BASE CHANGE AND GALOIS DEFORMATION

HARUZO HIDA

Contents

Date: October 30, 2017.
The author is partially supported by the NSF grant: DMS 0753991 and DMS 0854949.

1. Introduction

In this course, we discuss the following four topics:

(1) Basics of Galois deformation theory (and representation theory of pro-finite groups);
(2) Relation of deformation rings for a given starting representation restricted to open subgroups;
(3) Introduction to Galois cohomology;
(4) "$R = T$" theorem (in [W95]), applications and open questions (if time allows).

The purpose is to introduce the audience to base-change theorems of deformation rings relative to Galois extension $F/\mathbb{Q}$ and to show how such theorems have been useful in establishing base change in the automorphic side. Alongside, we describe p-adic representation theory of p-profinite groups. At the end, we describe some open problems on deformation rings and its relation to L-values.

We fix a prime $p > 2$, an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and field embeddings $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ and $i_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Let F be a number field, and S be a finite set of primes of F and F^S/F be the maximal field extension inside $\overline{\mathbb{Q}}$ unramified outside p and ∞. Put $\mathfrak{G}_F = \mathrm{Gal}(F^S/F)$. Usually S is made of primes above p (but not always. In this note, W is a discrete valuation ring over the p-adic integer ring $\mathbb{Z}_p$ with residue field $\mathbb{F}$. For a local ring A, its maimal ideal is denoted by $\mathfrak{m}_A$.

2. Galois deformation rings

We prove existence of the universal Galois deformation rings.

2.1. **The Iwasawa algebra as a deformation ring.** We can interpret the Iwasawa algebra Λ as a universal Galois deformation ring. Fix a continuous character $\overline{\psi} : \mathfrak{G}_{\mathbb{Q}} \to \mathbb{F}^\times$. We write CL_W for the category of p-profinite local W-algebras A with $A/\mathfrak{m}_A = \mathbb{F}$. A character $\rho : \mathfrak{G}_{\mathbb{Q}} \to A^\times$ for $A \in CL_W$ is called a W-deformation (or just simply a deformation) of $\overline{\psi}$ if $(\rho \mod \mathfrak{m}_A) = \overline{\psi}$. A couple $(\mathcal{R}, \boldsymbol{\rho})$ made of an object $\mathcal{R}$ of CL_W and a character $\boldsymbol{\rho} : \mathfrak{G}_F \to \mathcal{R}^\times$ is called a *universal couple* for ψ if for any deformation $\rho : \mathfrak{G}_F \to A$ of $\overline{\psi}$, we have a unique morphism $\phi_\rho : \mathcal{R} \to A$ in CL_W (so it is a local W-algebra homomorphism) such that $\phi_\rho \circ \boldsymbol{\rho} = \rho$. By the universality, if exists, the couple $(\mathcal{R}, \boldsymbol{\rho})$ is determined uniquely up to isomorphisms. The ring $\mathcal{R}$ is called the universal deformation ring and $\boldsymbol{\rho}$ is called the universal deformation of $\overline{\psi}$.

Consider the group of p-power roots of unity $\mu_{p^\infty} = \bigcup_n \mu_{p^n} \subset \overline{\mathbb{Q}}^\times$. Then writing $\zeta_n = \exp\left(\frac{2\pi i}{p^n}\right)$, we can identify the group μ_{p^n} with $\mathbb{Z}/p^n\mathbb{Z}$ by $\zeta_n^m \leftrightarrow (m \mod p^n)$. The Galois action of $\sigma \in \mathfrak{G}_{\mathbb{Q}}$ sends ζ_n to $\zeta_n^{\nu_n(\sigma)}$ for $\nu_n(\sigma) \in \mathbb{Z}/p^n\mathbb{Z}$. Then $\mathfrak{G}_{\mathbb{Q}}$ acts on $\mathbb{Z}_p(1) = \varprojlim_n \mu_{p^n}$ by a character $\nu := \varprojlim_n \nu_n : \mathfrak{G}_{\mathbb{Q}} \to \mathbb{Z}_p^\times$, which is called the p-adic cyclotomic character. The logarithm power series $\log(1+x) = \sum_{n=1}^\infty -\frac{(-x)^n}{n}$ and exponential power series $\exp(x) = \sum_{n=0}^\infty \frac{x^n}{n!}$ converges absolutely p-adically on $p\mathbb{Z}_p$. Note that $\mathbb{Z}_p^\times = \mu_{p-1} \times \Gamma$ for $\Gamma = 1 + p\mathbb{Z}_p$ by $\mathbb{Z}_p^\times \mapsto (\omega(z) = \lim_{n\to\infty} z^{p^n}, \omega(z)^{-1}z) \in \mu_{p-1} \times \Gamma$. We define $\log_p : \mathbb{Z}_p^\times \to \Gamma$ by $\log_p(\zeta, s) = \log(s) \in p\mathbb{Z}_p$ for $\zeta\mu_{p-1}$ and $s \in 1 + p\mathbb{Z}_p = \Gamma$.

Exercise 2.1. *Compute the radius of convergence of* $\exp(x)$ *and* $\log(x)$ *in* $\mathbb{C}_p$ *under the standard* p*-adic norm* $|\cdot|_p$ *with* $|p|_p = p^{-1}$*.*

Let $\Lambda_W = W[[X]]$ (a one variable power series ring with coefficients in W) and $\Lambda = \mathbb{Z}_p[[X]]$. Since $s \mapsto \binom{s}{n} = \frac{(s-n+1)(s-n+2)\cdots s}{n!}$ has integer valued on the set $\mathbb{Z}_+$ of positive integers and p-adically continuous, it extends to a polynomial map $\mathbb{Z}_p \ni s \mapsto \binom{s}{n} \in \mathbb{Z}_p$. Then $(1+X)^s = \sum_{n=0}^{\infty} \binom{s}{n} X^n \in \mathbb{Z}_p$, getting an additive character $\mathbb{Z}_p \ni s \mapsto (1+X)^s \in \Lambda^\times$. Let $\gamma = 1+p$; so, $\Gamma = \gamma^{\mathbb{Z}_p}$. Consider the character $\kappa : \mathfrak{G}_\mathbb{Q} \to \Lambda^\times$ given by $\kappa(\sigma) = (1+X)^{\log_p(\nu_p(\sigma))/\log_p(\gamma)}$.

Exercise 2.2. *Prove* $1 + p\mathbb{Z}_p = \gamma^{\mathbb{Z}_p}$*.*

Since $\mathbb{Q}[\mu_{p^\infty}]$ is the maximal abelian extension of $\mathbb{Q}$ unramified outside p and ∞ by class field theory (or else, by the theorem of Kronecker-Weber), we have $\mathfrak{G}_\mathbb{Q}/\overline{[\mathfrak{G}_\mathbb{Q}, \mathfrak{G}_\mathbb{Q}]} = \mathrm{Gal}(\mathbb{Q}[\mu_{p^\infty}]/\mathbb{Q})$. On the other hand, we identified $\mathrm{Gal}(\mathbb{Q}[\mu_{p^\infty}]/\mathbb{Q})$ with $\mathbb{Z}_p^\times$ by ν_p. We write $[z] \in \mathrm{Gal}(\mathbb{Q}[\mu_{p^\infty}]/\mathbb{Q})$ for automorphism of $\mathbb{Q}[\mu_{p^\infty}]$ with $\nu_p([z]) = z$. Then we have $\kappa([\gamma^s]) = (1+X)^s$. Since $\overline{\psi}$ has values in $\mathbb{F}_p^\times \cong \mu_{p-1}$, we may identify the character $\overline{\psi}$ with a character $\psi : \mathfrak{G}_\mathbb{Q} \to \mu_{p-1} \subset \mathbb{Z}_p^\times$. Define $\boldsymbol{\psi} : \mathfrak{G}_\mathbb{Q} \to \Lambda^\times$ by $\boldsymbol{\psi}(\sigma) := \kappa(\sigma)\psi(\sigma)$; then $\boldsymbol{\psi} \equiv \overline{\psi} \mod \mathfrak{m}_\Lambda$, where $\mathfrak{m}_\Lambda$ is the maximal ideal of Λ; so, $\mathfrak{m}_\Lambda = (p, X)$. Thus $(\Lambda, \boldsymbol{\psi})$ is a deformation of $(\mathbb{F}, \overline{\psi})$ with $\boldsymbol{\psi}([\gamma]) = (1+X)$.

Proposition 2.3. *The couple* $(\Lambda_W = W[[X]], \boldsymbol{\psi})$ *(for a variable* X*) is the universal couple for* $\overline{\psi}$*.*

Proof. Since $\mathbb{Q}[\mu_{p^\infty}]$ is the maximal abelian extension of $\mathbb{Q}$ unramified outside p and ∞, each deformation $\rho : \mathfrak{G}_\mathbb{Q} \to A^\times$ factors through $\mathrm{Gal}(Q[\mu_{p^\infty}]/\mathbb{Q}) = \Gamma \times \mathrm{Gal}(\mathbb{Q}[\mu_p]/\mathbb{Q})$. Then the character ρ is determined by $\rho(\gamma)$, because $\rho|_{\mathbb{Q}[\mu_p]}$ is given by ψ and $\Gamma = \gamma^{\mathbb{Z}_p}$. Then we have $\phi_\rho : \Lambda_W = W[[X]] \to A$ by sending X to $\rho(\gamma) - 1$, and we have $\phi_\rho \circ \boldsymbol{\psi} = \rho$. □

For a given n-dimensional representation $\overline{\rho} : \mathfrak{G}_F \to GL_n(\mathbb{F})$, a deformation $\rho : \mathfrak{G}_F \to GL_n(R)$ is a continuous representation with $\rho \mod \mathfrak{m}_R \cong \overline{\rho}$. Two deformations $\rho, \rho' : \mathfrak{G}_F \to GL_n(R)$ for $R \in CL_W$ is equivalent, if there exists an invertible matrix $x \in GL_n(R)$ such that $x\rho(\sigma)x^{-1} = \rho'(\sigma)$ for all $\sigma \in \mathfrak{G}_F$. We write $\rho \sim \rho'$ if ρ and ρ' are equivalent. A couple $(R_{\overline{\rho}}, \boldsymbol{\rho})$ for a deformation $\boldsymbol{\rho} : \mathfrak{G}_F \to GL_n(R_{\overline{\rho}})$ is called a universal couple over W, if for any given deformation $\rho : \mathfrak{G}_F \to GL_n(R)$ there exists a unique W-algebra homomorphism $\iota_\rho : R_{\overline{\rho}} \to R$ such that $\iota_\rho \circ \boldsymbol{\rho} \sim \rho$.

2.2. **Pseudo representations.** In order to show the existence of the universal deformation ring, pseudo representations are very useful. We recall the definition of pseudo representations (due to Wiles) when $n = 2$. See [MFG] §2.2.2 for a higher dimensional generalization due to R. Taylor.

In this subsection, the coefficient ring A is always an object in CL_W with maximal ideal $\mathfrak{m}_A$. We write $\mathbb{F} = A/\mathfrak{m}_A$. Note that 2 is invertible in A as $p > 2$. We would like to characterize the trace of a representation of a group G.

We describe in detail traces of degree 2 representations $\rho : G \to GL_2(A)$ when G contains c such that $c^2 = 1$ and $\det \rho(c) = -1$. Let $V(\rho) = A^2$ on which G acts by ρ. Since 2 is invertible in A, we know that $V = V(\rho) = V_+ \oplus V_-$ for $V_\pm = \frac{1 \pm c}{2} V$. For $\overline{\rho} = \rho \mod \mathfrak{m}_A$, we write $\overline{V} = V(\overline{\rho})$. Then similarly as above, $\overline{V} = \overline{V}_+ \oplus \overline{V}_-$ and

$\overline{V}_\pm = V_\pm/\mathfrak{m}_A V_\pm$. Since $\dim_{\mathbb{F}} \overline{V} = 2$ and $\det \overline{\rho}(c) = -1$, $\dim_{\mathbb{F}} \overline{V}_\pm = 1$. This shows that $\overline{V}_\pm = \mathbb{F}\overline{v}_\pm$ for $\overline{v}_\pm \in \overline{V}_\pm$. Take $v_\pm \in V_\pm$ such that $v_\pm \mod \mathfrak{m}_A V_\pm = \overline{v}_\pm$, and define $\phi_\pm : A \to V_\pm$ by $\phi(a) = av_\pm$. Then $\phi_\pm \mod \mathfrak{m}_A V$ is surjective by Nakayama's lemma. Note that $\phi_\pm : A \cong V_\pm$ as A-modules. In other words, $\{v_-, v_+\}$ is an A–base of V. We write $\rho(r) = \left(\begin{smallmatrix} a(r) & b(r) \\ c(r) & d(r) \end{smallmatrix}\right)$ with respect to this base. Thus $\rho(c) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Define another function $x : G \times G \to A$ by $x(r,s) = b(r)c(s)$. Then we have

(W1) $a(rs) = a(r)a(s) + x(r,s)$, $d(rs) = d(r)d(s) + x(s,r)$ and
$x(rs,tu) = a(r)a(u)x(s,t) + a(u)d(s)x(r,t) + a(r)d(t)x(s,u) + d(s)d(t)x(r,u)$;

(W2) $a(1) = d(1) = d(c) = 1$, $a(c) = -1$ and $x(r,s) = x(s,t) = 0$ if $s = 1, c$;

(W3) $$x(r,s)x(t,u) = x(r,u)x(t,s).$$

These are easy to check: We have

$$\begin{pmatrix} a(r) & b(r) \\ c(r) & d(r) \end{pmatrix} \begin{pmatrix} a(s) & b(s) \\ c(s) & d(s) \end{pmatrix} = \begin{pmatrix} a(rs) & b(rs) \\ c(rs) & d(rs) \end{pmatrix}.$$

Then by computation, $a(rs) = a(r)a(s) + b(r)c(s) = a(r)a(s) + x(r,s)$. Similarly, we have $b(rs) = a(r)b(s) + b(r)d(s)$ and $c(rs) = c(r)a(s) + d(r)c(s)$. Thus

$$\begin{aligned} x(rs,tu) &= b(rs)c(tu) = (a(r)b(s) + b(r)d(s))(c(t)a(u) + d(t)c(u)) \\ &= a(r)a(u)x(s,t) + a(r)d(t)x(s,u) + a(u)d(s)x(r,t) + d(s)d(t)x(r,u). \end{aligned}$$

A triple $\{a,d,x\}$ satisfying the three conditions (W1-3) is called a *pseudo representation* of Wiles of (G,c). For each pseudo-representation $\tau = \{a,d,x\}$, we define

$$\mathrm{Tr}(\tau)(r) = a(r) + d(r) \quad \text{and} \quad \det(\tau)(r) = a(r)d(r) - x(r,r).$$

By a direct computation using (W1-3), we see

$$a(r) = \frac{1}{2}(\mathrm{Tr}(\tau)(r) - \mathrm{Tr}(\tau)(rc)), \quad d(r) = \frac{1}{2}(\mathrm{Tr}(\tau)(r) + \mathrm{Tr}(\tau)(rc))$$

and

$$x(r,s) = a(rs) - a(r)a(s), \quad \det(\tau)(rs) = \det(\tau)(r)\det(\tau)(s).$$

Thus the pseudo-representation τ is determined by the trace of τ as long as 2 is invertible in A.

Proposition 2.4 (A. Wiles, 1988)**.** *Let G be a group and $R = A[G]$. Let $\tau = \{a,d,x\}$ be a pseudo-representation (of Wiles) of (G,c). Suppose either that there exists at least one pair $(r,s) \in G \times G$ such that $x(r,s) \in A^\times$ or that $x(r,s) = 0$ for all $r,s \in G$. Then there exists a representation $\rho : R \to M_2(A)$ such that* $\mathrm{Tr}(\rho) = \mathrm{Tr}(\tau)$ *and* $\det(\rho) = \det(\tau)$ *on G. If A is a topological ring, G is a topological group and all maps in τ are continuous on G, then ρ is a continuous representation of G into $GL_2(A)$ under the topology on $GL_2(A)$ induced by the product topology on $M_2(A)$.*

Proof. When $x(r,s) = 0$ for all $r,s \in G$, we see from (W1) that $a,d : G \to A$ satisfies $a(rs) = a(r)a(s)$ and $d(rs) = d(r)d(s)$. Thus a,d are characters of G, and we define $\rho : G \to GL_2(A)$ by $\rho(g) = \left(\begin{smallmatrix} a(g) & 0 \\ 0 & d(g) \end{smallmatrix}\right)$, which satisfies the required property.

