NON ABELIAN CLASS NUMBER FORMULAS AND ADJOINT SELMER GROUPS

HARUZO HIDA

Contents

Date: April 15, 2019.
2010 *Mathematics Subject Classification.* primary 11R23, 11F25, 11F33, 11F80; secondary 11F11, 11G18, 11F27.
The author is partially supported by the NSF grant: DMS 1464106.

1. Introduction

We give an overview of what we will do in this topic course. Fix a prime $p \geq 5$. For a number field K, by class field theory, the maximal abelian extension $H_{/K}$ unramifeid everywhere has Galois group canonically isomorphic to the class group Cl_K of K. So Pontryagin dual of $\mathrm{Hom}(Cl_{K,p}, \mathbb{Q}_p/\mathbb{Z}_p) \cong Cl_{K,p}$ can be Galois cohomologically defined

$$\mathrm{Sel}_K = \mathrm{Ker}(H^1(\overline{\mathbb{Q}}/K, \mathbb{Q}_p/\mathbb{Z}_p) \to \prod_l H^1(I_l, \mathbb{Q}_p/\mathbb{Z}_p)).$$

Writing the induced representation $\mathrm{Ind}_K^{\mathbb{Q}}\mathbf{1} = \mathbf{1} \oplus \chi$, we have the celebrated class number formula giving the size $|Cl_K|$ by the integral part of the value $L(1, \chi)$ (Artin L-value) up to a canonical transcendental factor. We have studied in the recent past 207 courses the fundamental question:

$$\text{When } \mathrm{Sel}_K \cong Cl_{K,p} \text{ is cyclic?}$$

(and therefore, the structure of Sel_K is determined by by the value $L(1, \chi)$). Though we do not require any knowledge of past courses, here are links to the lecture notes of the relevant past two courses:

- `http://www.math.ucla.edu/~hida/207b.1.18s/Lec18s.pdf`,
- `http://www.math.ucla.edu/~hida/207a.1.18w/Lec1.pdf`.

There is one more example of proven such formulas giving the size of Selmer groups. Start with a modular form $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$ and suppose f is an eigenform of all Hecke operators $T(n)$; so, $f|T(n) = \lambda(T(n))f$. Each f has its p-adic irreducible Galois representation $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_p[\lambda])$, where $\mathbb{Q}_p[\lambda]$ is the field generated over the p-adic field $\mathbb{Q}_p$ by the eigenvalues $\lambda(T(n))$. Let $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on

$$\mathfrak{sl}_2(\mathbb{Q}_p[\lambda]) = \{x \in M_2(\mathbb{Q}_p[\lambda]) | \mathrm{Tr}(x) = 0\}$$

by conjugation, which results a 3-dimensional Galois representation $Ad(\rho_f)$. In this case, again we have the formula of $|\mathrm{Sel}(Ad(\rho_f))|$ by the L-value $L(1, Ad(\rho_f))$ (a non-abelian class number formula). We explore in this courese the question when $\mathrm{Sel}(Ad(\rho_f))$ is cyclic over $\mathbb{Z}_p[\rho_f]$?

We cover

(1) How to get the non-abelian "class number" formula;
(2) Properties of Galois representations $Ad(\rho_f)$ and ρ_f;
(3) Definitions of $\mathrm{Sel}(Ad(\rho_f))$;
(4) the cyclicity question.

Here is a slightly more detailed sketch of what we are going to do; so, no proofs given (just short explanation of concepts).

1.1. **Hilbert class field.**

Let K be a number field with integer ring $O = O_K$ embedded in $\mathbb{C}$. Let $H_{/K}$ be the Hilbert class field; i.e., the maximal abelian extension unramified everywhere including real places. A real place means any real embedding $K \hookrightarrow \mathbb{R}$ extending to an embedding of H into $\mathbb{R}$.

Define Cl_K to be the group of isomorphism classes of rank 1 projective O-modules M (the group structure is given by tensor product over O). Since $M \hookrightarrow M \otimes_O K \cong K$, we may identify M with a fractional O-ideal in K. Then

$$Cl_K \cong \frac{\text{fractional } O\text{-ideals}}{\text{principal fractional ideals } (\alpha) = \alpha O},$$

which is known to be finite (so, compact; [LFE, Theorem 1.2.1]). By class field theory, we have

$$Cl_K \cong \mathrm{Gal}(H/K) \quad \text{by } \mathfrak{l} \mapsto \mathrm{Frob}_{\mathfrak{l}} \text{ for primes } \mathfrak{l}.$$

1.2. **Dual class group $Cl_K^* = \mathrm{Hom}(Cl_K, \mathbb{Q}/\mathbb{Z})$.** Consider the algebraic closure

$$\overline{K} = \bigcup_{E/K\text{: finite Galois extension}} E$$

of K (E is taken in $\mathbb{C}$). Then $\mathfrak{G}_K = \mathrm{Gal}(\overline{K}/K)$ is a compact group as $\mathfrak{G}_K = \varprojlim_{E/K} \mathrm{Gal}(E/K)$ by restriction maps. Consider $\mathrm{Hom}(\mathfrak{G}_K, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(\mathfrak{G}_K^{ab}, \mathbb{Q}/\mathbb{Z})$ (Pontryagin dual of the maximal continuous abelian quotient $\mathfrak{G}_K^{ab}$). If $\phi : \mathfrak{G}_K \to \mathbb{Q}/\mathbb{Z}$ is unramified at a prime $\mathfrak{l}$, ϕ is trivial on the inertia subgroup $I_{\mathfrak{l}}$ of $\mathfrak{l}$. Thus

$$Cl_K^* = \mathrm{Gal}(H/K)^* := \mathrm{Hom}(\mathrm{Gal}(H/K), \mathbb{Q}/\mathbb{Z}) = \mathrm{Ker}(\mathrm{Hom}(\mathfrak{G}_K, \mathbb{Q}/\mathbb{Z}) \to \prod_{\mathfrak{l}} \mathrm{Hom}(I_{\mathfrak{l}}, \mathbb{Q}/\mathbb{Z})).$$

1.3. **Pontryagin dual.** Consider a profinite group G and a continuous G-module X. Assume that X has either discrete torsion or profinite topology.

