangent spaces are isomorphic too. $\boldsymbol{E}_{\bar{\rho}}$ has tangent space:

$$t_{\boldsymbol{E}_{\bar{\rho}}} = \boldsymbol{E}_{\bar{\rho}}(k[\varepsilon]) = \mathrm{Hom}_A(P, \Gamma_n(k[\varepsilon]))$$

As noted in theorem 22, $\Gamma_n(k[\varepsilon])$ has elements of the form $I + N\varepsilon$ for $N \in M_n(k)$ and multiplying two elements in $\Gamma_n(k[\varepsilon])$ corresponds to adding in $M_n(k)$. Moreover, the conjugation by A action commutes with the correspondence between $\Gamma_n(k[\varepsilon])$ and $M_n(k)$. Thus $\Gamma_n(k[\varepsilon])$ and $\mathrm{Ad}(\bar{\rho})$ are isomorphic as A modules. Thus

$$\mathrm{Hom}_A(P, \Gamma_n(k[\varepsilon])) = \mathrm{Hom}_A(P, \mathrm{Ad}(\bar{\rho}))$$

But since theorem 22 also stated that $\Gamma_n(k[\varepsilon]) = \mathrm{Ad}(\bar{\rho})$ is p-elementary abelian, so any A-morphism $P \to \mathrm{Ad}(\bar{\rho})$ factors uniquely through $\bar{P}$, the maximal p-elementary abelian quotient of P. Thus:

$$\mathrm{Hom}_A(P, \mathrm{Ad}(\bar{\rho})) = \mathrm{Hom}_A(\bar{P}, \mathrm{Ad}(\bar{\rho}))$$

In particular, we now know that:

Lemma 46.

$$\dim_k t_{\boldsymbol{D}_{\bar{\rho}}} = \dim_k t_{\boldsymbol{E}_{\bar{\rho}}} = \dim_k \mathrm{Hom}_A(\bar{P}, \mathrm{Ad}(\bar{\rho}))$$

Since the order of A is not divisible by p, by Maschke's Theorem, both $\bar{P}$ and $\mathrm{Ad}(\bar{\rho})$ can be decomposed as a sum of irreducible A-modules. This means that if we compute the decomposition of the two modules, then the dimension of the tangent space can be determined by the irreducible A-modules that appear in both the decompositions (by Schur's lemma, any morphism between irreducible representations is either zero or an isomorphism).

5.7 Explicit Deformations in a Special Case

Definition. Let $n = 2$ and p be an odd prime. Suppose $\sigma \in G_{\mathbb{Q},S}$ be the complex conjugation automorphism. Then $\sigma^2 = \mathrm{Id}$ and since p is an odd prime, $\bar{\rho}(\sigma)$ is a matrix of order 2 in $\mathrm{GL}_2(k)$.

We say $\bar{\rho}$ is *odd* if $\det \bar{\rho}(\sigma) = -1$ and *even* if $\det \bar{\rho}(\sigma) = +1$.

We state the final result of this essay:

Theorem 47 ([Bos91])**.** Let p be an odd prime and suppose that $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$ is tame, odd, and absolutely irreducible. Recall that and K be the field fixed by $\mathrm{Ker}\,\bar{\rho}$, and $H = \mathrm{Im}(\bar{\rho})$ and $P = \mathrm{Gal}(L/K)$, and define:

$$V = \mathrm{coker}\left(\mu_p(K) \to \bigoplus_{v \in S} \mu_p(K_v)\right)$$

And let $B = B_S = Z_S/(K^\times)^p$. Then both V and B are $\mathbb{F}_p[H]$-modules. Suppose that the class number of K is not divisible by p and V and B have no common irreducible factors with $\mathrm{Ad}(\bar{\rho})$ when decomposed into irreducible $\mathbb{F}_p[H]$-modules. Then:

$$\mathcal{R}_{\bar{\rho}} \cong \mathbb{Z}_p[[T_1, T_2, T_3]]$$

The rest of this section will work towards a proof of this theorem. So for the remainder of the section assume that the hypothesis of the above theorem is true.