We now suppose $x(r,s) \in A^\times$ for $r,s \in G$. Then we define $b(g) = x(g,s)/x(r,s)$ and $c(g) = x(r,g)$ for $g \in G$. Then by (W3), $b(g)c(h) = x(r,h)x(g,s)/x(r,s) =$

$x(g,h)$. Put $\rho(g) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$. By (W2), we see that $\rho(1)$ is the identity matrix and $\rho(c) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. By computation,

$$\rho(g)\rho(h) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix} \begin{pmatrix} a(h) & b(h) \\ c(h) & d(h) \end{pmatrix} = \begin{pmatrix} a(g)a(h)+b(g)c(h) & a(g)b(h)+b(g)d(h) \\ c(g)a(h)+d(g)c(h) & d(g)d(h)+c(g)b(h) \end{pmatrix}.$$

By (W1), $a(gh) = a(g)a(h) + x(g,h) = a(g)a(h) + b(g)c(h)$ and $d(gh) = d(g)d(h) + x(h,g) = d(g)d(h) + b(h)c(g)$. Now let us look at the lower left corner:

$$c(g)a(h) + d(g)c(h) = x(r,g)a(h) + d(g)x(r,h).$$

Now apply (W1) to $(1,r,g,h)$ in place of (r,s,t,u), and we get

$$c(gh) = x(r,gh) = a(h)x(r,g) + d(g)x(r,h),$$

because $x(1,g) = x(1,h) = 0$. As for the upper right corner, we apply (W1) to $(g,h,1,s)$ in place of (r,s,t,u). Then we get

$$b(gh)x(r,s) = x(gh,s) = a(g)x(h,s) + d(h)x(g,s) = (a(g)b(h) + d(h)b(g))x(r,s),$$

which shows that $\rho(gh) = \rho(g)\rho(h)$. We now extends ρ linearly to $R = A[G]$. This shows the first assertion. The continuity of ρ follows from the continuity of each entries, which follows from the continuity of τ. □

Start from an absolutely irreducible representation $\overline{\rho} : G \to GL_n(\mathbb{F})$. Here a representation of a group into $GL_n(K)$ for a field K is called *absolutely irreducible* if it is irreducible as a representation into $GL_n(\overline{K})$ for an algebraic closure $\overline{K}$ of K.

Exercise 2.5. (1) *Give an example of irreducible representations of a group G into $GL_2(\mathbb{Q})$ which is not absolutely irreducible.*

(2) *Show that if a representation $\rho : G \to GL_n(K)$ is absolutely irreducible, the K-subalgebra generated by $\rho(g)$ for all $g \in G$ coincides with $M_n(K)$.*

(3) *If A is a local ring with residue field $\mathbb{F}$ with a representation $\rho : G \to GL_n(A)$ such that $\overline{\rho} = (\rho \mod \mathfrak{m}_A)$ is absolutely irreducible, show that the subalgebra generated over A by $\rho(g)$ for all $g \in G$ is equal to $M_n(A)$.*

We fix an absolutely irreducible representation $\overline{\rho} : G \to GL_2(\mathbb{F})$ with $\det(\overline{\rho})(c) = -1$. If we have a representation $\rho : G \to GL_2(A)$ with $\rho \mod \mathfrak{m}_A \sim \overline{\rho}$, then $\det(\rho(c)) \equiv \det(\overline{\rho}(c)) \equiv -1 \mod \mathfrak{m}_A$. Since $c^2 = 1$, if 2 is invertible in A ($\Leftrightarrow$ the characteristic of $\mathbb{F}$ is different from 2), $\det(\rho(c)) = -1$. This is a requirement to have a pseudo-representation τ_ρ of Wiles associated to ρ. Since $\overline{\rho}$ is absolutely irreducible, we find $r, s \in G$ such that $b(r) \not\equiv 0 \mod \mathfrak{m}_A$ and $c(s) \not\equiv 0 \mod \mathfrak{m}_A$. Thus τ_ρ satisfies the condition of Proposition 2.4. Conversely if we have a pseudo representation $\tau : G \to A$ such that $\tau \equiv \overline{\tau} \mod \mathfrak{m}_A$ for $\overline{\tau} = \tau_{\overline{\rho}}$, again we find $r, s \in G$ such that $x(r,s) \in A^\times$. The correspondence $\rho \mapsto \tau_\rho$ induces a bijection:

$$\{\rho : G \to GL_2(A) : \text{representation} | \rho \mod \mathfrak{m}_A \sim \overline{\rho}\} / \sim \leftrightarrow \{\tau : G \to A : \text{pseudo-representation} | \tau \mod \mathfrak{m}_A = \overline{\tau}\}, \tag{2.1}$$

where $\overline{\tau} = \tau_{\overline{\rho}}$ and "$\sim$" is the conjugation under $GL_2(A)$. The map is surjective by Proposition 2.4 combined with Proposition 2.6 and one to one by Proposition 2.6 we admit, because a pseudo-representation is determined by its trace.

Proposition 2.6 (Carayol, Serre, 1994)**.** *Let A be an pro-artinian local ring with finite residue field $\mathbb{F}$. Let $R = A[G]$ for a profinite group G. Let $\rho : R \to M_n(A)$ and $\rho' : R \to M_{n'}(A)$ be two continuous representations. If $\overline{\rho} = \rho \mod \mathfrak{m}_A$ is absolutely irreducible and $\mathrm{Tr}(\rho(\sigma)) = \mathrm{Tr}(\rho'(\sigma))$ for all $\sigma \in G$, then $\rho \sim \rho'$.*

See [MFG] Proposition 2.13 for a proof of this result.

2.3. **Two dimensional non-abelian universal deformations.** We fix an absolutely irreducible representation $\overline{\rho} : G \to GL_2(\mathbb{F})$ for a profinite group G. Assume that we have $c \in G$ with $c^2 = 1$ and $\det(\overline{\rho}(c)) = -1$. First we consider a universal pseudo-representation. Let $\overline{\tau} = (\overline{a}, \overline{d}, \overline{x})$ be the pseudo representation associated to $\overline{\rho}$. A couple consisting of an object $R_{\overline{\tau}} \in CL_W$ and a pseudo-representation $T = (A, D, X) : G \to R_{\overline{\tau}}$ is called a universal couple if the following universality condition is satisfied:

(univ) *For each pseudo-representation $\tau : G \to A$ ($A \in CL_W$) with $\tau \cong \overline{\tau}$ mod $\mathfrak{m}_A$, there exists a unique W–algebra homomorphism $\iota_\tau : R_{\overline{\tau}} \to A$ such that*
$$\tau = \iota_\tau \circ T.$$

We now show the existence of $(R_{\overline{\tau}}, T)$ for a profinite group G. First suppose G is a finite group. Let $\omega : W^\times \to \mu_{q-1}(W)$ be the Teichmüller character, that is,
$$\omega(x) = \lim_{n\to\infty} x^{q^n} \quad (q = |\mathbb{F}| = |W/\mathfrak{m}_W|).$$
We also consider the following isomorphism: $\mu_{q-1}(W) \ni \zeta \mapsto \zeta \mod \mathfrak{m}_W \in \mathbb{F}^\times$. We write $\varphi : \mathbb{F}^\times \to \mu_{q-1}(W) \subset W^\times$ for the inverse of the above map. We look at the power series ring: $\mathbf{\Lambda} = \mathbf{\Lambda}_G = W[[A_g, D_h, X_{(g,h)}; g, h \in G]]$. We put
$$A(g) = A_g + \varphi(\overline{a}(g)),\ D(g) = D_g + \varphi(\overline{d}(g)) \ \text{ and } \ X(g,h) = X_{g,h} + \varphi(\overline{x}(g,h)).$$
We construct the ideal I so that
$$T = (g \mapsto A(g) \mod I, g \mapsto D(g) \mod I, (g,h) \mapsto X(g,h) \mod I)$$
becomes the universal pseudo representation. Thus we consider the ideal I of $\mathbf{\Lambda}$ generated by the elements of the following type:

(w1) $A(rs) - (A(r)A(s) + X(r,s))$, $D(rs) - (D(r)D(s) + X(s,r))$ and
$X(rs,tu) - (A(r)A(u)X(s,t) + A(u)D(s)X(r,t) + A(r)D(t)X(s,u) + D(s)D(t)X(r,u))$;

(w2) $A(1) - 1 = A_1$, $D(1) - 1 = D_1$, $D(c) - 1 = D_c$, $A(c) + 1 = A_c$ and $X(r,s) - X(s,t)$ if $s = 1, c$;

(w3) $$X(r,s)X(t,u) - X(r,u)X(t,s).$$

Then we put $R_{\overline{\tau}} = \mathbf{\Lambda}/I$ and define $T = (A(g), D(h), X(g,h)) \mod I$. By the above definition, T is a pseudo-representation with $T \mod \mathfrak{m}_{R_{\overline{\tau}}} = \overline{\tau}$. For a pseudo representation $\tau = (a, d, x) : G \to A$ with $\tau \equiv \overline{\tau} \mod \mathfrak{m}_A$, we define $\iota_\tau : \mathbf{\Lambda} \to A$ with $\iota_\tau(f) \in A$ for a power series $f(A_g, D_h, X_{(g,h)}) \in \mathbf{\Lambda}$ by
$$\begin{aligned} f(A_g, D_h, X_{(g,h)}) &\mapsto f(\tau(g) - \varphi(\overline{\tau}(g))) \\ &= f(a(g) - \varphi(\overline{a}(g)), d(h) - \varphi(\overline{d}(h)), x(g,h) - \varphi(\overline{x}(g,h))). \end{aligned}$$
Since f is a power series of $A_g, D_h, X_{g,h}$ and $\tau(g) - \varphi(\overline{\tau}(g)) \in \mathfrak{m}_A$, the value $f(\tau(g) - \varphi(\overline{\tau}(g)))$ is well defined. Let us see this. If A is artinian, a sufficiently high power $\mathfrak{m}_A^N$ vanishes. Thus if the monomial of the variables $A_g, D_h, X_{(g,h)}$ is of degree higher than N, it is sent to 0 via ι_τ, and $f(\tau(g) - \varphi(\overline{\tau}(g)))$ is a finite sum of terms of degree $\leq N$. If A is pro-artinian, the morphism ι_τ is just the projective limit of the corresponding ones well defined for artinian quotients. By the axioms of pseudo-representation (W1-3), $\iota_\tau(I) = 0$, and hence ι_τ factors through $R_{\overline{\tau}}$. The

uniqueness of ι_τ follows from the fact that $\{A_g, D_h, X_{(g,h)}|g, h \in G\}$ topologically generates $R_{\overline{\tau}}$.

Now assume that $G = \varprojlim_N G/N$ for open normal subgroups N (so, G/N is finite). Since $\mathrm{Ker}(\overline{\rho})$ is an open subgroup of G, we may assume that N runs over subgroups of $\mathrm{Ker}(\overline{\rho})$. Since $\overline{\rho}$ factors through $G/\mathrm{Ker}(\overline{\rho})$, $\mathrm{Tr}(\overline{\tau}) = \mathrm{Tr}(\overline{\rho})$ factors through G/N. Therefore we can think of the universal couple $(R^N_{\overline{\tau}}, T_N)$ for $(G/N, \overline{\tau})$. If $N \subset N'$, the algebra homomorphism $\mathbf{\Lambda}_{G/N} \to \mathbf{\Lambda}_{G/N'}$ taking $(A_{gN}, D_{hN}, X_{(gN,hN)})$ to $(A_{gN'}, D_{hN'}, X_{(gN',hN')})$ induces a surjective W–algebra homomorphism $\pi_{N,N'} : R^N_{\overline{\tau}} \to R^{N'}_{\overline{\tau}}$ with $\pi_{N,N'} \circ T_N = T_{N'}$. We then define $T = \varprojlim_N T_N$ and $R_{\overline{\tau}} = \varprojlim_N R^N_{\overline{\tau}}$. If $\tau : G \to A$ is a pseudo representation, by Proposition 2.4, we have the associated representation $\rho : G \to GL_2(A)$ such that $\mathrm{Tr}(\tau) = \mathrm{Tr}(\rho)$. If A is artinian, then $GL_2(A)$ is a finite group, and hence ρ and $\mathrm{Tr}(\tau) = \mathrm{Tr}(\rho)$ factors through G/N for a sufficiently small open normal subgroup N. Thus we have $\iota_\tau : R_{\overline{\tau}} \xrightarrow{\pi_N} R^N_{\overline{\tau}} \xrightarrow{\iota^N_\tau} A$ such that $\iota_\tau \circ T = \tau$. Since $(A(g), D(h), X(g,h))$ generates topologically $R_{\overline{\tau}}$, ι_τ is uniquely determined.

Writing $\boldsymbol{\rho}$ for the representation $\boldsymbol{\rho} : G \to GL_n(R_{\overline{\tau}})$ associated to the universal pseudo representation T and rewriting $R_{\overline{\rho}} = R_{\overline{\tau}}$, for $n = 2$, we have proven by (2.1) the following theorem, which was first proven by Mazur [M89] in in 1989 (see [MFG] Theorem 2.26 for a proof valid for any n).

Theorem 2.7 (Mazur)**.** *Suppose that $\overline{\rho} : G \to GL_n(\mathbb{F})$ is absolutely irreducible. Then there exists the universal deformation ring $R_{\overline{\rho}}$ in CL_W and a universal deformation $\boldsymbol{\rho} : G \to GL_n(R_{\overline{\rho}})$. If we write $\overline{\tau}$ for the pseudo representation associated to $\overline{\rho}$, then for the universal pseudo-representation $T : G \to R_{\overline{\tau}}$ deforming $\overline{\tau}$, we have a canonical isomorphism of W–algebras $\iota : R_{\overline{\rho}} \cong R_{\overline{\tau}}$ such that $\iota \circ \mathrm{Tr}(\boldsymbol{\rho}) = \mathrm{Tr}(T)$.*

Let $(R_{\overline{\rho}}, \boldsymbol{\rho})$ be the universal couple for an absolutely irreducible representation $\overline{\rho} : \mathfrak{G}_{\mathbb{Q}} \to GL_n(\mathbb{F})$. We can also think of $(R_{\det(\overline{\rho})}, \nu)$, which is the universal couple for the character $\det(\overline{\rho}) : \mathfrak{G}_{\mathbb{Q}} \to GL_1(\mathbb{F}) = \mathbb{F}^\times$. As we have studied already, $R_{\det(\overline{\rho})} \cong W[[\Gamma]] = \Lambda_W$. Note that $\det(\boldsymbol{\rho}) : \mathfrak{G}_{\mathbb{Q}} \to GL_1(R_{\overline{\rho}})$ satisfies $\det(\boldsymbol{\rho}) \bmod \mathfrak{m}_{R_{\overline{\rho}}} = \det(\overline{\rho})$. Thus $\det(\boldsymbol{\rho})$ is a deformation of $\det(\overline{\rho})$, and hence by the universality of $(\Lambda_W \cong R_{\det(\overline{\rho})}, \nu)$, there is a unique W–algebra homomorphism $\iota : \Lambda_W \to R_{\overline{\rho}}$ such that $\iota \circ \nu = \det(\boldsymbol{\rho})$. In this way, $R_{\overline{\rho}}$ becomes naturally a Λ_W–algebra via ι.

Corollary 2.8. *Let the notation and the assumption be as above and as in the above theorem. Then the universal ring $R_{\overline{\rho}}$ is canonically an algebra over the Iwasawa algebra $\Lambda_W = W[[\Gamma]]$.*

When $G = \mathfrak{G}_{\mathbb{Q}}$ (or more generally, $\mathfrak{G}_F$), it is known that $R_{\overline{\rho}}$ is noetherian (cf. [MFG] Proposition 2.30). We will come back to this point after relating certain Selmer groups with the universal deformation ring.

2.4. **Ordinary universal deformation rings.** Let $\overline{\rho} : \mathfrak{G}_{\mathbb{Q}} \to GL_2(\mathbb{F})$ be a Galois representation with coefficients in a finite field $\mathbb{F}$ of characteristic p. We consider the following condition for a subfield F of $\mathbb{Q}^{(p)}$:

- (ai$_F$) $\overline{\rho}$ restricted to $\mathfrak{G}_F$ is absolutely irreducible;
- (rg$_p$) Suppose $\overline{\rho}|_{D_p} \cong \left(\begin{smallmatrix} \overline{\epsilon} & * \\ 0 & \overline{\delta} \end{smallmatrix}\right)$ for each decomposition subgroup D_p at p in $\mathfrak{G}_{\mathbb{Q}}$ and that $\overline{\epsilon}$ is ramified with unramified $\overline{\delta}$ (so, $\overline{\epsilon} \neq \overline{\delta}$ on I_p).