For any abelian profinite compact or torsion discrete module X, we define the Pontryagin dual module X^* by $X^* = \mathrm{Hom}_{cont}(X, \mathbb{Q}/\mathbb{Z})$ 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 (e.g., [LFE, 8.3]), we have $(X^*)^* \cong X$ canonically. 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^*.

1.4. **Group cohomology.** 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 assuming all maps are continuous,

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

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

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

Thus if G acts trivially on X, we have $H^1(G, X) = \mathrm{Hom}(G, X)$. If $G = \mathrm{Gal}(E/K)$, we often write $H^j(E/K, X)$, and if $E = \overline{K}$, we write $H^j(K, X)$ for $G = \mathfrak{G}_K$.

1.5. **Compatible system of Galois representations.** A (weakly) compatible system of Galois representations over K with coefficient (number field) T is a system of continuous representation $\rho = \{\rho_{\mathfrak{l}} : \mathfrak{G}_K \to \mathrm{GL}_n(O_{T,\mathfrak{l}})\}$ such that

- There exists a finite set of primes S of K such that $\rho_{\mathfrak{l}}$ is unramified outside S and the residual characteristic l of $\mathfrak{l}$;
- The characteristic polynomial of $\rho_{\mathfrak{l}}(\mathrm{Frob}_{\mathfrak{p}})$ is in $T[X]$ independent of $\mathfrak{l}$ as long as $\mathfrak{p} \notin S \cup \{l\}$.

1.6. **Selmer group.** Let $\rho_{\mathfrak{l}}^{div} = \rho_{\mathfrak{l}} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l/\mathbb{Z}_l$ as a discrete $\mathfrak{G}_K$-module. For a datum $\mathcal{L}$ of subgroup $L_{\mathfrak{q}} \subset H^1(K_{\mathfrak{q}}, \rho_{\mathfrak{l}}^{div})$ for each prime $\mathfrak{q}$ of K, we define

$$\mathrm{Sel}_{\mathcal{L}}(\rho_{\mathfrak{l}}) = \mathrm{Ker}(H^1(K, \rho_{\mathfrak{l}}^{div}) \to \prod_{\mathfrak{q}} H^1(K_{\mathfrak{q}}, \rho_{\mathfrak{l}}^{div})/L_{\mathfrak{q}}).$$

If we take $L_{\mathfrak{q}} := \mathrm{Ker}(H^1(K_{\mathfrak{q}}, \rho_{\mathfrak{l}}^{div}) \to H^1(I_{\mathfrak{q}}, \rho_{\mathfrak{l}}^{div}))$, then

$$\mathrm{Sel}_{\mathcal{L}}(\rho_{\mathfrak{l}}) = \mathrm{Ker}(H^1(K, \rho_{\mathfrak{l}}^{div}) \to \prod_{\mathfrak{q}} H^1(I_{\mathfrak{q}}, \rho_{\mathfrak{l}}^{div})).$$

If ρ is made of trivial representation $\mathbf{1}$ with coefficients in $\mathbb{Q}$,

$$\mathrm{Sel}_K(\mathbf{1}) := \mathrm{Sel}_{\mathcal{L}}(\rho_l) \cong Cl_K^* \otimes_{\mathbb{Z}} \mathbb{Z}_l \quad \text{for the above choice of } \mathcal{L}.$$

By class number formula for an imaginary quadratic field $K = \mathbb{A}[\sqrt{-D}]$, we find, if $l > 3$,

$$|Cl_K \otimes_{\mathbb{Z}} \mathbb{Z}_l| = ||Cl_K||_l^{-1} = |\mathrm{Sel}_K(\mathbf{1})| = |L(0, \chi)|_l$$

for the Dirichlet character $\chi = \left(\frac{-D}{}\right)$. In this case, we can check $\mathrm{Ind}_K^{\mathbb{Q}} \mathbf{1} = \mathrm{Ind}_{\mathfrak{G}_K}^{\mathfrak{G}_{\mathbb{Q}}} \mathbf{1} = \mathbf{1} \oplus \chi$, $\mathrm{Sel}_K(\mathbf{1}) = \mathrm{Sel}_{\mathbb{Q}}(\chi)$ as $\mathrm{Sel}_{\mathbb{Q}}(\mathbf{1}) = 0$; so,

$$|Cl_K \otimes_{\mathbb{Z}} \mathbb{Z}_l| = ||Cl_K||_l^{-1} = |\mathrm{Sel}_{\mathbb{Q}}(\chi)| = |L(0, \chi)|_l.$$

1.7. **A variant of Bloch-Kato conjecture.** Define the L function of ρ by $L(s, \rho) = \prod_{\mathfrak{p}} \det(1 - \rho_{\mathfrak{l}}(\mathrm{Frob}_{\mathfrak{p}})N(\mathfrak{p})^{-s})^{-1}$ and assume analytic continuation and functional equation as predicted by Serre if ρ is associated top a motive (see [HMI, 1.2.1]). If ρ is critical (i.e., the $L(s, \rho)$ does not have a pole at $s = 0$ and the Γ-factor of $L(s, \rho)$ and its counter-part of the functional equation are finite at $s = 0$), we expect

$$|\mathrm{Sel}_{\mathcal{L}}(\rho_{\mathfrak{l}})| = \left|\frac{L(0, \rho_{\mathfrak{l}})}{\text{period}}\right|_l^{-1}$$

for a suitable transcendental factor "**period**" and a suitable data $\mathcal{L}$ (depending on how to define "period").