The main idea of the proof is to show that the dimension d_1 of the tangent space is equal to 3, and use the identity from the Global Euler Characteristic Formula (Theorem 42) to show that the deformation problem is unobstructed (i.e. $d_2 = 0$). From this we conclude using Theorem 31 that the universal deformation ring must be the power series ring in 3 variables over $\mathbb{Z}_p$, $\mathcal{R} \cong \mathbb{Z}_p[[T_1, T_2, T_3]]$.

To simplify notation, for M a H-module we write:

$$\mathcal{D}(M) := \dim \mathrm{Hom}_H(M, \mathrm{Ad}\,\bar{\rho})$$

From lemma 46 we have shown that the dimension of the tangent space is in fact equal to the dimension of $\dim_k t_{\boldsymbol{E}_{\bar{\rho}}} = \dim_k \mathrm{Hom}_H(\bar{P}, \mathrm{Ad}(\bar{\rho})) = \mathcal{D}(\bar{P})$, so we will compute that now. The main idea will be that the hypothesis of V and B being prime-to-adjoint will imply that many terms of this dimension calculation will go to zero.

Then in order to calculate the dimension of the tangent space, we wish to compute $\mathcal{D}(\bar{P})$. We prove a series of lemmas:

Lemma 48. We have an identity:

$$\mathcal{D}\left(\bar{P}\right) = \mathcal{D}\left(\mathbb{F}_p[H]\right) + \mathcal{D}\left(\bigoplus_{l\in S_0} \operatorname{Ind}_{H_l}^{H} \mu_p(K_l)\right) - \mathcal{D}\left(\mu_p(K)\right) - \mathcal{D}\left(\operatorname{Ind}_{H_\infty}^{H} \mathbb{F}_p\right) + \mathcal{D}\left(\mathbb{F}_p\right)$$

Proof. We first use the exact sequence given in theorem 38:

$$0 \to B_S \to \bar{E} \to \bigoplus_{v\in S_0} \bar{E}_v \to \bar{P} \to 0$$

Since B_S is prime to adjoint, we know that $\operatorname{Hom}_H(B_S, \operatorname{Ad}(\bar{\rho})) = 0$, so using the exact sequence we have an identity on dimensions:

$$\dim \operatorname{Hom}_H(\bar{P}, \operatorname{Ad}(\bar{\rho})) = \dim \operatorname{Hom}_H\left(\bigoplus_{v\in S_0} \bar{E}_v, \operatorname{Ad}(\bar{\rho})\right) - \dim \operatorname{Hom}_H(\bar{E}, \operatorname{Ad}(\bar{\rho})) \qquad (\star)$$

The key observation is that dimension of homomorphisms between H-modules is bilinear over direct sums of the modules. i.e.

$$\dim \operatorname{Hom}_H(X_1 \oplus X_2, Y) = \dim \operatorname{Hom}_H(X_1, Y) + \dim \operatorname{Hom}_H(X_2, Y)$$
$$\dim \operatorname{Hom}_H(X, Y_1 \oplus Y_2) = \dim \operatorname{Hom}_H(X, Y_1) + \dim \operatorname{Hom}_H(X, Y_2)$$

We apply this to the two decompositions of modules from theorem 39 to obtain the following identity on dimensions:

$$\mathcal{D}\left(\bigoplus_{v\in S} \bar{E}_v\right) = \mathcal{D}\left(\mathbb{F}_p[H]\right) + \mathcal{D}\left(\bigoplus_{l\in S_0} \operatorname{Ind}_{H_l}^{H} \mu_p(K_l)\right)$$
$$\mathcal{D}\left(\bar{E}\right) + \mathcal{D}\left(\mathbb{F}_p\right) = \mathcal{D}\left(\mu_p(K)\right) + \mathcal{D}\left(\operatorname{Ind}_{H_\infty}^{H} \mathbb{F}_p\right)$$