Let CL_W be the category of p–profinite local W–algebras A with $A/\mathfrak{m}_A = \mathbb{F}$. Hereafter we always assume that W–algebra is an object of CL_W. Let $\rho : \mathfrak{G}_{\mathbb{Q}} \to GL_2(A)$ be a deformation of $\overline{\rho}$ and $\phi : \mathfrak{G}_{\mathbb{Q}} \to W^\times$. We consider the following conditions

(det) $\det\rho = \phi$ regarding ϕ as a character having values in $A^\times$ by composing ϕ with the W-algebra structure morphism $W \to A$;

(ord) Suppose $\rho|_{D_p} \cong \left(\begin{smallmatrix}\epsilon & *\\ 0 & \delta\end{smallmatrix}\right)$ for each decomposition subgroup D_p at p in $\mathfrak{G}_{\mathbb{Q}}$ with unramified $\overline{\delta}$ (so, $\overline{\epsilon} \neq \overline{\delta}$ on I_p).

A couple $(R^{ord,\phi} \in CL_W, \boldsymbol{\rho}^{ord,\phi} : \mathfrak{G}_{\mathbb{Q}} \to GL_2(R^{ord,\phi}))$ is called a p–ordinary universal couple (over $\mathfrak{G}_{\mathbb{Q}}$) with determinant ϕ if $\boldsymbol{\rho}^{ord,\phi}$ satisfies (ord) and (det) and for any deformation $\rho : \mathfrak{G}_{\mathbb{Q}} \to GL_2(A)$ of $\overline{\rho}$ $(A \in CL_W)$ satisfying (ord) and (det), there exists a unique W–algebra homomorphism $\varphi = \varphi_\rho : R^{ord,\phi} \to A$ such that $\varphi \circ \boldsymbol{\rho}^{ord,\phi} \sim \rho$ in $GL_2(A)$. If the uniqueness of φ does not hold, we just call $(R^{ord,\phi}, \boldsymbol{\rho}^{ord,\phi})$ a versal p–ordinary couple with determinant ϕ.

Similarly a couple $(R^{ord} \in CL_W, \boldsymbol{\rho}^{ord} : \mathfrak{G}_{\mathbb{Q}} \to GL_2(R^{ord}))$ (resp. $(R^\phi, \boldsymbol{\rho}^\phi)$) is called a p–ordinary universal couple (over $\mathfrak{G}_{\mathbb{Q}}$) (resp. a universal couple with determinant ϕ) if $\boldsymbol{\rho}^{ord}$ satisfies (ord) (resp. $\det(\boldsymbol{\rho}^\phi) = \phi$) and for any deformation $\rho : \mathfrak{G}_{\mathbb{Q}} \to GL_2(A)$ of $\overline{\rho}$ $(A \in CL_W)$ satisfying (ord) (resp. $\det(\rho) = \phi$), there exists a unique W–algebra homomorphism $\varphi = \varphi_\rho : R^{ord} \to A$ (resp. $\varphi = \varphi_\rho : R^\phi \to A$) such that $\varphi \circ \boldsymbol{\rho}^{ord} \sim \rho$ (resp. $\varphi \circ \boldsymbol{\rho}^\phi \sim \rho$) in $GL_2(A)$.

By the universality, if a universal couple exists, it is unique up to isomorphisms in CL_W.

Theorem 2.9 (Mazur)**.** *Under* (ai$_{\mathbb{Q}}$)*, universal couples* $(R, \boldsymbol{\rho})$ *and* $(R^\phi, \boldsymbol{\rho}^\phi)$ *exist. Under* (rg$_p$) *and* (ai$_{\mathbb{Q}}$)*, universal couples* $(R^{ord}, \boldsymbol{\rho}^{ord} : \mathfrak{G}_{\mathbb{Q}} \to GL_2(R))$ *and* $(R^{ord,\phi}, \boldsymbol{\rho}^{ord,\phi})$ *exist (as long as* $\overline{\rho}$ *satisfies* (ord) *and* (det)*). All these universal rings are noetherian if they exist.*

This fact is proven in Mazur's paper in [M89]. The existence of the universal couple $(R, \boldsymbol{\rho} : \mathfrak{G}_{\mathbb{Q}} \to GL_2(R))$ is proven in previous subsection (see Theorem 2.7) by a different method (and its noetherian property is just mentioned). Here we prove the existence of the universal couples $(R^\phi, \boldsymbol{\rho}^\phi)$, $(R^{ord}, \boldsymbol{\rho}^{ord})$ and $(R^{ord,\phi}, \boldsymbol{\rho}^{ord,\phi})$ assuming the existence of a universal couple $(R, \boldsymbol{\rho})$.

Proof. An ideal $\mathfrak{a} \subset R$ is called ordinary if $\boldsymbol{\rho} \mod \mathfrak{a}$ satisfies (ord). Let $\mathfrak{a}^{ord}$ be the intersection of all ordinary ideals, and put $R^{ord} = R/\mathfrak{a}^{ord}$ and $\boldsymbol{\rho}^{ord} = \boldsymbol{\rho} \mod \mathfrak{a}^{ord}$. If $\rho : \mathfrak{G}_{\mathbb{Q}} \to GL_2(A)$ satisfies (ord), we have a unique morphism $\varphi_\rho : R \to A$ such that $(\boldsymbol{\rho} \mod \mathrm{Ker}(\varphi_\rho)) \sim \varphi_\rho \circ \boldsymbol{\rho} \sim \rho$. Thus $\mathrm{Ker}(\varphi_\rho)$ is ordinary, and hence $\mathrm{Ker}(\varphi_\rho) \supset \mathfrak{a}^{ord}$. Thus φ_ρ factors through R^{ord}. The only thing we need to show is the ordinarity of $\boldsymbol{\rho} \mod \mathfrak{a}^{ord}$. Since $\mathfrak{a}^{ord}$ is an intersection of ordinary ideals, we need to show that if $\mathfrak{a}$ and $\mathfrak{b}$ are ordinary, then $\mathfrak{a} \cap \mathfrak{b}$ is ordinary.

To show this, we prepare some notation. Let V be an A–module with an action of $\mathfrak{G}_{\mathbb{Q}}$. Let $I = I_{\mathfrak{P}}$ be an inertia group at p, and put $V_I = V/\sum_{\sigma\in I}(\sigma - 1)V$. Then by (rg$_p$), ρ is ordinary if and only if $V(\rho)_I$ is A–free of rank 1. The point here is that, writing $\pi : V(\rho) \twoheadrightarrow V(\rho)_I$ for the natural projection, then $\mathrm{Ker}(\pi)$ is an A–direct summand of $V(\rho)$ and hence $V(\rho) \cong \mathrm{Ker}(\pi) \oplus V(\rho)_I$ as A–modules (but not necessarily as $\mathfrak{G}_{\mathbb{Q}}$–modules). Since $V(\rho) \cong A^2$, the Krull-Schmidt theorem tells us that $\mathrm{Ker}(\pi)$ is free of rank 1. Then taking an A–basis (x, y) of $V(\rho)$ so that

$x \in \mathrm{Ker}(\pi)$, we write the matrix representation ρ with respect to this basis, we have desired upper triangular form with $V(\rho)_I/\mathfrak{m}_A V(\rho)_I = V(\overline{\delta})$.

Now suppose that $\rho = \boldsymbol{\rho} \mod \mathfrak{a}$ and $\rho' = \boldsymbol{\rho} \mod \mathfrak{b}$ are both ordinary. Let $\rho'' = \boldsymbol{\rho} \mod \mathfrak{a}\cap\mathfrak{b}$, and write $V = V(\rho)$, $V' = V(\rho')$ and $V'' = V(\rho'')$. By definition, $V''/\mathfrak{a}V'' = V$ and $V''/\mathfrak{b}V'' = V'$. This shows by definition: $V''_I/\mathfrak{a}V''_I = V_I$ and $V''_I/\mathfrak{b}V''_I = V'_I$. Then by Nakayama's lemma, V''_I is generated by one element, thus a surjective image of $A = R/\mathfrak{a}\cap\mathfrak{b}$. Since in A, $\mathfrak{a}\cap\mathfrak{b} = 0$, we can embed A into $A/\mathfrak{a} \oplus A/\mathfrak{b}$ by the Chinese remainder theorem. Since $V_I \cong A/\mathfrak{a}$ and $V'_I \cong A/\mathfrak{b}$, the kernel of the diagonal map $V''_I \to V_I \oplus V'_I \cong A/\mathfrak{a} \oplus A/\mathfrak{b}$ has to be zero. Thus $V''_I \cong A$, which was desired.

As for R^{ϕ} and $R^{ord,\phi}$, we see easily that

$$R^{\phi} = R/\sum_{\sigma\in\mathfrak{G}_{\mathbb{Q}}} R(\det \boldsymbol{\rho}(\sigma) - \phi(\sigma))$$

$$R^{ord,\phi} = R^{ord}/\sum_{\sigma\in\mathfrak{G}_{\mathbb{Q}}} R^{ord}(\det \boldsymbol{\rho}^{ord}(\sigma) - \phi(\sigma)),$$

which finishes the proof. □

2.5. **Tangent spaces of local rings.** To study when $R_{\overline{\rho}}$ is noetherian, here is a useful lemma for an object A in CL_W:

Lemma 2.10. *If $t^*_{A/W} = \mathfrak{m}_A/(\mathfrak{m}_A^2 + \mathfrak{m}_W)$ is a finite dimensional vector space over $\mathbb{F}$, then $A \in CL_W$ is noetherian. The space $t^*_{A/W}$ is called the co-tangent space of A at $\mathfrak{m}_A \in \mathrm{Spec}(A)$ over $\mathrm{Spec}(W)$.*

Proof. Define t^*_A by $\mathfrak{m}_A/\mathfrak{m}_A^2$, which is called the (absolute) co-tangent space of A at $\mathfrak{m}_A$. Since we have an exact sequence:

$$\mathbb{F} \cong \mathfrak{m}_W/\mathfrak{m}_W^2 \longrightarrow t^*_A \longrightarrow t^*_{A/W} \longrightarrow 0,$$

we conclude that t^*_A is of finite dimension over $\mathbb{F}$. First suppose that $pA = 0$ and $\mathfrak{m}_A^N = 0$ for sufficiently large N. Let $\overline{x}_1, \dots, \overline{x}_m$ be an $\mathbb{F}$–basis of t^*_A. We choose $x_j \in A$ so that $x_j \mod \mathfrak{m}_A^2 = \overline{x}_j$. Then we consider the ideal $\mathfrak{a}$ generated by x_j. We have the inclusion map: $\mathfrak{a} = \sum_j Ax_j \hookrightarrow \mathfrak{m}_A$. After tensoring $A/\mathfrak{m}_A$, we have the surjectivity of the induced linear map: $\mathfrak{a}/\mathfrak{m}_A\mathfrak{a} \cong \mathfrak{a}\otimes_A A/\mathfrak{m}_A \to \mathfrak{m}\otimes_A A/\mathfrak{m}_A \cong \mathfrak{m}/\mathfrak{m}_A^2$ because $\{\overline{x}_1, \dots, \overline{x}_m\}$ is an $\mathbb{F}$–basis of t^*_A. This shows that $\mathfrak{m}_A = \mathfrak{a} = \sum_j Ax_j$. Therefore $\mathfrak{m}_A^k/\mathfrak{m}_A^{k+1}$ is generated by the monomials in x_j of degree k as an $\mathbb{F}$–vector space. In particular, $\mathfrak{m}_A^{N-1}$ is generated by the monomials in x_j of degree $N-1$. Then we define $\pi : B = \mathbb{F}[[X_1, \dots, X_m]] \to A$ by $\pi(f(X_1, \dots, X_m)) = f(x_1, \dots, x_m)$. Since any monomial of degree $> N$ vanishes after applying π, π is a well defined W–algebra homomorphism. Let $\mathfrak{m} = \mathfrak{m}_B = (X_1, \cdots, X_m)$ be the maximal ideal of B. By the above argument, $\pi(\mathfrak{m}^{N-1}) = \mathfrak{m}_A^{N-1}$. Suppose now that $\pi(\mathfrak{m}^{N-j}) = \mathfrak{m}_A^{N-j}$, and try to prove the surjectivity of $\pi(\mathfrak{m}^{N-j-1}) = \mathfrak{m}_A^{N-j-1}$. Since $\mathfrak{m}_A^{N-j-1}/\mathfrak{m}_A^{N-j}$ is generated by monomials of degree $N-j-1$ in x_j, for each $x \in \mathfrak{m}_A^{N-j-1}$, we find a homogeneous polynomial $P \in \mathfrak{m}^{N-j-1}$ of $x_1, \dots, x_m$ of degree $N-j-1$ such that $x - \pi(P) \in \mathfrak{m}_A^{N-j} = \pi(\mathfrak{m}^{N-j})$. This shows the assertion: $\pi(\mathfrak{m}^{N-j-1}) = \mathfrak{m}_A^{N-j-1}$. Thus by induction on j, we get the surjectivity of π.

Now suppose only that $\mathfrak{m}_A^N = 0$. Then in particular, $p^N A = 0$. Thus A is an $W/p^N W$–module. We can still define $\pi : B = W/p^N W[[X_1, \dots, X_m]] \to A$ by sending X_j to x_j. Then by the previous argument applied to B/pB and A/pA, we find that $\pi \mod p : B \otimes_W W/pW \cong B/pB \to A/pA \cong A \otimes_W W/pW$ is surjective. In particular, for the maximal ideal $\mathfrak{m}'$ of $W/p^N W$, $\pi \mod \mathfrak{m}' : B \otimes_W \mathbb{F} \cong B/\mathfrak{m}'B \to A/\mathfrak{m}'A \cong A \otimes_W \mathbb{F}$ is surjective. Then by Nakayama's lemma (cf. [CRT] §2 or [MFG] §2.1.3) applied to the nilpotent ideal $\mathfrak{m}'$, π is surjective.

In general, write $A = \varprojlim_i A_i$ for artinian rings A_i. Then the projection maps induce surjections $t^*_{A_{i+1}} \to t^*_{A_i}$. Since t^*_A is of finite dimensional, for sufficiently large i, $t^*_{A_{i+1}} \cong t^*_{A_i}$. Thus choosing x_j as above in A, we have its image $x_j^{(i)}$ in A_i. Use $x_j^{(i)}$ to construct $\pi_i : W[[X_1, \dots, X_m]] \to A_i$ in place of x_j. Then π_i is surjective as already shown, and $\pi = \varprojlim_i \pi_i : W[[X_1, \dots, X_m]] \to A$ remains surjective, because projective limit of surjections, if all sets involved are finite sets, remain surjective (Exercise 1). Since $W[[X_1, \dots, X_m]]$ is noetherian ([CRT] Theorem 3.3), its surjective image A is noetherian. □

2.6. **Recall of group cohomology.** To prove noetherian property of Galois deformation ring R, we need to show the tangent space of $\mathrm{Spec}(R)$ has finite dimension. In order to give a Galois theoretic computation of the tangent space of the deformation ring, we introduce here briefly Galois cohomology groups. Consider a profinite group G and a continuous G-module X. Assume that X has either discrete or profinite topology.

Let $\mathbb{T}_p = \mathbb{Q}_p/\mathbb{Z}_p$. For any abelian p-profinite compact or p-torsion discrete module X, we define the Pontryagin dual module X^* by $X^* = \mathrm{Hom}_{cont}(X, \mathbb{T}_p)$ and give X^* the topology of uniform convergence on every compact subgroup of X. The G-action on $f \in X^*$ is given by $\sigma f(x) = f(\sigma^{-1}x)$. Then by Pontryagin duality theory (cf. [FAN]), we have $(X^*)^* \cong X$ canonically.

Exercise 2.11. *Show that if X is finite, $X^* \cong X$ noncanonically.*

Exercise 2.12. *Prove that X^* is a discrete module if X is p-profinite and X^* is compact if X is discrete.*

By this fact, if X^* is the dual of a profinite module $X = \varprojlim_n X_n$ for finite modules X_n with surjections $X_m \twoheadrightarrow X_n$ for $m > n$, $X^* = \bigcup_n X_n^*$ is a discrete module which is a union of finite modules X_n^*.