Thus at least conjecturally we can compute $|\mathrm{Sel}_{\mathcal{L}}(\rho_{\mathfrak{l}})|$. Our main questions are

- Is there any way to determine the structure of $\mathrm{Sel}_{\mathcal{L}}(\rho_{\mathfrak{l}})$?
- Or at least, is there any way to compute the number of generators of $\mathrm{Sel}_{\mathcal{L}}(\rho_{\mathfrak{l}})$ over $O_{T_{\mathfrak{l}}}$?

2. Congruence modules

Start with an n-dimensional compatible system $\rho = \{\rho_{\mathfrak{l}}\}$ of $\mathfrak{G}_K$. For simplicity, we assume that its coefficient field T is $\mathbb{Q}$. Pick a prime p and its member ρ_p (since $\mathfrak{G}_K$ is compact, ρ_p has values in the maximal compact subgroup $\mathrm{GL}_n(\mathbb{Z}_p)$ up to conjugation). Let $\overline{\rho} = \rho_p \mod p; \mathfrak{G}_K \to \mathrm{GL}_n(\mathbb{F}_p)$. A deformation $\varphi : \mathfrak{G}_K \to \mathrm{GL}_n(A)$ for a local $\mathbb{Z}_p$-algebra A is such that $\varphi \mod \mathfrak{m}_A \cong \overline{\rho}$. The universal deformation ring with some specific property P parameterizes all deformations with P. In other words, there exists a universal deformation $\boldsymbol{\rho} : \mathfrak{G}_K \to \mathrm{GL}_n(R)$ with property P such that for any deformation φ as above, there exists a $\mathbb{Z}_p$-algebra homomorphism $\phi : R \to A$ such that $\phi \circ \boldsymbol{\rho} \cong \varphi$. We study the relation between the module of differential $\Omega_{R/\mathbb{Z}_p}$ and a certain Selmer group $\mathrm{Sel}_P(Ad(\boldsymbol{\rho}))$. We start studying differentials for general rings.

2.1. **Set up.**

- W: the base ring which is a DVR over $\mathbb{Z}_p$ with finite residue field $\mathbb{F}$ for a prime $p > 2$.

- For a local W-algebra A sharing same residue field $\mathbb{F}$ with W (i.e., $A/\mathfrak{m}_A = \mathbb{F}$), we write CL_A the category of complete local A-algebras R with $R/\mathfrak{m}_R = \mathbb{F}$ for its maximal ideal $\mathfrak{m}_R$. Morphisms of CL_A are local A-algebra homomorphisms. If A is noetherian, CNL_A is the full subcategory of CL_A of noetherian local rings.

- Fix $R \in CNL_A$. For a continuous R-module M with continuous R–action, define continuous A–*derivations* by

$$Der_A(R, M) = \left\{\delta : R \to M \in \mathrm{Hom}_A(R, M) \middle| \delta\text{: continuous, } \delta(ab) = a\delta(b) + b\delta(a)\ (a, b \in R)\right\}.$$

  Here the A-linearity of a derivation δ is equivalent to $\delta(A) = 0$. The association $M \mapsto Der_A(R, M)$ is a covariant functor from the category $MOD_{/R}$ of continuous R-modules to modules MOD.

2.2. **Differentials.** The differential R-module $\Omega_{R/A}$ is defined as follows: The multiplication $a\otimes b\mapsto ab$ induces a A–algebra homomorphism $m : R\widehat{\otimes}_A R \to R$ taking $a\otimes b$ to ab. We put $I = \mathrm{Ker}(m)$, which is an ideal of $R\widehat{\otimes}_A R$. Then we define $\Omega_{R/A} = I/I^2$. It is an easy exercise to check that the map $d : R \to \Omega_{R/A}$ given by $d(a) = a\otimes 1 - 1\otimes a \mod I^2$ is a continuous A–derivation. Indeed

$$\begin{aligned} a\cdot d(b) + b\cdot d(a) - d(ab) &= ab\otimes 1 - a\otimes b - b\otimes a + ba\otimes 1 - ab\otimes 1 + 1\otimes ab \\ &= ab\otimes 1 - a\otimes b - b\otimes a + 1\otimes ab = (a\otimes 1 - 1\otimes a)(b\otimes 1 - 1\otimes b) \equiv 0 \mod I^2. \end{aligned}$$

We have a morphism of functors:

$$\mathrm{Hom}_R(\Omega_{R/A}, ?) \to Der_A(R, ?) : \ \phi \mapsto \phi\circ d.$$

2.3. **Universality.**

Proposition 2.1. *The above morphism of two functors*

$$M \mapsto \mathrm{Hom}_R(\Omega_{R/A}, M)$$

and $M \mapsto Der_A(R, M)$ is an isomorphism, where M runs over the category of continuous R–modules. In other words, for each A-derivation $\delta : R \to M$, there exists a unique R-linear homomorphism $\phi : \Omega_{R/A} \to M$ such that $\delta = \phi\circ d$.