Substituting these two identities into $(\star)$, we obtain:

$$\mathcal{D}\left(\bar{P}\right) = \mathcal{D}\left(\mathbb{F}_p[H]\right) + \mathcal{D}\left(\bigoplus_{l\in S_0} \operatorname{Ind}_{H_l}^{H} \mu_p(K_l)\right) - \mathcal{D}\left(\mu_p(K)\right) - \mathcal{D}\left(\operatorname{Ind}_{H_\infty}^{H} \mathbb{F}_p\right) + \mathcal{D}\left(\mathbb{F}_p\right)$$

As desired. □

So we have decomposed $\mathcal{D}(\bar{P})$ into a sum of dimensions of modules, and we will now compute these terms separately:

Lemma 49.

$$\mathcal{D}(\mathbb{F}_p[H]) = \dim \operatorname{Hom}_H(\mathbb{F}_p[H], \operatorname{Ad}(\bar{\rho})) = 4$$

Proof. Note that $\mathbb{F}_p[H]$ is the regular representation of H, and from a result in representation theory, the multiplicity of an irreducible module in the regular representation is just the dimension of the irreducible module. But then for any H-module X we can simply decompose X into irreducible submodules $X = X_1 \oplus \cdots \oplus X_r$ and we have:

$$\dim \operatorname{Hom}_H(\mathbb{F}_p[H], X) = \sum_{i=1}^{r} \dim \operatorname{Hom}_H(\mathbb{F}_p[H], X_i) = \sum_{i=1}^{r} \dim X_i = \dim X$$

Thus this implies:

$$\dim \operatorname{Hom}_H(\mathbb{F}_p[H], \operatorname{Ad}(\bar{\rho})) = \dim \operatorname{Ad}(\bar{\rho}) = 4$$

□

Lemma 50.

$$\mathcal{D}\left(\operatorname{Ind}_{H_\infty}^{H}\mathbb{F}_p\right) = \dim\operatorname{Hom}_H\left(\operatorname{Ind}_{H_\infty}^{H}\mathbb{F}_p, \operatorname{Ad}(\bar{\rho})\right) = 2$$

and

$$\mathcal{D}\left(\mathbb{F}_p\right) = \dim\operatorname{Hom}_H\left(\mathbb{F}_p, \operatorname{Ad}(\bar{\rho})\right) = 1$$

Proof. Let σ be the complex conjugation in $G_{\mathbb{Q},S}$. Through a change of basis, we can assume without loss of generality that

$$\bar{\rho}(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

We can pick the following basis for the representation $\operatorname{Ad}(\bar{\rho})$:

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

And the conjugation action of $\bar{\rho}(\sigma)$ scales the 4 basis matrices by $1, 1, -1, -1$ respectively.

By Frobenius reciprocity we have the following identity:

$$\dim\operatorname{Hom}_H\left(\operatorname{Ind}_{H_\infty}^{H}\mathbb{F}_p, \operatorname{Ad}(\bar{\rho})\right) = \dim\operatorname{Hom}_{H_\infty}\left(\mathbb{F}_p, \operatorname{Res}_{H_\infty}^{H}\operatorname{Ad}(\bar{\rho})\right) = \dim_{\mathbb{F}_p}\operatorname{Ad}(\bar{\rho})^{H_\infty}$$

Since H_∞ is the subgroup of H generated by complex conjugation, and the action of $\bar{\rho}(\sigma)$ fixes exactly 2 of the basis matrices of $\operatorname{Ad}(\bar{\rho})$. This implies that

$$\mathcal{D}\left(\operatorname{Ind}_{H_\infty}^{H}\mathbb{F}_p\right) = \dim_{\mathbb{F}_p}\operatorname{Ad}(\bar{\rho})^{H_\infty} = 2$$

On the other hand, since $C_k(\bar{\rho}) = k$, the only matrices in $\operatorname{Ad}\bar{\rho}$ fixed under the H-action are the scalar matrices, so we conclude that:

$$\mathcal{D}\left(\mathbb{F}_p\right) = \dim\operatorname{Hom}_H\left(\mathbb{F}_p, \operatorname{Ad}(\bar{\rho})\right) = 1$$

□

Lemma 51.

$$\mathcal{D}\left(\bigoplus_{l\in S_0}\operatorname{Ind}_{H_l}^{H}\mu_p(K_l)\right) - \mathcal{D}\left(\mu_p(K)\right) = 0$$

Proof. The proof of this lemma uses the fact that

$$V = \operatorname{coker}\left(\mu_p(K) \to \bigoplus_{v\in S}\mu_p(K_v)\right)$$

is a prime-to-adjoint module.