We denote by $H^q(G, X)$ the continuous group cohomology with coefficients in X. If X is finite, $H^q(G, X)$ is as defined in [MFG] 4.3.3. Thus we have

$$H^0(G, X) = X^G = \{x \in X | gx = x \text{ for all } g \in G\},$$

and if X is finite,

$$H^1(G, X) = \frac{\{G \xrightarrow{c} X : \text{continuous} | c(\sigma\tau) = \sigma c(\tau) + c(\sigma) \text{ for all } \sigma, \tau \in G\}}{\{G \xrightarrow{b} X | b(\sigma) = (\sigma - 1)x \text{ for } x \in X \text{ independent of } \sigma\}},$$

and $H^2(G, X)$ is given by

$$\frac{\{G \xrightarrow{c} X : \text{continuous} | c(\sigma, \tau) + c(\sigma\tau, \rho) = \sigma c(\tau, \rho) + c(\sigma, \tau\rho) \text{ for all } \sigma, \tau, \rho \in G\}}{\{G \xrightarrow{b} X | b(\sigma, \tau) = c(\sigma) + \sigma c(\tau) - c(\sigma\tau) \text{ for a continuous map } c : G \to X\}}.$$

If $X = \varprojlim_n X_n$ (resp. $X = \varinjlim_x X_n$) for finite G-modules X_n, we define

$$H^j(G, X) = \varprojlim_n H^j(G, X_n) \text{ (resp. } H^j(G, X) = \varinjlim_n H^j(G, X_n)).$$

For each Galois character $\psi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to W^\times$ and a W-module X with continuous action of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, we write $X(\psi)$ for the Galois module whose underlying W-module is X and Galois action is given by ψ. We simply write $X(i)$ for $X(\nu^i)$ for the p-adic cyclotomic character. In particular $\mathbb{Z}_p(1) \cong \varprojlim_n \mu_{p^n}(\overline{\mathbb{Q}})$ as Galois modules.

Let G be the (profinite) Galois group $G = \mathfrak{G}_F$ or $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ for a finite extension $K/\mathbb{Q}_p$. By a result of Tate, Galois cohomology "essentially" has cohomological dimension 2; so, H^0, H^1 and H^2 are important. If $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ for a finite extension $K/\mathbb{Q}_p$, by Tate duality (see [MFG] 4.42),

$$H^{2-i}(G, X) \cong \mathrm{Hom}(H^i(G, X^*(1)), \mathbb{Q}/\mathbb{Z})$$

for finite X.

For a general K-vector space V with a continuous action of G and a G-stable W-lattice L of V, we define $H^q(G, V) = H^q(G, L) \otimes_W K$.

Write $\mathfrak{G}_M = \mathrm{Gal}(F^{(p)}/M)$ for any intermediate field M of $F^{(p)}/F$, where $F^{(p)}/F$ is the maximal extension unramified outside p and ∞. By the inflation-restriction sequence (e.g., [MFG] 4.3.4),

$$0 \to H^1(\mathrm{Gal}(M/F), H^0(\mathfrak{G}_M, X)) \to H^1(\mathfrak{G}_F, X) \to H^1(\mathfrak{G}_M, X)$$

is exact. More generally, we can equip a natural action of $\mathrm{Gal}(M/F)$ on $H^1(\mathfrak{G}_M, X)$ and the sequence is extended to

$$\begin{aligned} 0 \to H^1(\mathrm{Gal}(M/F), H^0(\mathfrak{G}_M, X)) & \\ \to H^1(\mathfrak{G}_F, X) \to H^0(\mathrm{Gal}(M/F), H^1(\mathfrak{G}_M, X)) & \\ \to H^2(\mathrm{Gal}(M/F), H^0(\mathfrak{G}_M, X)) & \end{aligned}$$

which is still exact.

2.7. **Cohomological interpretation of tangent spaces.** Let $R = R_{\overline{\rho}}$. We let $\mathfrak{G}_{\mathbb{Q}}$ acts on $M_n(\mathbb{F})$ by $gv = \overline{\rho}(g)v\overline{\rho}(g)^{-1}$. This $\mathfrak{G}_{\mathbb{Q}}$–module will be written as $ad(\overline{\rho})$.

Lemma 2.13. *Let $R = R_{\overline{\rho}}$ for an absolutely irreducible representation $\overline{\rho} : \mathfrak{G}_{\mathbb{Q}} \to GL_n(\mathbb{F})$. Then*

$$t_{R/W} = \mathrm{Hom}_{\mathbb{F}}(t^*_{R/W}, \mathbb{F}) \cong H^1(\mathfrak{G}_{\mathbb{Q}}, ad(\overline{\rho})),$$

where $H^1(\mathfrak{G}_{\mathbb{Q}}, ad(\overline{\rho}))$ is the continuous first cohomology group of $\mathfrak{G}_{\mathbb{Q}}$ with coefficients in the discrete $\mathfrak{G}_{\mathbb{Q}}$–module $V(ad(\overline{\rho}))$.

The space $t_{R/W}$ is called the tangent space of $\mathrm{Spec}(R)_{/W}$ at $\mathfrak{m}$.

Proof. Let $A = \mathbb{F}[X]/(X^2)$. We write ε for the class of X in A. Then $\varepsilon^2 = 0$. We consider $\phi \in \mathrm{Hom}_{W-alg}(R, A)$. Write $\phi(r) = \phi_0(r) + \phi_\varepsilon(r)\varepsilon$. Then we have from $\phi(ab) = \phi(a)\phi(b)$ that $\phi_0(ab) = \phi_0(a)\phi_0(b)$ and

$$\phi_\varepsilon(ab) = \phi_0(a)\phi_\varepsilon(b) + \phi_0(b)\phi_\varepsilon(a).$$

Thus $\mathrm{Ker}(\phi_0) = \mathfrak{m}_R$ because R is local. Since ϕ is W–linear, $\phi_0(a) = \overline{a} = a \bmod \mathfrak{m}_R$, and thus ϕ kills $\mathfrak{m}_R^2$ and takes $\mathfrak{m}_R$ W–linearly into $\mathfrak{m}_A = \mathbb{F}\varepsilon$. Moreover for $r \in W$, $\overline{r} = r\phi(1) = \phi(r) = \overline{r} + \phi_\varepsilon(r)\varepsilon$, and hence ϕ_ε kills W. Since R shares its residue field $\mathbb{F}$ with W, any element $a \in R$ can be written as $a = r + x$ with $r \in W$ and $x \in \mathfrak{m}_R$. Thus ϕ is completely determined by the restriction of ϕ_ε to $\mathfrak{m}_R$, which factors through $t^*_{R/W}$. We write ℓ_ϕ for ϕ_ε regarded as an $\mathbb{F}$–linear map from $t^*_{R/W}$

into $\mathbb{F}$. Then we can write $\phi(r+x) = \overline{r} + \ell_\phi(x)\varepsilon$. Thus $\phi \mapsto \ell_\phi$ induces a linear map $\ell : \mathrm{Hom}_{W-alg}(R, A) \to \mathrm{Hom}_{\mathbb{F}}(t^*_{R/W}, \mathbb{F})$. Note that $R/(\mathfrak{m}_R^2 + \mathfrak{m}_W) = \mathbb{F} \oplus t^*_{R/W}$. For any $\ell \in \mathrm{Hom}_{\mathbb{F}}(t^*_{R/W}, \mathbb{F})$, we extends ℓ to $R/\mathfrak{m}_R^2$ declaring its value on $\mathbb{F}$ is zero. Then define $\phi : R \to A$ by $\phi(r) = \overline{r} + \ell(r)\varepsilon$. Since $\varepsilon^2 = 0$, ϕ is an W–algebra homomorphism. In particular, $\ell(\phi) = \ell$, and hence ℓ is surjective. Since algebra homomorphisms killing $\mathfrak{m}_R^2 + \mathfrak{m}_W$ are determined by its values on $t^*_{R/W}$, ℓ is injective.

By the universality, we have

$$\mathrm{Hom}_{W-alg}(R, A) \cong \{\rho : \mathfrak{G}_{\mathbb{Q}} \to GL_n(A) | \rho \mod \mathfrak{m}_A = \overline{\rho}\}/\sim .$$

Then we can write $\rho(g) = \overline{\rho}(g) + u'_\rho(g)\varepsilon$. From the mutiplicativity, we have

$$\overline{\rho}(gh) + u'_\rho(gh)\varepsilon = \rho(gh) = \rho(g)\rho(h) = \overline{\rho}(g)\overline{\rho}(h) + (\overline{\rho}(g)u'_\rho(h) + u'_\rho(g)\overline{\rho}(h))\varepsilon,$$

Thus as a function $u' : \mathfrak{G}_{\mathbb{Q}} \to M_n(\mathbb{F})$, we have

$$u'_\rho(gh) = \overline{\rho}(g)u'_\rho(h) + u'_\rho(g)\overline{\rho}(h). \tag{2.2}$$

Define a map $u_\rho : \mathfrak{G}_{\mathbb{Q}} \to ad(\overline{\rho})$ by $u_\rho(g) = u'_\rho(g)\overline{\rho}(g)^{-1}$. Then by a simple computation, we have $gu_\rho(h) = \overline{\rho}(g)u_\rho(h)\overline{\rho}(g)^{-1}$ from the definition of $ad(\overline{\rho})$. Then from the above formula (2.2), we conclude that $u_\rho(gh) = gu_\rho(h) + u_\rho(g)$. Thus $u_\rho : \mathfrak{G}_{\mathbb{Q}} \to ad(\overline{\rho})$ is a 1–cocycle. Starting from a 1–cocycle u, we can reconstruct representation reversing the the above process. Then again by computation,

$$\begin{aligned}\rho \sim \rho' &\iff \overline{\rho}(g) + u'_\rho(g) = (1 + x\varepsilon)(\overline{\rho}(g) + u'_{\rho'}(g))(1 - x\varepsilon) \quad (x \in ad(\overline{\rho}))\\ &\iff u'_\rho(g) = x\overline{\rho}(g) - \overline{\rho}(g)x + u'_{\rho'}(g) \iff u_\rho(g) = (1-g)x + u_{\rho'}(g).\end{aligned}$$

Thus the cohomology classes of u_ρ and $u_{\rho'}$ are equal if and only if $\rho \sim \rho'$. This shows:

$$\begin{aligned}&\mathrm{Hom}_{\mathbb{F}}(t^*_{R/W}, \mathbb{F}) \cong \mathrm{Hom}_{W-alg}(R, A) \cong\\ &\qquad \{\rho : \mathfrak{G}_{\mathbb{Q}} \to GL_n(A) | \rho \mod \mathfrak{m}_A = \overline{\rho}\}/\sim \cong H^1(\mathfrak{G}_{\mathbb{Q}}, ad(\overline{\rho})).\end{aligned}$$

In this way, we get a bijection between $\mathrm{Hom}_{\mathbb{F}}(t^*_{R/W}, \mathbb{F})$ and $H^1(\mathfrak{G}_{\mathbb{Q}}, ad(\overline{\rho}))$. By tracking down (in the reverse way) our construction, one can check that the map is an $\mathbb{F}$–linear isomorphism. □

For each open subgroup H of a profinite group G, we write H_p for the maximal p–profinite quotient. We consider the following condition:

(Φ) *For any open subgroup H of G, the p-Frattini quotient $\Phi(H_p)$ is a finite group,*

where $\Phi(H_p) = H_p/\overline{(H_p)^p(H_p, H_p)}$ for the the commutator subgroup (H_p, H_p) of H_p.

Proposition 2.14 (Mazur)**.** *By class field theory, $\mathfrak{G}_{\mathbb{Q}}$ satisfies (Φ), and $R_{\overline{\rho}}$ is a noetherian ring.*

Proof. Let $H = \mathrm{Ker}(\overline{\rho})$. Then the action of H on $ad(\overline{\rho})$ is trivial. By the inflation-restriction sequence for $G = \mathfrak{G}_{\mathbb{Q}}$, we have the following exact sequence:

$$0 \to H^1(G/H, H^0(H, ad(\overline{\rho}))) \to H^1(G, ad(\overline{\rho})) \to \mathrm{Hom}(\Phi(H_p), M_n(\mathbb{F})).$$

From this, it is clear that $\dim_{\mathbb{F}} H^1(G, ad(\overline{\rho})) < \infty$ if $\mathfrak{G}_{\mathbb{Q}}$ satisfies the p-Frattini condition (Φ). The fact that $\mathfrak{G}_{\mathbb{Q}}$ satisfies (Φ) follows from class field theory. Indeed, if F is the fixed field of H, then $\Phi(H_p)$ fixes the maximal p-abelian extension M/F of type $(p, p, \ldots, p)$ unramified outside p. Here a p-abelian extension M/F is of type $(p, p, \ldots, p)$ if $\mathrm{Gal}(M/F)$ is abelian killed by p. By class field theory, $[M : F]$ is finite. □

2.8. **Applications to representation theory.** Group cohomology can be used to measure obstruction of extending a representation of a subgroup to the entire group. The theory is a version of Schur's theory of projective representations [MRT] Section 11E.

Let G be a profinite group with a normal open subgroup H of finite index. We put $\Delta = G/H$. Fix a complete noetherian local $\mathbb{Z}_p$–algebra W with residue field $\mathbb{F}$. Any algebra A in this section will be assumed to be an object of CL_W. For each continuous representation $\rho : H \to GL_n(A)$ and $\sigma \in G$, we define $\rho^\sigma(g) = \rho(\sigma g \sigma^{-1})$.

We take a representation $\pi : H \to GL_n(A)$ for an artinian local W–algebra A with residue field $\mathbb{F}$. We assume the following condition:

$$(\mathrm{AI}_H) \qquad \overline{\rho} = \pi \mod \mathfrak{m}_A \text{ is absolutely irreducible.}$$

For the moment, we assume another condition:

$$(\mathrm{C}) \qquad \pi = c(\sigma)^{-1}\pi^\sigma c(\sigma) \text{ with some } c(\sigma) \in GL_n(A) \text{ for each } \sigma \in G.$$

If we find another $c'(\sigma) \in GL_n(A)$ satisfying $\pi = c'(\sigma)^{-1}\pi^\sigma c'(\sigma)$, we have

$$\pi = c'(\sigma)^{-1}c(\sigma)\pi c(\sigma)^{-1}c'(\sigma),$$

and hence by Exercise 2.5 (3), $c(\sigma)^{-1}c'(\sigma)$ is a scalar. In particular, for σ, $\tau \in G$,

$$c(\sigma\tau)^{-1}\pi^{\sigma\tau}c(\sigma\tau) = \pi = c(\tau)^{-1}\pi^\tau c(\tau) = c(\tau)^{-1}c(\sigma)^{-1}\pi^{\sigma\tau}c(\sigma)c(\tau),$$

and hence, $b(\sigma, \tau) = c(\sigma)c(\tau)c(\sigma\tau)^{-1} \in A^\times$. Thus $c(\sigma)c(\tau) = b(\sigma, \tau)c(\sigma\tau)$. This shows by the associativity of the matrix multiplication that

$$(c(\sigma)c(\tau))c(\rho) = b(\sigma, \tau)c(\sigma\tau)c(\rho) = b(\sigma, \tau)b(\sigma\tau, \rho)c(\sigma\tau\rho) \text{ and}$$
$$c(\sigma)(c(\tau)c(\rho)) = c(\sigma)b(\tau, \rho)c(\tau\rho) = b(\tau, \rho)b(\sigma, \tau\rho)c(\sigma\tau\rho),$$

and hence $b(\sigma, \tau)$ is a 2–cocycle of G. If $h \in H$, then

$$\pi(g) = c(h\tau)^{-1}\pi(h\tau g\tau^{-1}h^{-1})c(h\tau) =$$
$$c(h\tau)^{-1}\pi(h)c(\tau)\pi(g)c(\tau)^{-1}\pi(h)^{-1}c(h\tau).$$

Thus $c(h\tau)^{-1}\pi(h)c(\tau) \in A^\times$.