Proof. The ideal I is generated over R by $d(a)$. Indeed, if $\sum_{a,b} m(a,b)ab = 0$ (i.e., $\sum_{a,b} m(a,b)a\otimes b \in I$), then

$$\begin{aligned} \sum_{a,b} m(a,b)a\otimes b &= \sum_{a,b} m(a,b)a\otimes b - \sum_{a,b} m(a,b)ab\otimes 1 \\ &= \sum_{a,b} m(a,b)a(1\otimes b) - b\otimes 1) = -\sum_{a,b} m(a,b)d(b). \end{aligned}$$

Define $\phi : R\times R \to M$ by $(x,y)\mapsto x\delta(y)$ for $\delta\in Der_A(R,M)$. If $a,c\in R$ and $b\in A$, $\phi(ab,c) = ab\delta(c) = a(b\delta(c)) = b\phi(a,c)$ and $\phi(a,bc) = a\delta(bc) = ab\delta(c) = b(a\delta(c)) = b\phi(a,c)$. Thus ϕ gives a continuous A-bilinear map.

By the universality of the tensor product, $\phi : R\times R \to M$ extends to a A-linear map $\phi : R\widehat{\otimes}_A R \to M$. Now we see that

$$\phi(a\otimes 1 - 1\otimes a) = a\delta(1) - \delta(a) = -\delta(a)$$

and

$$\phi((a\otimes 1 - 1\otimes a)(b\otimes 1 - 1\otimes b)) = \phi(ab\otimes 1 - a\otimes b - b\otimes a + 1\otimes ab) = -a\delta(b) - b\delta(a) + \delta(ab) = 0.$$

This shows that $\phi|_I$-factors through $I/I^2 = \Omega_{R/A}$ and $\delta = \phi\circ d$, as desired. The map ϕ is unique as $d(R)$ generates $\Omega_{R/A}$. □

2.4. **Functoriality.**

Corollary 2.2 (Second fundamental exact sequence)**.**
Let $\pi : R \twoheadrightarrow C$ be a surjective morphism in CL_W, and write $J = Ker(\pi)$. Then we have the following natural exact sequence:

$$J/J^2 \xrightarrow{\beta^*} \Omega_{R/A}\widehat{\otimes}_R C \longrightarrow \Omega_{C/A} \to 0.$$

Moreover if $A = C$, then $J/J^2 \cong \Omega_{R/A}\widehat{\otimes}_R C$.

Proof. By assumption, we have algebra morphism $A \to R \twoheadrightarrow C = R/J$. By the Yoneda's lemma, we only need to prove that

$$\begin{array}{ccccc} Der_A(C,M) & \underset{\hookrightarrow}{\xrightarrow{\alpha}} & Der_A(R,M) & \xrightarrow{\beta} & \mathrm{Hom}_C(J/J^2, M) \\ \wr\downarrow & & \wr\downarrow & & \|\downarrow \\ \mathrm{Hom}_A(\Omega_{C/A}, M) & \longrightarrow & \mathrm{Hom}_A(\Omega_{R/A}\widehat{\otimes}_R C, M) & \longrightarrow & \mathrm{Hom}_C(J/J^2, M) \end{array}$$

is exact for all continuous C–modules M. The first α is the pull back map. Thus the injectivity of α is obvious.

The map β is defined as follows: For a given A-derivation $D : R \to M$, we regard D as a A-linear map of J into M. Since J kills the C-module M, $D(jj') = jD(j') + j'D(j) = 0$ for $j, j' \in J$. Thus D

induces C-linear map: $J/J^2 \to M$. Then for $b \in R$ and $x \in J$, $D(bx) = bD(x) + xD(b) = bD(x)$. Thus D is C-linear, and $\beta(D) = D|_J$.

Now prove the exactness at the mid-term of the second exact sequence. The fact $\beta \circ \alpha = 0$ is obvious. If $\beta(D) = 0$, then D kills J and hence is a derivation well defined on $C = R/J$. This shows that D is in the image of α.

Now suppose that $A = C$. To show injectivity of β^*, we create a surjective C-linear map: $\gamma : \Omega_{R/A} \otimes C \twoheadrightarrow J/J^2$ such that $\gamma \circ \beta^* = \mathrm{id}$.

Let $\pi : R \to C$ be the projection and $\iota : A = C \hookrightarrow R$ be the structure homomorphism giving the A-algebra structure on R. We first look at the map $\delta : R \to J/J^2$ given by $\delta(a) = a - P(a) \mod J^2$ for $P = \iota \circ \pi$. Then

$$\begin{aligned} a\delta(b) + b\delta(a) - \delta(ab) &= a(b - P(b)) + b(a - P(a)) - ab + P(ab) \\ &\overset{P(ab)=P(a)P(b)}{=} ab - aP(b) + ba - bP(a) - ab + P(a)P(b) = (a - P(a))(b - P(b)) \equiv 0 \mod J^2. \end{aligned}$$

Thus δ is a A-derivation.

By the universality of $\Omega_{R/A}$, we have an R-linear map

$$\phi : \Omega_{R/A} \to J/J^2$$

such that $\phi \circ d = \delta$. By definition, $\delta(J)$ generates J/J^2 over R, and hence ϕ is surjective.