We first make sense of how to interpret $\bigoplus_{v\in S}\mu_p(K_v)$ as an H-module. First we fix a prime $l \in S_0$ and consider the the direct sum over all primes $v \in S$ which lie over l of $\mu_p(K_v)$. Then given an element $h \in H$, the action of h is simply to permute the summands around, sending $\mu_p(K_v) \mapsto \mu_p(K_{h(v)})$. Thus for a fixed l, we have that is an H-module.

On the other hand, the induced module $\operatorname{Ind}_{H_l}^{H}\mu_p(K_l)$ is a direct sum of $g_i \otimes \mu_p(K_l)$ over a transversal $g_1, \cdots, g_s$ of H_l. It can be shown that we have an isomorphism of H-modules:

$$\operatorname{Ind}_{H_l}^{H}\mu_p(K_l) \cong \bigoplus_{v|l}\mu_p(K_v)$$

Taking the direct sum over all primes $l \in S_0$, we have the isomorphism:

$$\bigoplus_{l\in S_0}\operatorname{Ind}_{H_l}^{H}\mu_p(K_l) \cong \bigoplus_{l\in S_0}\bigoplus_{v|l}\mu_p(K_v) \cong \bigoplus_{v\in S}\mu_p(K_v)$$

Consider the map $\varphi : \mu_p(K) \to \bigoplus_{v\in S} \mu_p(K_v)$. The inclusion $\mu_p(K) \hookrightarrow \mu_p(K_v)$ is clearly injective, so this implies that φ is injective and so $\operatorname{Im}\varphi \cong \mu_p(K)$.

Finally we note that the cokernel V is the codomain of φ quotiented by its image. So we have an exact sequence:

$$0 \to \mu_p(K) \to \bigoplus_{v\in S} \mu_p(K_v) \to V \to 0$$

But using the fact that V is prime-to-adjoint, we conclude:

$$\begin{aligned} 0 &= \mathcal{D}(V) \\ &= \mathcal{D}\left(\bigoplus_{v\in S} \mu_p(K_v)\right) - \mathcal{D}(\mu_p(K)) \\ &= \mathcal{D}\left(\bigoplus_{l\in S_0} \operatorname{Ind}_{H_l}^{H} \mu_p(K_l)\right) - \mathcal{D}(\mu_p(K)) \end{aligned}$$

As desired. ∎

Now we show that this deformation problem has trivial obstruction:

Lemma 52. Under the hypotheses stated at the start of this subsection:

$$d_1 - d_2 = 3$$

Proof. From the corollary of the global Euler characteristic formula (Corollary 42) we have that:

$$\begin{aligned} d_1 - d_2 &= 1 + dn^2 - \sum_{v\in S_\infty} \dim H^0(G_{\mathbb{Q}_v}, \operatorname{Ad}(\bar\rho)) \\ &= 1 + 4 - \dim H^0(H_\infty, \operatorname{Ad}(\bar\rho)) \end{aligned}$$

Note that we substituted $d = 1, n = 2$ since we are looking at 2 dimensional representations of $G_{\mathbb{Q},S}$, and the sum over infinite places in the original formula has been replaced by a single term, since there is only one infinite place in $\mathbb{Q}$.

We know that the zeroth cohomology $H^0(H_\infty, \operatorname{Ad}(\bar\rho)) = \operatorname{Ad}(\bar\rho)^{H_\infty}$ is simply the elements in $\operatorname{Ad}(\bar\rho)$ which are fixed by the group H_∞.

By the proof of lemma 50 we have shown that H_∞ fixes a dimension 2 subspace of $\operatorname{Ad}(\bar\rho)$.