Write $G = \bigsqcup_{\tau \in R} H\tau$ (disjoint). We redefine c by $c(h\tau) = \pi(h)c(\tau)$ for $\tau \in R$ and $h \in H$. Then c satisfies $c(h\tau) = \pi(h)c(\tau)$ for all $h \in H$ and $\tau \in R$. Since $c(hh'\tau) = \pi(hh')c(\tau) = \pi(h)c(h'\tau)$, actually c satisfies that

$$(\pi) \qquad c(h\tau) = \pi(h)c(\tau) \text{ for all } h \in H \text{ and all } \tau \in G.$$

Since $c(1)$ commutes with $\mathrm{Im}(\pi)$, $c(1)$ is scalar. Thus we may also assume

$$(\mathrm{id}) \qquad c(1) = 1.$$

Note that for $h,\ h' \in H$,

$$\begin{aligned} b(h\sigma, h'\tau) &= c(h\sigma)c(h'\tau)c(h\sigma h'\tau)^{-1} \\ &= \pi(h)c(\sigma)\pi(h')c(\tau)c(\sigma\tau)^{-1}\pi(h\sigma h'\sigma^{-1})^{-1} \\ &= \pi(h)\pi^{\sigma}(h')b(\sigma,\tau)\pi(h\sigma h'\sigma^{-1})^{-1} = b(\sigma,\tau). \end{aligned}$$

Thus b is a 2–cocycle factoring through Δ.

If we change c by c', then by (C), $c'(\sigma) = c(\sigma)\zeta(\sigma)$ for $\zeta(\sigma) \in A^\times$. Thus we see from $c(\sigma)c(\tau) = b(\sigma,\tau)c(\sigma\tau)$ that $c'(\sigma)c'(\tau) = b(\sigma,\tau)\zeta(\sigma)\zeta(\tau)c'(\sigma\tau)\zeta(\sigma\tau)^{-1}$. Thus the 2–cocycle b' made out of c' is cohomologous to b, and the cohomology class $[b] = [\pi] \in H^2(\Delta, A^\times)$ is uniquely determined by π.

If $b(\sigma,\tau) = \zeta(\sigma)\zeta(\tau)\zeta(\sigma\tau)^{-1}$ is further a coboundary of $\zeta : \Delta \to A^\times$, we modify c by $\zeta^{-1}c$. Since ζ factors through Δ, this modification does not destroy the property (π). Then $c(\sigma\tau) = c(\sigma)c(\tau)$ and $c(h\tau) = \pi(h)c(\tau)$ for $h \in H$. Thus c is a representation of G and extends π to G. Let d be another extension of π. Then $\chi(\sigma) = c(\sigma)d(\sigma)^{-1} \in A^\times$ is a character of G, because χ commutes with π. Thus $c = d \otimes \chi$.

We consider another condition

(inv) $$\mathrm{Tr}(\pi) = \mathrm{Tr}(\pi^{\sigma}) \text{ for all } \sigma \in G.$$

Under (AI_H), it has been proven by Carayol and Serre (Proposition 2.6) that (inv) is actually equivalent to (C). Thus we have

Theorem 2.15. *Let $\pi : H \to GL_n(A)$ be a continuous representation for a p–adic artinian local ring A. Suppose* (AI_H) *and* (inv)*.*

1. *We can choose c satisfying (π);*
2. *Choosing c as above, $b(\sigma,\tau) = c(\sigma)c(\tau)c(\sigma\tau)^{-1}$ is a 2–cocycle of Δ with values in $A^\times$;*
3. *The cohomology class $[b] = [\pi]$ (called the obstruction class of π) of the above b only depends on π but not on the choice of c, etc. There exists a continuous representation π_E of G into $GL_n(A)$ extending π if and only if $[\pi] = 0$ in $H^2(\Delta, A^\times)$;*
4. *All other extensions of π to G are of the form $\pi_E \otimes \chi$ for a character χ of Δ with values in $A^\times$.*
5. *If $H^2(\Delta, A^\times) = 0$, then any representation π satisfying* (AI_H) *and* (inv) *can be extended to G.*

Corollary 2.16. *If Δ is a p–group, then any representation π with values in $GL_n(\mathbb{F})$ for a finite field $\mathbb{F}$ of characteristic p satisfying* (AI_H) *and* (inv) *can be extended to G.*

Proof. This follows from the fact that $|\mathbb{F}^\times|$ is prime to p. Hence $H^2(\Delta, \mathbb{F}^\times) = 0$. □

When Δ is cyclic, then $H^2(\Delta, A^\times) \cong A^\times/(A^\times)^d$ for $d = |\Delta|$. If for a generator σ of G, $\xi = c(\sigma^d)\pi(\sigma^d)^{-1} \in (A^\times)^d$, then b is a coboundary of $\zeta(\sigma^j) = \xi^{j/d}$. By extending scalar to $B = A[X]/(X^d - \xi)$, in $H^2(G, B^\times)$, the class of b vanishes. Thus we have

Corollary 2.17. *Suppose* (AI_H) *and* (inv)*. If* Δ *is a cyclic group of order* d*, then* π *can be extended to a representation of* G *into* $GL_n(B)$ *for a local* A*–algebra* B *which is* A*–free of rank at most* $d = |\Delta|$.

Let $\overline{\rho} = \pi \mod \mathfrak{m}_A$. We suppose that $\overline{\rho}$ can be extended to G. Then we may assume that the cohomology class of $b(\sigma,\tau) \mod \mathfrak{m}_A$ vanishes in $H^2(G,\mathbb{F}^\times)$. Thus we can find $\zeta : G \to A^\times$ such that

$$a(\sigma,\tau) = b(\sigma,\tau)\zeta(\sigma)\zeta(\tau)\zeta(\sigma\tau)^{-1} \mod \mathfrak{m}_A \equiv 1.$$

Then a has values in $\widehat{\mathbb{G}}_m(A) = 1 + \mathfrak{m}_A$. In particular, if the Sylow p–subgroup S of Δ is cyclic, we have $H^2(S, \widehat{\mathbb{G}}_m(A)) \cong \widehat{\mathbb{G}}_m(A)/\widehat{\mathbb{G}}_m(A)^{|S|}$. Write ξ for the element in $\widehat{\mathbb{G}}_m(A)$ corresponding to a. Then for $B = A[X]/(X^{|S|} - \xi)$, the cohomology class of a vanishes in $H^2(S, \widehat{\mathbb{G}}_m(B))$. This implies that in $H^2(S, B^\times)$, the cohomology class of b vanishes. Since $\mathrm{Tr} \circ \mathrm{Res} : H^q(\Delta, M) \to H^q(S, M)$ is a multiplication by $(\Delta : S)$ prime to p, if M is p-profinite, Res is injective; so, $H^q(\Delta, \widehat{\mathbb{G}}_m(B)) = 0$.

Corollary 2.18. *Suppose* (AI_H) *and* (inv)*. Suppose* Δ *has a cyclic Sylow* p*–subgroup of order* q*. If* $\overline{\rho}$ *can be extended to* G*, then* π *can be extended to a representation of* G *into* $GL_n(B)$ *for a local* A*–algebra* B *which is* A*–free of rank at most* q.

We now prove the following fact:

(AI) When Δ is cyclic of odd order and $n = 2$, the condition (AI_H) is equivalent to (AI_G).

Proof. Let ρ be an absolutely irreducible representation of G into $GL_2(K)$ for a field K. We assume that Δ is cyclic of odd order. We prove that ρ cannot contain a character of H as a representation of H, which shows the equivalence, since ρ is 2–dimensional. Suppose by absurdity that ρ restricted to H contains a character χ. Let $H' = \{g \in G | \chi(ghg^{-1}) = \chi\}$. Then χ can be extended to a character of H' (Corollary 2.17). We pick one extension $\widetilde{\chi} : H' \to B^\times$ for a finite flat extension B/A in CL. Let $\rho' = \rho|_{H'}$. By Frobenius reciprocity, we have

$$\mathrm{Hom}_{\mathbb{Z}[H']}(\rho', \mathrm{Ind}_H^{H'} \chi) \cong \mathrm{Hom}_{\mathbb{Z}[H]}(\rho'|_H, \chi), \tag{2.3}$$

where, by definition, $\mathrm{Ind}_G^H M = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[H], M)$ and we let $g \in H'$ act on $\phi \in \mathrm{Hom}_{\mathbb{Z}}(M,N)$ by $(g\phi)(x) = g(\phi(g^{-1}x))$ for two H'–modules M and N. If $\rho' = \rho|_{H'}$ remains irreducible, this shows that $\rho' \subset \mathrm{Ind}_H^{H'} \chi$. It is easy to check from definition that

$$\mathrm{Ind}_H^{H'} \chi \cong \oplus_\xi \widetilde{\chi}\xi,$$

ξ running all characters of the cyclic group H'/H. Thus ρ' cannot be irreducible, and we may assume that $H = H'$. Then conjugates of χ under Δ are all distinct. Since, by Shapiro's lemma again, $\rho \subset \mathrm{Ind}_H^G \chi$ and $\rho \cong \rho^\sigma \subset \mathrm{Ind}_{H'}^G {\chi'}^\sigma$. Therefore $\rho|_{H'}$ contains all conjugates of χ' with the equal multiplicity. Thus $(G : H')|2$, which is absurd because $(G : H)$ is odd. □

3. Base change of deformation rings

In this section, we describe a general theory (given in [MFG, §5.4]) of controlling the deformation rings of representations of a normal subgroup under the action of the quotient finite group.

Throughout the section, we fix a profinite group G and a open normal subgroup H. We write the quotient $\Delta = G/H$. Our deformation functor can be defined over the category CL_W, but if the following finite p–Frattini condition is satisfied by G, all the functors introduced here, if representable in CL_W, they are actually representable over the smaller full subcategory CNL_W of noetherian pro-artinian rings:

(Φ) All open subgroup of G has finite p–Frattini quotient.

The p–Frattini quotient of a profinite group G is $G/\overline{G^p(G:G)}$ for the commutater subgroup $(G:G)$. By class field theory, this condition is satisfied by $\mathrm{Gal}(F^S/F)$ for a number field F (e.g., [MFG, Proposition 2.30]), where F^S/F is the maximal extension unramified outside a finite set S of places of F. Thus, assuming (Φ) does not cause any harm to our later application; so, we will assume (Φ) throughout this section for simplicity.

3.1. **Deformation functors of group representations.** We fix a representation $\overline{\rho} : G \to GL_n(\mathbb{F})$ and consider the following condition

(AI_H) $\overline{\rho}_H = \overline{\rho}|_H$ *is absolutely irreducible.*

In this subsection, we study various deformation problems of $\overline{\rho}$ and relation among the universal rings.

We consider a deformation functor $\mathcal{F}_H : CNL_W \to SETS$ given by

$$\mathcal{F}_H(A) = \{\rho : H \to GL_n(A) \mid \rho \equiv \overline{\rho} \mod \mathfrak{m}_A\}/\sim$$

where "$\sim$" is the conjugation equivalence in $GL_n(A)$. The functor $\mathcal{F}_H$ is representable under (AI_H) by Theorem 2.7. We write (R_H, ρ_H) for the universal couple. Since ρ_G restricted to H is an element in $\mathcal{F}_H(R_H)$, we have an W–algebra homomorphism (called the base-change map) $\alpha : R_H \to R_G$ such that $\alpha\rho_H = \rho_G|_H$.

We would like to determine $\mathrm{Ker}(\alpha)$ and $\mathrm{Im}(\alpha)$ in terms of Δ. We briefly recall the theory of extending representation described in 2.8. By choosing a lift $c_0(\sigma) \in GL_n(W)$ for $\sigma \in G$ such that $c_0(\sigma) \equiv \overline{\rho}(\sigma) \mod \mathfrak{m}_W$, we can define for any $\rho \in \mathcal{F}_G(A)$, $\rho^\sigma(g) = \rho(\sigma g \sigma^{-1})$ and $\rho^{[\sigma]}(g) = c_0(\sigma)^{-1}\rho^\sigma(g)c_0(\sigma)$ in $\mathcal{F}_H(A)$. In this way, Δ acts via $\sigma \mapsto [\sigma]$ on $\mathcal{F}_H$ and R_H. Then as seen in 2.8, we can attach a 2–cocycle b of Δ with values in $\widehat{\mathbb{G}}_m(A)$ to any representation $\rho \in \mathcal{F}_H(A)$ with $\rho^{[\sigma]} \sim \rho$ in the following way. Let us recall the construction of b briefly: First choose a lift $c(\sigma)$ of $\overline{\rho}(\sigma)$ in $GL_n(A)$ for each $\sigma \in G$ such that $c(1) = 1$, $\rho = c(\sigma)^{-1}\rho^\sigma c(\sigma)$ and $c(h\tau) = \rho(h)c(\tau)$ for $h \in H$ and $\tau \in G$. Then we have that $c(\sigma)c(\tau) = b(\sigma,\tau)c(\sigma\tau)$ for a 2–cocycle b of Δ with values in $\widehat{\mathbb{G}}_m(A)$. The cohomology class $[\rho]$ is uniquely determined by ρ independently of the choice of c and is called the *obstruction* class to extending ρ to G. If $[\rho] = 0$, then $b(\sigma,\tau) = \zeta(\sigma)^{-1}\zeta(\tau)^{-1}\zeta(\sigma\tau)$ for a 1–cochain ζ. We then modify c by $c\zeta$. Then c extends the representation ρ to a representation $\pi = c$ of G (Theorem 2.15).

Lemma 3.1. *Let $\rho \in \mathcal{F}_H(A)$. Suppose* (AI_H) *and that n is prime to p and $\rho^{[\sigma]} \sim \rho$ for all $\sigma \in \Delta$. If $\det(\rho)$ can be extended to a deformation of $\det\overline{\rho}$ (over G) having values in an A–algebra B containing A, then ρ can be extended uniquely to a deformation $\pi : G \to GL_n(B)$ of $\overline{\rho}$ whose determinant coincides with the extension to G of $\det(\rho)$.*

Proof. By applying "det" to c and b, we know that $[\det(\rho)] = [\det(b)] = n[\rho]$. If n is prime to p, the vanishing of $n[\rho]$ in $H^2(\Delta, \widehat{\mathbb{G}}_m(B))$ is equivalent to the vanishing of the obstruction class $[\rho]$. Thus if $\det(\rho)$ extends to G (that is $n[\rho] = 0$), then ρ extends to a representation π of G which has determinant equal to the extension of $\det(\rho)$ prearranged. Since $[\overline{\rho}_H] = 0$, we may assume that π is a deformation of $\overline{\rho}$. We now show the uniqueness of π. We get, out of π, other extensions $\pi \otimes \chi \in \mathcal{F}_G(B)$ for $\chi \in H^1(\Delta, \widehat{\mathbb{G}}_m(B)) = \mathrm{Hom}(\Delta, \widehat{\mathbb{G}}_m(B))$. Conversely, if π and π' are two extensions of ρ in $\mathcal{F}_G(B)$, then for $h \in H$, $\pi'(\sigma)\rho(h)\pi'(\sigma)^{-1} = \pi(\sigma)\rho(h)\pi(\sigma)^{-1}$ and hence $\pi(\sigma)^{-1}\pi'(\sigma)$ commutes with ρ. Then by Exercise 2.5 (3), $\chi(\sigma) = \pi(\sigma)^{-1}\pi'(\sigma)$ is a scalar in $\widehat{\mathbb{G}}_m(B)$.

$$\begin{aligned}\chi(\sigma\tau) = \pi(\sigma\tau)^{-1}\pi'(\sigma\tau) &= \pi(\tau)^{-1}\pi(\sigma)^{-1}\pi'(\sigma)\pi'(\tau)\\ &= \pi(\tau)^{-1}\chi(\sigma)\pi'(\tau) = \chi(\sigma)\chi(\tau).\end{aligned}$$

Thus χ is an element in $H^1(\Delta, \widehat{\mathbb{G}}_m(B))$ and $\pi' = \pi \otimes \chi$, which shows that $\det(\pi')$ is equal to $\det(\pi)\chi^n$. If $\det(\pi') = \det(\pi)$, then $\chi^n = 1$. Since χ is of p–power order, if n is prime to p, $\chi = 1$. □

Here is a consequence of the proof of the lemma:

Corollary 3.2. *Let $\pi_0 \in \mathcal{F}_G(B)$ be an extension of $\rho \in \mathcal{F}_H(A)$ for an A–algebra B containing A. Then we have*

$$\{\pi_0 \otimes \chi \mid \chi \in \mathrm{Hom}(\Delta, \widehat{\mathbb{G}}_m(B))\} = \{\pi \in \mathcal{F}_G(B) \mid \pi_{|H} = \rho\}.$$

It is easy to see that if $H^2(\Delta, \mathbb{F}) = 0$, then $H^2(\Delta, \widehat{\mathbb{G}}_m(A)) = 0$ for all A in CNL (Exercise 1). Therefore we see, if $H^2(\Delta, \mathbb{F}) = 0$,

$$(*)\qquad \mathcal{F}_H^{\Delta}(A) = H^0(\Delta, \mathcal{F}_H(A)) \cong \mathcal{F}_G(A)/\widehat{\Delta}(A) \text{ for } \widehat{\Delta}(A) = \mathrm{Hom}(\Delta, \widehat{\mathbb{G}}_m(A)).$$

Here we let $\chi \in \widehat{\Delta}(A)$ act on $\mathcal{F}_G(A)$ via $\pi \mapsto \pi \otimes \chi$. Suppose that $\mathcal{F}_H^{\Delta}$ is represented by a universal couple $(R_{H,\Delta}, \rho_{H,\Delta})$ and $[\rho_{H,\Delta}] = 0$ in $H^2(\Delta, \widehat{\mathbb{G}}_m(R_{H,\Delta}))$. Then for each $\rho \in \mathcal{F}_H^{\Delta}(A)$, we have $\varphi : R_{H,\Delta} \to A$ such that $\varphi\rho_{H,\Delta} \sim \rho$. Then $\varphi_*[\rho_{H,\Delta}] = [\rho]$ and therefore, $[\rho] = 0$ in $H^2(\Delta, \widehat{\mathbb{G}}_m(A))$. This shows again $(*)$.