Since J kills J/J^2, the surjection ϕ factors through $\Omega_{R/A} \otimes_R C$ and induces γ. Note that $\beta(d \otimes 1_C) = d \otimes 1_C|_J$ for the identity 1_C of C; so, $\gamma \circ \beta^* = \mathrm{id}$ as desired. □

Corollary 2.3. *Let the notation and the assumption be as in* Corollary 2.2. *If we restrict the functor* $M \mapsto Der_A(R, M)$ *to the category* $MOD_{/C}$ *of* C*-modules,* $\Omega_{R/A} \widehat{\otimes}_R C$ *represents* $MOD_{/C} \ni M \mapsto Der_A(R, M)$.

We often write $C_1(\pi; C) := \Omega_{R/A} \widehat{\otimes}_R C$ (which is called the differential module of π).

Proof. By Proposition 2.1, for each $\delta \in Der_A(R, M)$, we find a unique $\phi \in \mathrm{Hom}_R(\Omega_{R/A}, M)$ such that $\phi \circ d = \delta$. If M is a C-module, ϕ factors through $\Omega_{R/A}/J\Omega_{R/A} = \Omega_{R/A} \otimes_R C$.

Conversely, if $\phi \in \mathrm{Hom}_C(\Omega_{R/A} \otimes_R C, M)$ for a C-module M, plainly $\delta = \phi \circ (d \otimes 1)$ gives $Der_A(R, M)$; so, the result follows. □

2.5. **An algebra structure on $R \oplus M$ and derivation.** For any continuous R-module M, we write $R[M]$ for the R-algebra with square zero ideal M. Thus $R[M] = R \oplus M$ with the multiplication given by

$$(r \oplus x)(r' \oplus x') = rr' \oplus (rx' + r'x).$$

It is easy to see that $R[M] \in CNL_W$, if M is of finite type, and $R[M] \in CL_W$ if M is a p-profinite R-module. By definition,

$$Der_A(R, M) \cong \left\{ \phi \in \mathrm{Hom}_{A-alg}(R, R[M]) \middle| \phi \mod M = \mathrm{id} \right\},$$

where the map is given by $\delta \mapsto (a \mapsto (a \oplus \delta(a))$.

Note that $i : R \to R\widehat{\otimes}_A R$ given by $i(a) = a \otimes 1$ is a section of $m : R\widehat{\otimes}_A R \to R$. We see easily that $R\widehat{\otimes}_A R/I^2 \cong R[\Omega_{R/A}]$ by $x \mapsto m(x) \oplus (x - i(m(x)))$. Note that $d(a) = 1 \otimes a - i(a)$ for $a \in R$.

2.6. **Congruence modules.** We assume that A is a domain and R is a reduced finite flat A-algebra. Let $\phi : R \twoheadrightarrow A$ be an onto A-algebra homomorphism. Then the total quotient ring $\mathrm{Frac}(R)$ can be decomposed uniquely

$$\mathrm{Frac}(R) = \mathrm{Frac}(\mathrm{Im}(\phi)) \times X$$

as an algebra direct product. Write 1_ϕ for the idempotent of $\mathrm{Frac}(\mathrm{Im}(\phi))$ in $\mathrm{Frac}(R)$. Let $\mathfrak{a} = \mathrm{Ker}(R \to X) = (1_\phi R \cap R)$, $S = \mathrm{Im}(R \to X)$ and $\mathfrak{b} = \mathrm{Ker}(\phi)$. Here the intersection $1_\phi R \cap R$ is taken in $\mathrm{Frac}(R) = \mathrm{Frac}(\mathrm{Im}(\phi)) \times X$. First note that $\mathfrak{a} = R \cap (A \times 0)$ and $\mathfrak{b} = (0 \times X) \cap R$. Put

$$C_0(\phi; A) = (R/\mathfrak{a}) \otimes_{R,\phi} \mathrm{Im}(\phi) \cong \mathrm{Im}(\phi)/(\phi(\mathfrak{a})) \cong A/\mathfrak{a} \cong R/(\mathfrak{a} \oplus \mathfrak{b}) \cong S/\mathfrak{b} \text{ and } C_1(\phi; C) := \Omega_{R/A} \widehat{\otimes}_R C.$$

The module $C_0(\phi; A)$ is called the *congruence* module of ϕ but is actually a ring. The module $C_1(\phi; A)$ is called the *differential* module of ϕ.

Write $K = \mathrm{Frac}(A)$. Fix an algebraic closure $\overline{K}$ of K. Since the spectrum $\mathrm{Spec}(C_0(\phi; A))$ of the congruence ring $C_0(\phi; A)$ is the scheme theoretic intersection of $\mathrm{Spec}(\mathrm{Im}(\phi))$ and $\mathrm{Spec}(R/\mathfrak{a})$ in $\mathrm{Spec}(R)$:

$$\mathrm{Spec}(C_0(\lambda; A)) = \mathrm{Spec}(\mathrm{Im}(\phi)) \cap \mathrm{Spec}(R/\mathfrak{a}),$$

we conclude that

Proposition 2.4. *Let the notation be as above. Then a prime* $\mathfrak{p}$ *is in the support of* $C_0(\phi; A)$ *if and only if there exists an* A*-algebra homomorphism* $\phi' : R \to \overline{K}$ *factoring through* $R/\mathfrak{a}$ *such that* $\phi(a) \equiv \phi'(a) \mod \mathfrak{p}$ *for all* $a \in R$.