Thus $\dim H^0(H_\infty, \operatorname{Ad}(\bar\rho)) = \dim \operatorname{Ad}(\bar\rho)^{H_\infty} = 2$. And we conclude that

$$d_1 - d_2 = 1 + 4 - 2 = 3$$

∎

Finally we can conclude the section by finishing the proof to Theorem 47:

Proof of Theorem 47. We substitute the dimension calculations from lemmas 49, 50, and 51 into the identity given in lemma 48:

$$\begin{aligned} d_1 &= \dim \operatorname{Hom}_H(\bar P, \operatorname{Ad}(\bar\rho)) \\ &= \mathcal{D}\left(\bar P\right) \\ &= \mathcal{D}\left(\mathbb{F}_p[H]\right) + \mathcal{D}\left(\bigoplus_{l\in S_0} \operatorname{Ind}_{H_l}^{H} \mu_p(K_l)\right) - \mathcal{D}\left(\mu_p(K)\right) - \mathcal{D}\left(\operatorname{Ind}_{H_\infty}^{H} \mathbb{F}_p\right) + \mathcal{D}\left(\mathbb{F}_p\right) \\ &= 4 + 0 - 2 + 1 \\ &= 3 \end{aligned}$$

But by lemma 52 we know that $d_1 - d_2 = 3$. Since d_2 is non-negative, this implies that $d_2 = 0$.

Finally we conclude from Theorem 31 that the deformation ring is simply equal to the power series ring in d_1 variables:

$$\mathcal{R} \cong \mathbb{Z}_p[[T_1, T_2, T_3]]$$

□

6 Conclusion

Over this essay we proved the existence of the Universal Deformation Ring following Mazur's paper, and deduced some properties of the Universal Deformation Ring via the tangent space of the deformation functor. We also computed the Universal Deformation Ring in several specific cases.

One of the hypotheses required in the statement of theorem 47 is that V and B has to be prime-to adjoint. While this condition greatly simplified the computation of the dimension of the tangent space, the condition imposed does seem a bit artificial. A natural next step would be to attempt to find residual representations $\bar{\rho}$ which indeed satisfy the hypotheses.

References

[Sch68] M. Schlessinger. "Functors of Artin rings". In: *Transactions of the American Mathematical Society* 130 (1968), pp. 208–222.

[Koc70] H. Koch. "Endliche Globale Körper". In: *Galoissche Theorie der p-Erweiterungen*. Ed. by W. Gröbner and H. Reichardt. Berlin, Heidelberg: Springer Berlin Heidelberg, 1970, pp. 106–125. ISBN: 978-3-642-92997-7. DOI: 10.1007/978-3-642-92997-7_12. URL: https://doi.org/10.1007/978-3-642-92997-7_12.

[BM89] Nigel Boston and Barry Mazur. "Explicit Universal Deformations of Galois Representations". In: *Advanced Studies in Pure Mathematic* (1989), pp. 1–12.

[Maz89] B. Mazur. "Deforming Galois Representations". In: *Galois Groups over* $\mathbb{Q}$. 1989, pp. 385–437.

[Bos91] Nigel Boston. "Explicit deformation of Galois representations". In: *Inventiones mathematicae* 103 (1991), pp. 181–196.

[Rob96] Derek J. S. Robinson. "Representations of Groups". In: *A Course in the Theory of Groups*. New York, NY: Springer New York, 1996, pp. 213–251. ISBN: 978-1-4419-8594-1. DOI: 10.1007/978-1-4419-8594-1_8. URL: https://doi.org/10.1007/978-1-4419-8594-1_8.

[Mil06] J.S. Milne. *Arithmetic Duality Theorems*. Second. BookSurge, LLC, 2006, pp. viii+339. ISBN: 1-4196-4274-X.

[Gou08] Fernando Gouvêa. "Deformations of Galois representations". In: Feb. 2008, pp. 233–406. ISBN: 9780821844489. DOI: 10.1090/pcms/009/05.

[Tia14] Yichao Tian. *Lectures on algebraic number theory*. 2014. URL: http://www.mcm.ac.cn/people/members/202108/W020210820570287081597.pdf.

[Mil20] J.S. Milne. *Class Field Theory (v4.03)*. 2020. URL: https://www.jmilne.org/math/CourseNotes/CFT.pdf.