Under (AI_H), by Proposition 2.6, $\mathcal{F}_H^{\Delta}(A) \ni \rho \mapsto \mathrm{Tr}(\rho)$ sends representations ρ to Δ–invariant pseudo representations which are deformations of $\mathrm{Tr}(\overline{\rho})$, bijectively. In the same way as in the proof of Theorem 2.7, it is easy to check that this deformation functor of pseudo-representations is representable (Exercise 2). Then the subfunctor $\mathcal{F}_H^{\Delta}$ is represented by a residue ring $R_H/\mathfrak{a}$ for an ideal $\mathfrak{a}$. Again by the unicity lemma, $\mathcal{F}_H^{\Delta}$ is represented by $R_{H,\Delta} = R_H/\Sigma_{\sigma\in\Delta}R_H([\sigma]-1)R_H$ (Exercise 3).

Proposition 3.3. *Suppose* (AI_H). *Then $\mathcal{F}_H^{\Delta}$ is represented by $(R_{H,\Delta}, \rho_{H,\Delta})$ for $R_{H,\Delta} = R_H/\mathfrak{a}$ with $\mathfrak{a} = \Sigma_{\sigma\in\Delta}R_H([\sigma]-1)R_H$ and $\rho_{H,\Delta} = \rho_H \mod \mathfrak{a}$. If either $[\rho_{H,\Delta}] = 0$ in $H^2(\Delta, \widehat{\mathbb{G}}_m(R_{H,\Delta}))$ or $H^2(\Delta, \mathbb{F}) = 0$, then we have $\mathcal{F}_G/\widehat{\Delta} \cong \mathcal{F}_H^{\Delta}$ via $\pi \mapsto \pi|_H$.*

We now consider the following subfunctor $\mathcal{F}_{G,H}$ of $\mathcal{F}_H$ given by

$$\mathcal{F}_{G,H}(A) = \left\{ \rho|_H \in \mathcal{F}_H(A) \middle| \rho \in \mathcal{F}_G(B) \text{ for a flat } A\text{–algebra } B \text{ in } CNL_W \right\}.$$

Here the algebra B may not be unique and depends on A. Let us check that $\mathcal{F}_{G,H}$ is really a functor. If $\varphi : A \to A'$ is a morphism in CNL and $\rho|_H \in \mathcal{F}_{G,H}(A)$ with $\rho \in \mathcal{F}_G(B)$, B being flat over A, then $A'\widehat{\otimes}_A B$ is a flat A'–algebra in CNL. Then $(\varphi \otimes id)\rho \in \mathcal{F}_G(A'\widehat{\otimes}_A B)$ such that $\varphi(\rho|_H) = ((\varphi \otimes id)\rho)|_H$. Thus $\mathcal{F}_H(\varphi)$ takes $\mathcal{F}_{G,H}(A)$ into $\mathcal{F}_{G,H}(A')$, which shows that $\mathcal{F}_{G,H}$ is a well defined functor. For each $\rho \in \mathcal{F}_{G,H}(A)$, we have an extension $\rho \in \mathcal{F}_G(B)$. By the universality of (R_G, ρ_G), we have $\varphi : R_G \to B$ such that $\varphi\rho_G = \rho$. Then $\rho|_H = (\varphi\rho_G)|_H = \varphi(\rho_G|_H) = \varphi\alpha\rho_H$. This shows that $\varphi\alpha$ is uniquely determined by $\rho|_H \in \mathcal{F}_{G,H}(A)$. Therefore φ restricted to $\mathrm{Im}(\alpha)$ has values in A and is uniquely determined by $\rho|_H \in \mathcal{F}_{G,H}(A)$. Conversely, supposing that $[\alpha\rho_H] = 0$ in $H^2(\Delta, \widehat{\mathbb{G}}_m(B))$ for a flat extension B of $\mathrm{Im}(\alpha)$ in CNL, for a given $\varphi : \mathrm{Im}(\alpha) \to A$ which is a morphism in CNL, we shall show that $\rho = \varphi\alpha\rho_H$ is an element of $\mathcal{F}_{G,H}(A)$. Anyway $\alpha\rho_H$ can be extended to G as an element in $\mathcal{F}_G(B)$, and hence $\alpha\rho_H \in \mathcal{F}_{G,H}(\mathrm{Im}(\alpha))$. We note that ρ can be extended to G because $[\varphi\alpha\rho_H] = \varphi_*[\alpha\rho_H]$ which vanishes in $H^2(\Delta, \widehat{\mathbb{G}}_m(B'))$ for $B' = B\widehat{\otimes}_{\mathrm{Im}(\alpha),\varphi} A$. Thus $\rho \in \mathcal{F}_{G,H}(A)$, and $\mathcal{F}_{G,H}$ is represented by $(\mathrm{Im}(\alpha), \alpha\rho_H)$ as long as $[\alpha\rho_H] = 0$ in $H^2(\Delta, \widehat{\mathbb{G}}_m(B))$ for a flat extension B of $\mathrm{Im}(\alpha)$ in CNL.

We have the following inclusions of functors: $\mathcal{F}_G/\widehat{\Delta} \hookrightarrow \mathcal{F}_{G,H} \subset \mathcal{F}_H^{\Delta} \subset \mathcal{F}_H$, the first map being given by $\rho \mapsto \rho|_H$, which is injective by Corollary 3.2. The functor $\mathcal{F}_H^{\Delta}$ is represented by $R_H/\mathfrak{a}$ for $\mathfrak{a} = \Sigma_{\sigma\in\Delta} R_H([\sigma]-1)R_H$. Because of the above inclusion, if $[\alpha\rho_H] = 0$ in $H^2(\Delta, \widehat{\mathbb{G}}_m(B))$ for a flat extension B of $\mathrm{Im}(\alpha)$ in CNL, the ring $\mathrm{Im}(\alpha)$ is a surjective image of $R_H/\mathfrak{a} = R_{H,\Delta}$. If $[\rho_{H,\Delta}] = 0$ (for $\rho_{H,\Delta} = \rho_H \mod \mathfrak{a}$) in $H^2(\Delta, \widehat{\mathbb{G}}_m(B'))$ for a flat extension B' of $R_{H,\Delta}$ in CNL, then $\rho_{H,\Delta} \in \mathcal{F}_{G,H}(R_{H,\Delta})$ and thus $\mathcal{F}_H^{\Delta} = \mathcal{F}_{G,H}$.

Proposition 3.4. *Assume* (AI_H) *and that* $[\alpha\rho_H] = 0$ *in* $H^2(\Delta, \widehat{\mathbb{G}}_m(B))$ *for a flat extension* B *of* $\mathrm{Im}(\alpha)$ *in* CNL*. Then* $\mathcal{F}_{G,H}$ *is represented by* $(\mathrm{Im}(\alpha), \alpha\rho_H)$*. If further* $[\rho_{H,\Delta}] = 0$ *in* $H^2(\Delta, \widehat{\mathbb{G}}_m(B'))$ *for a flat extension* B' *of* $R_{H,\Delta}$*, then we have* $\mathcal{F}_{G,H} = \mathcal{F}_H^{\Delta}$*.*

The character $\det(\rho_H)$ induces an W–algebra homomorphism: $W[[H^{ab}]] \to R_H$ for the maximal continuous abelian quotient H^{ab} of H. We write its image as Λ_H and write simply Λ for Λ_G. Since the map $W[[H^{ab}]] \to R_H$ factors through the local ring $W[[H_p^{ab}]]$ in CNL_W for the maximal p–profinite quotient H_p^{ab} of H^{ab}, Λ_H is an object in CNL_W. Thus we have a character $\det(\rho_H) : H \to \Lambda_H^{\times}$. We consider the category CNL_{Λ_H} of complete noetherian local Λ_H–algebras with residue field $\mathbb{F}$. We consider the functor $\mathcal{F}_{\Lambda_H,H} : CNL_{\Lambda_H} \to SETS$ given by

$$\mathcal{F}_{\Lambda_H,H}(A) = \{\rho : H \to GL_n(A) \mid \rho \equiv \overline{\rho} \mod \mathfrak{m}_A \text{ and } \det(\rho) = \det(\rho_H)\}/\sim.$$

Pick $\rho : H \to GL_n(A) \in \mathcal{F}_{\Lambda_H,H}(A)$. Then regarding A as an W–algebra naturally, we know that $\rho \in \mathcal{F}_H(A)$. Thus there is a unique morphism $\varphi : R_H \to A$ such that $\varphi\rho_H \sim \rho$. Then $\varphi(\det(\rho_H)) = \det(\rho)$, and φ is a morphism in CNL_{Λ_H}. Therefore (R_H, ρ_H) represents $\mathcal{F}_{\Lambda_H}$. Similarly to $\mathcal{F}_{G,H}$, we consider another functor on CNL_Λ:

$$\mathcal{F}_{\Lambda,G,H}(A) = \left\{ \rho|_H \in \mathcal{F}_H(A) \middle| \rho \in \mathcal{F}_{\Lambda,G}(B) \text{ for a flat } A\text{–algebra } B \text{ in } CNL_\Lambda \right\}.$$

Take $\rho \in \mathcal{F}_{\Lambda,G,H}(A)$ such that $\rho = \rho'|_H$ for $\rho' \in \mathcal{F}_{\Lambda,G}(B)$. Then there exists a unique $\varphi : R_G \to B$ with $\det(\rho') = \varphi(\det(\rho_G))$. Since the Λ–algebra structure of B is given by $\det(\rho')$, φ induces a Λ–algebra homomorphism of $\mathrm{Im}(\alpha)\Lambda$ into B for the algebra $\mathrm{Im}(\alpha)\Lambda$ generated by $\mathrm{Im}(\alpha)$ and Λ. From $\rho = (\varphi\rho_G)|_H = \varphi(\rho_G|_H) = \varphi\alpha\rho_H$, we see that the Λ–algebra homomorphism φ restricted $\mathrm{Im}(\alpha)\Lambda$ is uniquely determined by ρ. Supposing that $[\alpha\rho_H]$ vanishes in $H^2(\Delta, \widehat{\mathbb{G}}_m(B))$ for a flat extension B of $\mathrm{Im}(\alpha)$, we knows that $[\alpha\rho_H]$ vanishes in the cohomology group $H^2(\Delta, \widehat{\mathbb{G}}_m(\mathrm{Im}(\alpha)\Lambda \otimes_{\mathrm{Im}(\alpha)} B))$. For any morphism $\varphi : \mathrm{Im}(\alpha)\Lambda \to A$ in CNL_Λ, $[\varphi\alpha\rho_H] = \varphi_*[\alpha\rho_H]$ vanishes in $H^2(\Delta, \widehat{\mathbb{G}}_m(B'))$ for $B' = A \otimes_{\mathrm{Im}(\alpha)} B$ which is flat over A. Thus we have an extension π of ρ to G having values in B'. Suppose further that n is prime to p. In this case, as already remarked, we can always extend ρ without extending A and without assuming the vanishing of $[\alpha\rho_H]$, because $\det(\rho)$ can be extended to G by $\varphi \circ \det(\rho_G)$. Thus we know:

$$\mathcal{F}_{\Lambda,G,H}(A) = \left\{ \rho|_H \in \mathcal{F}_H(A) \middle| \rho \in \mathcal{F}_{\Lambda,G}(A) \right\}.$$

Since $\det(\rho)$ can be extended to G without changing A, there is a unique extension of π with values in $GL_n(A)$ such that $\det(\pi) = \iota \circ (\det(\rho_G))$, which implies that $\pi \in \mathcal{F}_{\Lambda,G}(A)$ and hence $\pi|_H \in \mathcal{F}_{\Lambda,G,H}(A)$. Thus $\mathcal{F}_{\Lambda,G,H}$ is represented by $(\mathrm{Im}(\alpha)\Lambda, \alpha\rho_H)$ if n is prime to p. We consider the morphism of functors: $\mathcal{F}_{\Lambda,G} \to \mathcal{F}_{\Lambda,G,H}$ sending π to $\pi|_H$. As we have already remarked, the extension of $\rho \in \mathcal{F}_{\Lambda,G,H}(A)$ to $\pi \in \mathcal{F}_\Lambda(A)$ is unique if n is prime to p. Thus in this case, the morphism of functors is an isomorphism of functors. Therefore $(R_G, \rho_G) \cong (\mathrm{Im}(\alpha)\Lambda, \alpha\rho_H)$. Thus we get

Theorem 3.5. *Suppose* (AI_H) *and that either* n *is prime to* p *or* $[\alpha\rho_H]$ *vanishes in* $H^2(\Delta, \widehat{\mathbb{G}}_m(B))$ *for a flat extension* B *of* $\mathrm{Im}(\alpha)$*. Then* $\mathcal{F}_{\Lambda,G,H}$ *is representable by* $(\mathrm{Im}(\alpha)\Lambda_G, \alpha\rho_H)$*. Moreover if* n *is prime to* p*, we have the equality* $R_G = \mathrm{Im}(\alpha)\Lambda_G$*.*

Since α restricted to Λ_H coincides with the algebra homomorphism induced by the inclusion $H \subset G$, $\alpha(\Lambda_H) \subset \Lambda$. We put $R' = \mathrm{Im}(\alpha) \otimes_{\Lambda_H} \Lambda$. By definition, the character $1 \otimes \det(\rho_G)$ of G coincides on H with $(\alpha \circ \det(\rho_H)) \otimes 1$ in R'. Thus $\alpha\rho_H$ can be extended uniquely to $\rho'_G : G \to GL_n(R')$ such that $\det(\rho'_G) = 1 \otimes \det(\rho_G)$ if n is prime to p. Thus we have a natural map $\iota : R_G \to R'$ such that $\iota\rho_G = \rho'_G$. Since R_G is an algebra over Λ and $\mathrm{Im}(\alpha)$, it is an algebra over R'. Thus we have the structural morphism $\iota' : R' \to R_G$. By Theorem 3.5, ι' is surjective. By definition, $\iota\alpha\rho_H = \iota\rho_H|_H = \iota\rho'_G|_H = \alpha\rho_H \otimes 1$ and $\iota\det(\rho_G) = \det(\rho'_G) = 1 \otimes \det(\rho_G)$. Thus $\iota'\iota\alpha\rho_H = \iota'(\alpha\rho_H \otimes 1) = \alpha\rho_H$ and $\iota'\iota\det(\rho_G) = \iota'(1 \otimes \det(\rho_G)) = \det(\rho_G)$. Thus $\iota'\iota$ is identity on Λ and $\mathrm{Im}(\alpha)$, and hence $\iota'\iota = id$. Similarly, $\iota\iota'\rho'_g = \iota\rho_G = \rho'_G$. This shows that

$$\iota\iota'(\alpha\rho_H \otimes 1) = \iota(\alpha\rho_H) = (\alpha\rho_H \otimes 1) \text{ and}$$
$$\iota\iota'(1 \otimes \det(\rho_G)) = \iota(\det(\rho_G)) = 1 \otimes \det(\rho_G).$$

Thus $\iota\iota'$ is again identity on $\mathrm{Im}(\alpha) \otimes 1$ and $1 \otimes \Lambda$, and $\iota\iota' = id$. Let X_p (resp. $X^{(p)}$) indicate the maximal p–profinite (resp. prime–to–p profinite) quotient of a profinite group X. Write ω for the restriction of $\det(\rho_G)$ to $(G^{ab})^{(p)}$. Define $\kappa : G^{ab} \to W[[G_p^{ab}]]^\times$ by $\kappa(g) = \omega(g)[g_p]$ for the projection g_p of g into G_p^{ab}, where $[x]$ denotes the group element of $x \in G_p^{ab}$ in the group algebra. Assuming that $\mathbb{F}$ is big enough to contain all g–th roots of unity for the order g of $\mathrm{Im}(\omega)$, we can perform the same argument replacing $(\Lambda_H, \Lambda_G, \det(\rho_G))$ by $(W[[H_p^{ab}]], W[[G_p^{ab}]], 1\otimes\kappa)$. Thus we get

Corollary 3.6. *Suppose* (AI_H) *and that* n *is prime to* p. *Then we have*

$$(R_G, \rho_G) \cong (\mathrm{Im}(\alpha)\otimes_{\Lambda_H}\Lambda_G, \alpha\rho_H\otimes\det(\rho_G))$$
$$\cong (\mathrm{Im}(\alpha)\otimes_{W[[H_p^{ab}]]} W[[G_p^{ab}]], \alpha\rho_H\otimes\kappa).$$

In particular, R_G *is flat over* $\mathrm{Im}(\alpha)$.