Since ϕ is onto, we see $C_1(\phi; A) = \mathfrak{b}/\mathfrak{b}^2$. We could define $C_n = \mathfrak{b}^n/\mathfrak{b}^{n+1}$. Then $C(\phi; A) = \bigoplus_n C_n(\phi; A)$ is a graded algebra. If $\mathfrak{b}$ is principal, this is a polynomial ring $C_0(\phi; A)[T]$.

Proposition 2.5. *If* A *is a noetherian domain, we have* $\mathrm{Supp}_A(C_0(\phi; A)) = \mathrm{Supp}_A(C_1(\phi; A))$ *and* $\mathrm{Ass}_A(C_0(\phi; A)) = \mathrm{Ass}_A(C_1(\phi; A))$.

For an A-module M, $\mathrm{Supp}_A(M)$ is defined by a Zariski closed subset $\{P \in \mathrm{Spec}(A) | M_P \neq 0\}$ of $\mathrm{Spec}(A)$. Writing $\mathrm{Ann}_A(M) = \{x \in A | xM = 0\}$ (the annihilator ideal of M), we find $\mathrm{Supp}_A(M) = \{P \supset \mathrm{Ann}_A(M) | P \in \mathrm{Spec}(A)\}$ if M is finitely generated over A as an A-module (see [CRT, §4]). The set $\mathrm{Ass}_A(M)$ of associated primes of M is defined to be the set of prime ideals P of A such that $P = \mathrm{Ann}_A(Ax)$ for some $x \in M$.

Proof. For simplicity, we write C_j for $C_j(\phi; A)$. Note that $C_{1,P} = C_1 \otimes_A A_P = \Omega_{R/A} \otimes_R A_P \cong \Omega_{R_P/A_P} \otimes_{R_P} A_P$ by [CRT, Exercise 25.4]. Thus if $C_{1,P} = 0$, by Nakayama's lemma $\Omega_{R_P/A_P} = 0$; so, R_P is étale over A_P [CRT, §25]. Therefore $R_P = A_P \oplus S_P$ as $R_P \twoheadrightarrow A_P$ splits, and hence $C_{0,P} = C_0 \otimes_A A_P = S_P \otimes_{R_P,\phi} A_P = 0$. Thus $\mathrm{Supp}_A(C_0) \subset \mathrm{Supp}_A(C_1)$.

If $C_{0,P} = 0$, then $\mathrm{Spec}(A_P) \cap \mathrm{Spec}(S_P) = \emptyset$; therefore, $R_P = A_P \oplus S_P$, and hence $\Omega_{R_P/A_P} = \Omega_{S_P/A_P}$, and hence $C_{1,P} = 0$. Thus shows the reverse inclusion $\mathrm{Supp}_A(C_0) \supset \mathrm{Supp}_A(C_1)$, and we conclude $\mathrm{Supp}_A(C_0) = \mathrm{Supp}_A(C_1)$.

Since the sub set of minimal primes of $\mathrm{Ann}_A(M)$ is equal to the subset of minimal primes in $\mathrm{Supp}_A(M)$ (see [CRT, Theorem 6.5 (iii)]), the identity $\mathrm{Supp}_A(C_0) = \mathrm{Supp}_A(C_1)$ implies the identity of associated primes. □

3. Galois deformation theory for $\mathbb{G}_m$

We study the universal deformation ring in the case of characters (i.e., representation into GL_1) and computes congruence modules C_0 and C_1. As before, we fix an odd prime p.

3.1. **Deformation of a character.** Let $F/\mathbb{Q}$ be a number field with integer ring O. We fix a set $\mathcal{P}$ of properties of Galois characters. The property $\mathcal{P}$ is often unramified outside p, or in addition, deformed characters has prime-to-p conductor a factor of a fixed ideal $\mathfrak{c}$ prime to p. Fix a continuous character $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathbb{F}^\times$ with the property $\mathcal{P}$.

A character $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to A^\times$ for $A \in CL_W$ is called a $\mathcal{P}$-deformation of $\overline{\rho}$ if $(\rho \mod \mathfrak{m}_A) = \overline{\rho}$ and ρ satisfies $\mathcal{P}$.

A couple $(R, \boldsymbol{\rho})$ (universal couple) made of an object R of CL_W and a character $\boldsymbol{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to R^\times$ satisfying $\mathcal{P}$ is called a *universal couple* for $\overline{\rho}$ if for any $\mathcal{P}$-deformation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to A^\times$ of $\overline{\rho}$, we have a unique morphism $\phi_\rho : R \to A$ 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 $(R, \boldsymbol{\rho})$ is determined uniquely up to isomorphisms.

3.2. **Ray class groups of finite level.** Fix an O-ideal $\mathfrak{c}$. Recall

$$Cl_F(\mathfrak{c}) = \frac{\{\text{fractional } O\text{-ideals prime to } \mathfrak{c}\}}{\{(\alpha) | \alpha \equiv 1 \mod^\times \mathfrak{c}\infty\}},$$

Here $\alpha \equiv 1 \mod^\times \mathfrak{c}$ means that $\alpha = a/b$ for $a, b \in O$ is totally positive (i.e., $\sigma(\alpha) > 0$ for all real embedding $F \xrightarrow{\sigma} \mathbb{R}$) such that $(b) + \mathfrak{c} = O$ and $a \equiv b \mod \mathfrak{c}$ (or equivalently, for all primes $\mathfrak{l} | \mathfrak{c}$, $\alpha \in O_\mathfrak{l}^\times$ and $\alpha \equiv 1 \mod \mathfrak{l}^{v_\mathfrak{l}(\mathfrak{c}\infty)}$ if the $\mathfrak{l}$-primary factor of $\mathfrak{c}$ has exponent $v_\mathfrak{l}(\mathfrak{c})$ (if $\mathfrak{l} | \infty$, it just means α is positive at $\mathfrak{l}$).

Write $H_{\mathfrak{c}p^n}/F$ for the ray class field modulo $\mathfrak{c}p^n$. In other words, there exists a unique abelian extension $H_{\mathfrak{c}p^n}/F$ only ramified at $\mathfrak{c}p\infty$ exists such that we can identify $\mathrm{Gal}(H_{\mathfrak{c}p^n}/F)$ with the strict ray class group $Cl_F(\mathfrak{c}p^n)$ by sending a class of prime $\mathfrak{l}$ in $Cl_F(\mathfrak{c}p^n)$ to the Frobenius element $\mathrm{Frob}_\mathfrak{l} \in \mathrm{Gal}(H_{\mathfrak{c}p^n}/F)$. This isomorphism is called the Artin symbol.

3.3. **Ray class group of infinite level.** The group $Cl_F(\mathfrak{c}p^n)$ is finite as we have an exact sequence:

$$(O/\mathfrak{c}p^n)^\times \xrightarrow{\alpha\mapsto(\alpha)} Cl_F(\mathfrak{c}p^n) \to Cl_F^+ \to 1$$

for the strict class group Cl_F^+ (we write the usual class group without condition at ∞ as Cl_F). Note that $|Cl_F^+|/|Cl_F|$ is a factor of 2^e for the number e of real embeddings of F.

Sending a class $[\mathfrak{a}] \in Cl_F(\mathfrak{c}p^m)$ to the class $[\mathfrak{a}] \in Cl_F(\mathfrak{c}p^n)$ for $m > n$, we have a projective system $\{Cl_F(\mathfrak{c}p^n)\}_n$. Put $Cl_F(\mathfrak{c}p^\infty) = \varprojlim_n Cl_F(\mathfrak{c}p^n)$. Then for $H_{\mathfrak{c}p^\infty} = \bigcup_n H_{\mathfrak{c}p^n}$, $Cl_F(\mathfrak{c}p^\infty) \cong \mathrm{Gal}(H_{\mathfrak{c}p^\infty}/F)$ by $[\mathfrak{l}] \mapsto \mathrm{Frob}_\mathfrak{l}$ for primes $\mathfrak{l} \nmid \mathfrak{c}p$.

If $F = \mathbb{Q}$ and $\mathfrak{c} = (N)$ for $0 < N \in \mathbb{Z}$, we have $H_{\mathfrak{c}p^n}$ is the cyclotomic field $\mathbb{Q}[\mu_{Np^n}]$ for the group μ_{Np^n} of Np^n-th roots of unity; so, $Cl_\mathbb{Q}(\mathfrak{c}p^n) \cong (\mathbb{Z}/Np^n\mathbb{Z})^\times$ and $Cl_\mathbb{Q}(\mathfrak{c}p^\infty) \cong (\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p{}^\times$.

3.4. **Groups algebra is universal.** For a profinite abelian group $\mathcal{G}$ with the maximal p-profinite (p-Sylow) quotient $\mathcal{G}_p$, consider the group algebra $W[[\mathcal{G}_p]] = \varprojlim_n W[\mathcal{G}_n]$ writing $\mathcal{G}_p = \varprojlim_n \mathcal{G}_n$ with finite $\mathcal{G}_n$. For example, $\Lambda = W[[\Gamma]]$ ($\Gamma = 1 + p\mathbb{Z}_p = (1+p)^{\mathbb{Z}_p}$) (the Iwasawa algebra) is isomorphic to $W[[T]]$ by $1 + p \leftrightarrow t = 1 + T$. Suppose that $\mathcal{G}_p$ is finite. Fix a character $\overline{\chi} : \mathcal{G} \to \mathbb{F}^\times$. Since $\mathbb{F}^\times \hookrightarrow W^\times$, we may regard $\overline{\chi}$ as a character $\chi_0 : \mathcal{G} \to W^\times$ (Teichmüller lift of $\overline{\chi}$). Define $\boldsymbol{\kappa} : \mathcal{G} \to W[[\mathcal{G}_p]]^\times$ by $\boldsymbol{\kappa}(g) = \chi_0(g)g_p$ for the image g_p of g in $\mathcal{G}_p$. Note that $W[\mathcal{G}_p]$ is a local ring with residue field $\mathbb{F}$. For any continuous deformation $\chi : \mathcal{G} \to A^\times$ of $\overline{\chi}$, $\varphi : W[\mathcal{G}_p] \ni \sum_g a_g g \mapsto \sum_g a_g \chi\chi_0^{-1}(g) \in A$ gives a unique W-algebra homomorphism such that $\varphi \circ \boldsymbol{\kappa} = \chi$. If $\mathcal{G}_p$ is infinite and $A = \varprojlim_n A_n$ for finite A_n with $A_n = A/\mathfrak{m}_n$, $\chi_n := \chi\chi_0^{-1} \mod \mathfrak{m}_n : \mathcal{G} \to A_n^\times$ has to factor through $\mathcal{G}_{m(n)}$ by continuity, and we get $\varphi_n : W[\mathcal{G}_{m(n)}] \to A_n$ such that $\varphi_n \circ \boldsymbol{\kappa} = \rho_n$. Passing to the limit, we have $\varphi \circ \boldsymbol{\kappa} = \rho$ for $\varphi = \varprojlim_n \varphi_n : W[[\mathcal{G}_p]] \to A$.