Exercise 3.7.
1. *Show that if* $H^2(\Delta,\mathbb{F})=0$, $H^2(\Delta,\widehat{\mathbb{G}}_m(A))=0$ *for all* A *in* CNL_W. *Hint:* $\widehat{\mathbb{G}}_m(A)$ *has a* Δ*–invariant filtration whose subquotients are isomorphic to* $\mathbb{F}$*;*
2. *Show that* $\mathcal{F}_H^{\Delta}$ *is representable in* CNL_W*;*
3. *Show that* $\mathcal{F}_H^{\Delta}$ *is represented by* $R_{H,\Delta}$.

3.2. **Nearly ordinary deformations.** Hereafter we assume that $n=2$. We would like to describe nearly p–ordinary Galois deformations. Let us first introduce some notation: let $S=S_G$ be a finite set of closed subgroups of G. For each $D\in S$, let $S(D)$ be a complete representative set for H–conjugacy classes of $\{gDg^{-1}\cap H \mid g\in G\}$. In application, $G=\mathfrak{G}_F$ for a number field F and D is given by decomposition subgroups of primes in S for a finite set of primes S. For simplicity, we assume that $D\cap H\in S(D)$ always. Then the disjoint union $S_H=\bigsqcup_{D\in S}S(D)$ is a finite set, because $|S(D)|=|H\backslash G/D|$.

Let $V=W^2$ be rank 2–free W–modules made of column vectors. We identify $GL_2(W)$ with the group of W–linear automorphisms $Aut_W(V)$. Then the algebraic group $GL(2)$ defined over W can be regarded as a covariant functor from CL_W into the category of groups given by $GL_2(A)=Aut_A(V\otimes_W A)$. An algebraic subgroup $B\subset GL(2)$ is called the *Borel subgroup* defined over W if there exists an W–submodule $W\subset V$ with $V/W\cong W$ such that

$$B(A)=\left\{x\in GL_2(A)\middle| x(W(A))\subset W(A)\right\},$$

where $W(A)=W\otimes_W A\subset V\otimes_W A=V(A)$. Thus any two Borel subgroups defined over W are conjugate each other by an element in $GL_2(W)$.

Let $\{B_D\}_{D\in S}$ be a set of Borel subgroup of $GL(2)_{/W}$ defined over W indexed by $D\in S$. For each $D'\in S(D)$ such that $D'=H\cap gDg^{-1}$, we define $B_{D'}=c(g)P_Dc(g)^{-1}$ for a lift $c(g)\in GL_n(W)$ of $\overline{\rho}(g)$. Now we impose the following additional condition to our deformation problem: We assume

(NO) $$\overline{\rho}(D)\subset P_D(\mathbb{F}) \text{ for each } D\in S_G.$$

Then we consider the following condition:

(no_H) there exists $g_D\in\widehat{GL}_2(A)$ for each $D\in S_H$ such that

$$g_D\rho(D)g_D^{-1}\subset B_D(A),$$

where $\widehat{GL}_n(A)=1+\mathfrak{m}_AM_n(A)$.

We define a subfunctor $\mathcal{F}_X^{n.ord}$ of the functor $\mathcal{F}_X$ by

$$\mathcal{F}_X^{n.ord}(A)=\{\rho\in\mathcal{F}_X(A)\mid \rho \text{ satisfies } (\mathrm{no}_X)\},$$

where X denotes either G or H depending on the group concerned. Then by (NO), (no_X) and our choice of B_D, $\mathcal{F}_X^{n.ord}(\mathbb{F})=\{\overline{\rho}|_X\}\neq\emptyset$.

For each $D \in S_H$, we have $B_D \subset GL(2)$ fixing rank 1 W–free module $W_D \subset V$. Suppose (no$_H$) for $\rho \in \mathcal{F}_X^{n.ord}(A)$. Then $\rho(D)$ leaves $g_D^{-1}W_D(A)$ stable. Thus $\rho(d)$ for $d \in D$ induces a scalar multiplication on $g_D^{-1}W(A) \cong W(A)$ and $g_D^{-1}V(A)/g_D^{-1}W(A) \cong V(A)/W(A)$. In other words, $\rho(d)w = \epsilon_{D,\rho}(d)w$ for $w \in g_D^{-1}W(A)$ and $\rho(d)v = \delta_{D,\rho}(d)v$ for $v \in g_D^{-1}V(A)/g_D^{-1}W(A)$. The map $\epsilon_\rho, \rho_\rho : D \to A^\times$ are continuous characters and are, respectively, deformations of $\overline{\epsilon}_D = \epsilon_{D,\overline{\rho}}$ and $\overline{\delta}_D = \delta_{D,\overline{\rho}}$. We consider the regularity condition:

$$(\mathrm{Rg}_D) \qquad \overline{\epsilon}_D \neq \overline{\delta}_D \quad \text{on } D \in S_H.$$

We can prove in exactly the same manner as in the proof of Proposition 2.9 the following fact:

Proposition 3.8. *Suppose* (AI$_H$), (NO) *and* (Rg$_H$) *for* $\overline{\rho}$. *Then the functor* $\mathcal{F}_X^{n.ord}$ *is representable by a universal couple* $(R_X^{n.ord}, \varrho_X^{n.ord})$ *in* CNL_W.

In the same manner as in the previous subsection, we can check that Δ acts on $\mathcal{F}_H^{n.ord}$ via $\rho \mapsto \rho^{[\sigma]}$. Take $D \in S$ and put $D' = D \cap H \in S(D)$. Since $\overline{\rho}$ is invariant under Δ and $\overline{\rho} \in \mathcal{F}_G^{n.ord}(\mathbb{F})$,

$$(\mathrm{Inv}) \qquad \overline{\epsilon}_{D'}^{[\sigma]} = \overline{\epsilon}_{D'} \text{ and } \overline{\delta}_{D'}^{[\sigma]} = \overline{\delta}_{D'} \text{ for all } \sigma \in D.$$

Now suppose $\rho \in \mathcal{F}_H^{\Delta,n.ord}(A)$ and $[\rho] = 0$ in $H^2(\Delta, \widehat{\mathbb{G}}_m(B))$ for a flat A–algebra B. Then we find an extension $\pi : G \to GL_n(B)$ of ρ. Let $\sigma \in D$ and $D' = H \cap D$. Thus $\pi(\sigma)\rho(d')\pi(\sigma)^{-1} = \rho(\sigma d' \sigma^{-1}) \in g_{D'}^{-1}B_D(A)g_{D'}$ for all $d' \in D'$ and hence

$$\epsilon_{D',\rho}(d') = \epsilon_{D',\rho}(\sigma d' \sigma^{-1}) \text{ and } \delta_{D',\rho}(d') = \delta_{D',\rho}(\sigma d' \sigma^{-1}).$$

By taking $d' \in D'$ with $\overline{\epsilon}_{D'}(d') \neq \overline{\delta}_{D'}(d')$, the above equalities implies $\pi(\sigma)$ has to be upper triangular (if we take a base of $V(\rho) \otimes_A B$ so that $g_{D'}^{-1}B_D(B)g_{D'}$ is upper triangular). Thus $\pi(D) \subset g_{D'}^{-1}B_D(B)g_{D'}$, and, taking $g_D = g_{D'}$, we confirm that $\pi \in \mathcal{F}_G^{n.ord}(A)$. Since $\mathcal{F}_G^{n.ord}$ is stable under the action of $\widehat{\Delta}$, all the arguments given for $\mathcal{F}_X$ in the previous paragraph are valid for $\mathcal{F}_X^{n.ord}$ for $X = G$ and H. Writing $(R_X^{n.ord}, \rho_X^{n.ord})$ for the universal couple representing $\mathcal{F}_X^{n.ord}$, we conclude

Theorem 3.9. *Suppose* (AI$_H$), (Rg$_D$) *for all* $D \in S_H$ *and that* n *is prime to* p. *Then we have the equality* $R_G^{n.ord} = \mathrm{Im}(\alpha^{n.ord})\Lambda_G^{n.ord}$, *where* $\alpha^{n.ord} : R_H^{n.ord} \to R_G^{n.ord}$ *is the base-change map given by* $\alpha^{n.ord}\rho_H^{n.ord} \sim \rho_G^{n.ord}|_H$ *and* $\Lambda_G^{n.ord}$ *is the image of* $W[[G_p^{ab}]]$ *in* $R_G^{n.ord}$. *Moreover we have*

$$(R_G^{n.ord}, \rho_G^{n.ord}) \cong (\mathrm{Im}(\alpha^{n.ord}) \otimes_{W[[H_p^{ab}]]} W[[G_p^{ab}]], \alpha^{n.ord}\rho_H^{n.ord} \otimes \kappa).$$

One can generalize the notion of nearly ordinary representation to $GL(n)$–representations, requiring to have $\rho(D) \subset g_D^{-1}P_D(A)g_D$ for a proper parabolic subgroup $P_D \subset GL(n)$ defined over W.

Exercise 3.10. (1) *Show that* $\mathcal{F}_H^{n.ord}$ *is representable under (AI$_H$) and (Rg$_D$);*
(2) *Show that* $\pi(\sigma) \in g_{D'}^{-1}P_D(B)g_{D'}$ *under (Rg$_{D'}$).*

3.3. **Ordinary deformations.** In this subsection, we continue to assume that $n = 2$ and all B_D are conjugate to the subgroup made of upper triangular matrices. Fix a normal closed subgroup $I = I_D$ of each $D \in S$. For $D' = gDg^{-1} \cap H \in S(D)$, we put $I_{D'} = gI_Dg^{-1} \cap H$. We call $\rho \in \mathcal{F}_X^{n.ord}(A)$ ordinary if ρ satisfies the following conditions:

(Ord$_X$) $\qquad I \subset \mathrm{Ker}(\delta_{D,\rho})$ for every $D \in S_X$.

We then consider the following subfunctor $\mathcal{F}_X^{ord}$ of $\mathcal{F}_X^{n.ord}$:

$$\mathcal{F}_X^{ord}(A) = \{\rho \in \mathcal{F}_X^{n.ord}(A) \mid \rho \text{ is ordinary}\}.$$

It is easy to see that the functor $\mathcal{F}_X^{ord}$ is representable by $(R_X^{ord}, \rho_X^{ord})$ under (Rg$_D$) for every $D \in S_X$ (see Proposition 2.9).

Let $\rho \in \mathcal{F}_H^{ord}(A)$. Suppose $[\rho] = 0$ in $H^2(\Delta, \widehat{\mathbb{G}}_m(B))$ for a flat A–algebra B. Then we have at least one extension π of ρ in $\mathcal{F}_G^{n.ord}(B)$. We consider $\delta_{D,\pi} : D \to A^\times$ for $D \in S$. We suppose one of the following two conditions for each $D \in S$:

- (Tr$_D$) $|I_D/I_D \cap H|$ is prime to p ;
- (Ex$_D$) Every p–power order character of $I_D/I_D \cap H$ can be extended to a character of Δ having values in a flat extension B' of B so that it is trivial on $I_{D'}$ for all $D' \in S$ different from D.

Under (Tr$_D$), as a homomorphism of groups, $\delta_{D,\pi}$ restricted to I_D factors through $\overline{\delta}_{D,\rho}$ which is trivial on I. Thus $\delta_{D,\pi}$ is trivial on I_D. We note that $\delta_{D,\pi}$ is of p–power order on $I_D/H \cap I_D$ because $\overline{\delta}_{D,\rho}$ is trivial on I_D and $\delta_{D,\rho}$ is trivial on $I_D \cap H$. Thus we may extend $\delta_{D,\pi}$ to a character η of Δ congruent 1 modulo $\mathfrak{m}_{B'}$. Then we twists π by η^{-1}, getting an extension $\pi' = \pi \otimes \eta^{-1}$ such that $\delta'_{D,\pi}$ is trivial on I_D. Repeating this process for the D's satisfying (Ex$_D$), we find an extension $\pi \in \mathcal{F}_G^{ord}(B)$ for a flat extension B of A. We now consider

$$\mathcal{F}_{G,H}^{ord}(A) = \{\rho|_H \in \mathcal{F}_H^{ord}(A) \big| \rho \in \mathcal{F}_G^{ord}(B) \text{ for a flat extension } B \text{ of } A\}.$$

In the same manner as in 3.1, if either $p > 2 = n$ or $[\alpha^{ord}\rho_H^{ord}] = 0$ in $H^2(\Delta, \widehat{\mathbb{G}}_m(B))$ for a flat extension B of $\mathrm{Im}(\alpha^{ord})$ in CNL_W, we know that $\mathcal{F}_{G,H}^{ord}$ is represented by $(\mathrm{Im}(\alpha^{ord}), \alpha^{ord}\rho_H^{ord})$, where $\alpha^{ord} : R_H^{ord} \to R_G^{ord}$ is an W–algebra homomorphism given by $\alpha^{ord}\rho_H^{ord} \sim \rho_G^{ord}|_H$.

Let $\rho \in \mathcal{F}_{G,H}^{ord}(A)$ and π be its extension in $\mathcal{F}_G^{ord}(B)$ for a flat A–algebra B in CNL_W. The character $\det(\pi)$ is uniquely determined by ρ on the subgroup of G_p^{ab} generated by all $I_{D,p}$, because another choice is $\pi \otimes \chi$ for a character χ of Δ and $(\delta)_{D,\pi\otimes\chi} = \chi$ on $I_{D,p}$. If G_p^{ab} is generated by the $I_{D,p}$'s and H_p, $\det(\pi)$ is uniquely determined by ρ. Thus assuming that $p > 2$, π itself is uniquely determined by ρ. Therefore the morphism of functors: $\mathcal{F}_G^{ord} \to \mathcal{F}_{G,H}^{ord}$ given by $\rho \mapsto \rho|_H$ identifies $\mathcal{F}_G^{ord}$ with a subfunctor of $\mathcal{F}_{G,H}^{ord}$, inducing a surjective W–algebra homomorphism $\beta : \mathrm{Im}(\alpha^{ord}) \to R_G^{ord}$ such that $\rho_G^{ord}|_H = \beta\alpha\rho_H^{ord}$. Since $\rho_G^{ord}|_H = \alpha\rho_H^{ord}$, β is the identity on $\mathrm{Im}(\alpha^{ord})$, and we conclude that $\mathrm{Im}(\alpha^{ord}) = R_G^{ord}$. This implies

Theorem 3.11. *Suppose that $n = 2$ and $p > 2$. Suppose* (AI$_H$), (Rg$_D$) *for $D \in S_H$ and either* (Tr$_D$) *or* (Ex$_D$) *for each $D \in S$. Suppose further that the $I_{D,p}$'s for all $D \in S$ and H_p generate G_p^{ab}. Then we have $\mathrm{Im}(\alpha^{ord}) = R_G^{ord}$. In particular, for any deformation $\rho \in \mathcal{F}_{G,H}^{ord}(A)$, there is a unique extension $\pi \in \mathcal{F}_G^{ord}(A)$ such that*

$\pi|_H = \rho$. If further $[\rho_H^{\Delta,ord}] = 0$ in $H^2(\Delta, \widehat{\mathbb{G}}_m(B))$ for a flat extension B of $R_{H,\Delta}^{ord}$, then

$$R_{H,\Delta}^{ord} \cong \mathrm{Im}(\alpha^{ord}) = R_G^{ord},$$

where $R_{H,\Delta}^{ord} = R_H^{ord}/\Sigma_{\sigma\in\Delta} R_H^{ord}([\sigma]-1)R_H^{ord}$.

3.4. **Deformations with fixed determinant.** We take a character $\chi : G \to W^\times$ such that $\chi \equiv \det(\overline{\rho}) \mod \mathfrak{m}_W$. We then define

$$\mathcal{F}_X^{\chi,?}(A) = \left\{\rho \in \mathcal{F}_X^?(A) \middle| \det(\rho) = \chi|_X\right\}.$$

Supposing the representability of $\mathcal{F}_X^?$, it is easy to check that $\mathcal{F}_X^{\chi,?}$ is representable. Since the determinant is already fixed and can be extended to G, by the argument in the previous subsections shows that if n is prime to p,

$$\mathcal{F}_H^{\chi,?,\Delta} = \mathcal{F}_{G,H}^{\chi,?} = \mathcal{F}_G^{\chi}.$$

Write $(R_X^{\chi,?}, \rho_X^{\chi,?})$ for the universal couple representing $\mathcal{F}_X^{\chi,?}$ and define $\alpha^{\chi,?} : R_H^{\chi,?} \to R_G^{\chi,?}$ so that $\alpha^{\chi,?}\rho_H^{\chi,} \sim \rho_G^{\chi,?}$. Then we have

Proposition 3.12. *Suppose* (AI_H), (Rg_D) *for $D \in S_H$ and that n is prime to p. Then we have*

$$R_H^{\chi,?}/\Sigma_{\sigma\in\Delta} R_H^{\chi,?}([\sigma]-1)R_H^{\chi,?} = R_{G,H}^{\chi,?} \cong \mathrm{Im}(\alpha^{\chi,?}) = R_G^{\chi,?},$$

where $R_G^{\chi,?}$ is either R_G^{χ} or $R_G^{\chi,n.ord}$.

3.5. **Base Change.** We now apply the results obtained in the previous section to Galois deformations in the following setting: Fix an odd prime p. We take a continuous Galois representation $\overline{\rho}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ into $GL_2(\mathbb{F})$ for a finite field $\mathbb{F}$ of characteristic p. Since $\overline{\rho}$ is continuous, it factors through the Galois group $\mathfrak{G} = \mathfrak{G}_F$ of the maximal extension of $\mathbb{Q}$ unramified outside a finite set of primes S. In this book, for simplicity, we take $S = \{p, \infty\}$, although our ideas certainly work well in a more general setting. Let $\mathfrak{H}$ be a closed normal subgroup of $\mathfrak{G}$. Thus $\Delta = \mathfrak{G}/\mathfrak{H} = \mathrm{Gal}(F/\mathbb{Q})$. We fix a valuation ring W finite flat over $\mathbb{Z}_p$ with residue field $\mathbb{F}$ and consider the category $CNL = CNL_W$ of complete noetherian local $W-$algebras with residue field $\mathbb{F}$.

3.6. **Various deformation rings.** A deformation of $\overline{\rho}|_{\mathfrak{H}}$ is a continuous representation $\rho : \mathfrak{H} \to GL_2(A)$ for an object A of CNL such that $\rho \bmod \mathfrak{m}_A = \overline{\rho}$. We call a deformation ρ nearly p–ordinary, if for a decomposition subgroup $D_{\mathfrak{p}}$ of $\mathfrak{H}$ at each p–adic place $\mathfrak{p}$, ρ restricted to $D_{\mathfrak{p}}$ is isomorphic to an upper triangular representation. Thus we have two characters $\epsilon_{D_{\mathfrak{p}},\rho}$ and $\delta_{D_{\mathfrak{p}},\rho}$ of $D_{\mathfrak{p}}$ realized as diagonal entries. We then consider the following two deformation functors $\mathcal{F} = \mathcal{F}_F : CNL \to SETS$ given by

$$\mathcal{F}_F(A) = \{\rho : \mathfrak{H} \to GL_2(A) \text{ is a deformation of } \overline{\rho}\}/\sim,$$
$$\mathcal{F}_F^{n.ord}(A) = \{\rho \in \mathcal{F}_F(A) \text{ is nearly } p\text{-ordinary}\}.$$

It has been shown in Theorem 2.7 that $\mathcal{F}_F$ is representable in CL_W under the following condition:

(AI_F) $\qquad$ $\overline{\rho}$ restricted to $\mathfrak{H}$ is absolutely irreducible.

If further $[F:\mathbb{Q}]$ is finite (that is, $\mathfrak{H}$ is open in $\mathfrak{G}$), the group satisfies (Φ) and hence, the functor is representable in CNL_W (see Proposition 2.14). In addition to the above condition, to assure the representability of $\mathcal{F}_F^{n.ord}$, we need to assume

$$(\mathrm{Rg}_F) \qquad \overline{\epsilon}_{D_\mathfrak{p}} = \epsilon_{D_\mathfrak{p},\overline{\rho}} \text{ and } \overline{\delta}_{D_\mathfrak{p}} = \delta_{D_\mathfrak{p},\overline{\rho}} \text{ are distinct for each } \mathfrak{p}.$$

When representable, write (R_F, ϱ_F) (resp. $(R_F^{n.ord}, \varrho_F^{n.ord})$) for the universal couple representing $\mathcal{F}_F$ (resp. $\mathcal{F}_F^{n.ord}$). When we consider a deformation problem with restriction "?", (for example $? = n.ord$), we write $(R_F^?, \varrho_F^?)$ for the universal couple with the condition "?". We list here two more restrictions we would like to study: We call a nearly p–ordinary deformation ρ p–ordinary if $\delta_{D,\rho}$ is unramified for every decomposition subgroup D of $\mathfrak{H}$ over p. For a given character $\chi : \mathfrak{G} \to W^\times$, we say that a deformation ρ has fixed determinant χ if $\det\rho = \chi$ in $A^\times$. Then we define the following subfunctors of $\mathcal{F}_F$:

$$\mathcal{F}_F^{ord}(A) = \{\rho \in \mathcal{F}_F^{n.ord}(A) | \rho \text{ is } p\text{-ordinary}\}$$
$$\mathcal{F}_F^{\chi}(A) = \{\rho \in \mathcal{F}_F(A) | \det(\rho) = \chi\}$$
$$\mathcal{F}_F^{\chi,n.ord}(A) = \mathcal{F}_F^{\chi}(A) \cap \mathcal{F}_F^{n.ord}(A), \quad \mathcal{F}_F^{\chi,ord}(A) = \mathcal{F}_F^{\chi}(A) \cap \mathcal{F}_F^{ord}(A).$$

It is easy to check that the above subfunctors of $\mathcal{F}_F^{n.ord}$ are representable under (AI_F) and (Rg_F), and $\mathcal{F}_F^{\chi}$ is representable under (AI_F) (cf. Proposition 2.9).

For the moment, we assume that $[F:\mathbb{Q}] < \infty$. Let $\mathfrak{H}^{ab} = \mathfrak{H}/\overline{(\mathfrak{H},\mathfrak{H})}$ be the maximal (*continuous*) abelian quotient. We write $\mathfrak{H}_p^{ab}$ for the maximal p–profinite quotient of $\mathfrak{H}^{ab}$. Thus $\mathfrak{H}^{ab} = \mathfrak{H}_p^{ab} \times \mathfrak{H}_{ab}^{(p)}$, and by class field theory, $\mathfrak{H}_p^{ab} \cong \mathbb{Z}_p^d \times \mu$ for a finite p–group μ, where d is an integer with $1 \le d < [F:\mathbb{Q}]$. Then as seen in Proposition 2.3, the functor $\mathcal{F}_{F,\det(\overline{\rho})}$ obtained by replacing $\overline{\rho}$ by $\det(\overline{\rho})$ is represented by the continuous group algebra $(W[[\mathfrak{H}_p^{ab}]], \kappa)$ for a suitable character κ with $\kappa(h) = h$ for $h \in \mathfrak{H}_p^{ab}$. Since

$$\det(\varrho_F^?) \in \mathcal{F}_{F,\det(\overline{\rho})}(R_F^?) \cong \mathrm{Hom}_{CNL}(W[[\mathfrak{H}_p^{ab}]], R_F^?),$$

there is a unique W–algebra homomorphism $\iota^? : W[[\mathfrak{H}_p^{ab}]] \to R_F^?$ such that $\iota^?\kappa = \det(\varrho_F^?)$. Thus R_F is an $W[[\mathfrak{H}_p^{ab}]]$–algebra. Similarly, since $\varrho_\mathbb{Q}^? \in \mathcal{F}_\mathbb{Q}^?(R_\mathbb{Q}^?)$, we see $\varrho_\mathbb{Q}^?|_\mathfrak{H} \in \mathcal{F}_F^?(R_\mathbb{Q}^?)$. Thus there exists a unique W–algebra homomorphism $\alpha^? : R_F^? \to R_\mathbb{Q}^?$ such that

$$\alpha^? \circ \varrho_F^? = \varrho_\mathbb{Q}^?|_\mathfrak{H}.$$

We call $\alpha^?$ the base change map (of Galois side). We now describe $\mathrm{Im}(\alpha^?)$ and $\mathrm{Ker}(\alpha^?)$ using the result in the previous section. For that, we take a complete representative set Δ' in $\mathfrak{G}$ for $\Delta = \mathfrak{G}/\mathfrak{H}$. Then we lift $\overline{\rho}(\sigma)$ $(\sigma \in \Delta')$ to an element $c(\sigma) \in GL_n(W)$ so that $c(\sigma) \bmod \mathfrak{m}_W = \overline{\rho}(\sigma)$. Then we let Δ act on $\mathcal{F}_F$ by $\rho^\sigma(g) = c(\sigma)^{-1}\rho(\sigma g \sigma^{-1})c(\sigma)$. This is a well defined functorial action on $\mathcal{F}_F^?$. By universality, Δ acts on $R_F^?$ via W–algebra automorphisms. We consider the following condition:

$$(\mathrm{TR}) \qquad p \text{ totally ramifies in } F/\mathbb{Q}.$$

Thus we have from the results in previous sections the following fact:

Theorem 3.13 (Base change theorem)**.** *Let F be a finite Galois extension of $\mathbb{Q}$ (with $\Delta = \mathrm{Gal}(F/\mathbb{Q})$) unramified outside $\{p,\infty\}$. We suppose* (AI_F) *and* (Rg_F) *for $\overline{\rho}$.*

(i) *If ? = ∅ or n.ord, suppose either that $H^2(\Delta,\mathbb{F}) = 0$ or that Δ is cyclic. Then we have*

$$R^?_{\mathbb{Q}} \cong \mathrm{Im}(\alpha^?) \otimes_{W[[\mathfrak{H}_p^{ab}]]} W[[\mathfrak{G}_p^{ab}]] \quad \textit{and} \quad \mathrm{Ker}(\alpha^?) = \sum_{\sigma\in\Delta} R^?_F(\sigma-1)R^?_F.$$

(ii) *If ? = χ, suppose that p is odd. Then we have*

$$R^\chi_{\mathbb{Q}} \cong R^\chi_F / \sum_{\sigma\in\Delta} R^\chi_F(\sigma-1)R^\chi_F.$$

(iii) *If ? = ord, suppose* (TR), *$p > 2$ and either that $H^2(\Delta,\mathbb{F}) = 0$ or Δ is cyclic. Then we have*

$$R^{ord}_{\mathbb{Q}} \cong R^{ord}_F / \sum_{\sigma\in\Delta} R^{ord}_F(\sigma-1)R^{ord}_F.$$

In all the above cases, Spec$(\mathrm{Im}(\alpha^?))$ *is isomorphic to the maximal closed subscheme of Spec*$(R^?_F)$ *fixed under* Δ.

We study the relation among the various subfunctors of $\mathcal{F}_F$. Suppose that p is odd and that χ mod $\mathfrak{m}_W = \det(\overline{\rho})$. Then we have a natural transformation for ? = ∅ or *n.ord*: $\mathcal{F}^?_{F,\overline{\rho}} \to \mathcal{F}^{\chi,?}_F \times \mathcal{F}_{F,\det(\overline{\rho})}$ given by $\rho \mapsto (\rho^\chi, \det(\rho))$, where

$$\rho^\chi = \rho \otimes (\det(\rho)^{-1}\chi)^{1/2}.$$

Note here that $\det(\rho)^{-1}\chi$ is of p–power order with p odd, and hence its square root is uniquely determined. By this remark, we can recover ρ from $(\rho^\chi, \det(\rho))$. Thus we have $\mathcal{F}^?_{F,\overline{\rho}} \cong \mathcal{F}^{\chi,?}_F \times \mathcal{F}_{F,\det(\overline{\rho})}$ and hence

$$R^?_F \cong R^{\chi,?}_F \widehat{\otimes}_W W[[\mathfrak{H}_p^{ab}]] \cong R^{\chi,?}_F[[\mathfrak{H}_p^{ab}]].$$

When $F = \mathbb{Q}$, the restriction of a character ξ of D to the inertia subgroup I has a unique extension $\xi^{\mathfrak{G}}$ to $\mathfrak{G}$, because the image of I in D^{ab} is naturally isomorphic to $\mathfrak{G}^{ab}$. Then, assuming that $\overline{\rho}$ is p–ordinary, we see that $\rho \mapsto (\rho \otimes (\delta^{-1}_{D,\rho})^{\mathfrak{G}}, (\delta_{D,\rho})^{\mathfrak{G}})$ induces a natural transformation: $F^{n.ord}_{\mathbb{Q}} \cong \mathcal{F}^{ord}_{\mathbb{Q}} \times \mathcal{F}_{\mathbb{Q},(\delta_{D,\overline{\rho}})^{\mathfrak{G}}}$. Thus we get

$$R^{n.ord}_{\mathbb{Q}} \cong R^{ord}_{\mathbb{Q}} \widehat{\otimes}_W W[[\Gamma]] \cong R^{ord}_{\mathbb{Q}}[[\Gamma]],$$

where we have written Γ for $\mathfrak{G}_p^{ab}$ ($\cong 1 + p\mathbb{Z}_p$ if p is odd) following the tradition in the Iwasawa theory. We summarize the above argument into the following

Proposition 3.14. *Suppose the assumption of Theorem 3.13 depending on the restriction "?". Suppose that χ mod $\mathfrak{m}_W = \det(\overline{\rho})$. Then we have the following canonical isomorphisms:*

(i) *For ? = ∅ or n.ord,*

$$R^?_F \cong R^{\chi,?}_F \widehat{\otimes}_W W[[\mathfrak{H}_p^{ab}]] \cong R^{\chi,?}_F[[\mathfrak{H}_p^{ab}]].$$

(ii) *Suppose that $\overline{\rho}$ is p–ordinary. Then*

$$R^{n.ord}_{\mathbb{Q}} \cong R^{ord}_{\mathbb{Q}} \widehat{\otimes}_W W[[\Gamma]] \cong R^{ord}_{\mathbb{Q}}[[\Gamma]].$$

In particular, we have a canonical isomorphism (if $F = \mathbb{Q}$):

$$R^{ord}_{\mathbb{Q}} \cong R^\chi_{\mathbb{Q}}$$

under the assumptions of (i) and (ii).

References

Books

[CRT] H. Matsumura, *Commutative Ring Theory*, Cambridge studies in advanced mathematics **8**, Cambridge Univ. Press, 1986

[FAN] D. Ramakrishnan and R. J. Valenza, *Fourier Analysis on Number Fields*, GTM **186**, 1999, Springer

[MFG] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, 2000, Cambridge University Press

[MRT] C.W. Curtis and I. Reiner, *Methods of representation theory*, John Wiley and Sons, New York, 1981.

Articles

[Kh10] C. Khare, Serre's conjecture and its consequences. Jpn. J. Math. **5** (2010), 103–125.

[KW09] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture. I, II. I: Invent. Math. **178** (2009), 485–504; II. Invent. Math. **178** (2009), 505–586

[M89] B. Mazur, Deforming Galois representations, MSRI Publications **16** (1989), 385–437

[TW95] R. Taylor and A. Wiles, Ring theoretic properties of certain Hecke algebras, Ann. of Math. **141** (1995), 553–572

[W95] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. **141** (1995), 443–551