3.5. **Universal deformation ring for a Galois character $\overline{\rho}$.** Let $C_F(\mathfrak{c}p^\infty)$ for the maximal p-profinite quotient of $Cl_F(\mathfrak{c}p^\infty)$. If $\overline{\rho}$ has prime-to-p conductor equal to $\mathfrak{c}$, we define a deformation ρ to satisfy $\mathcal{P}$ if ρ is unramified outside $\mathfrak{c}p$ and has prime-to-p conductor a factor of $\mathfrak{c}$ (i.e., ρ factors through $\mathrm{Gal}(H_{\mathfrak{c}p^\infty}/F)$).

For the Teichmüller lift ρ_0 of $\overline{\rho}$ and the inclusion $\kappa : C_F(\mathfrak{c}p^\infty) \hookrightarrow W[[C_F(\mathfrak{c}p^\infty)]]$, we define $\boldsymbol{\rho}(\sigma) := \rho_0(\sigma)\kappa(\sigma)$. Then the universality of the group algebra tells us

Theorem 3.1. *The couple $(W[[C_F(\mathfrak{c}p^\infty)]], \boldsymbol{\rho})$ is universal among all $\mathcal{P}$-deformations. If $\overline{\rho}$ is unramified everywhere, $(W[[C_F]], \boldsymbol{\rho})$ for $C_F := Cl_{F,p}$ is universal among everywhere unramified deformations.*

3.6. **Congruence modules for group algebras.** Let H be a finite p-abelian group. If $\mathfrak{m}$ is a maximal ideal of $W[H]$, then for the inclusion $\kappa : H \hookrightarrow W[H]^\times$ with $\kappa(\sigma) = \sigma$, $\kappa \mod \mathfrak{m}$ is trivial as the finite field $W[H]/\mathfrak{m}$ has no non-trivial p-power roots of unity; so, $\mathfrak{m}$ is generated by $\{\sigma - 1\}_{h\in H}$ and $\mathfrak{m}_W$. Thus $\mathfrak{m}$ is unique and $W[H]$ is a local ring.

We have a canonical algebra homomorphism: $W[H] \to W$ sending $\sigma \in H$ to 1. This homomorphism is called the *augmentation* homomorphism of the group algebra. Write this map $\pi : W[H] \to W$. Then $\mathfrak{b} = \mathrm{Ker}(\pi)$ is generated by $\sigma - 1$ for $\sigma \in H$. Thus

$$\mathfrak{b} = \sum_{\sigma\in H} W[H](\sigma - 1)W[H].$$

We compute the congruence module and the differential module $C_j(\pi, W)$ $(j = 0, 1)$.

Theorem 3.2. *We have*

$$C_0(\pi; W) \cong W/|H|W \quad \text{and} \quad C_1(\pi; W) = H \otimes_\mathbb{Z} W.$$

Proof. Let $K := \mathrm{Frac}(W)$. Then π gives rise to the algebra direct factor $K\varepsilon \subset K[H]$ for the idempotent $\varepsilon = \frac{1}{|H|}\sum_{\sigma\in H} \sigma$. Thus $\mathfrak{a} = K\varepsilon \cap W[H] = (\sum_{\sigma\in H} \sigma)$ and $\pi(W(H))/\mathfrak{a} = (\varepsilon)/\mathfrak{a} \cong W/|H|W$.

Consider the functor $\mathcal{F} : CL_W \to SETS$ given by

$$\mathcal{F}(A) = \mathrm{Hom}_{\mathrm{group}}(H, A^\times) = \mathrm{Hom}_{W\text{-alg}}(W[H], A).$$

Thus $R := W[H]$ and the character $\boldsymbol{\rho} : H \to W[H]$ (the inclusion: $H \hookrightarrow W[H]$) are universal among characters of H with values in $A \in CL_W$.

Then for any R-module X, consider $R[X] = R \oplus X$ with algebra structure given by $rx = 0$ and $xy = 0$ for all $r \in R$ and $x, y \in X$. Thus X is an ideal of $R[X]$ with $X^2 = 0$. Define $\Phi(X) = \{\rho \in \mathcal{F}(R[X]) | \rho \mod X = \boldsymbol{\rho}\}$. Write $\rho(\sigma) = \boldsymbol{\rho}(\sigma) \oplus u'_\rho(\sigma)$ for $u'_\rho : H \to X$.

Since

$$\boldsymbol{\rho}(\sigma\tau) \oplus u'_\rho(\sigma\tau) = \rho(\sigma\tau) = (\boldsymbol{\rho}(\sigma) \oplus u'_\rho(\sigma))(\boldsymbol{\rho}(\tau) \oplus u'_\rho(\tau)) = \boldsymbol{\rho}(\sigma\tau) \oplus (u'_\rho(\sigma)\boldsymbol{\rho}(\tau) + \boldsymbol{\rho}(\sigma)u'_\rho(\tau)),$$

we have $u'_\rho(\sigma\tau) = u'_\rho(\sigma)\boldsymbol{\rho}(\tau) + \boldsymbol{\rho}(\sigma)u'_\rho(\tau)$, and thus $u_\rho := \boldsymbol{\rho}^{-1}u'_\rho : H \to X$ is a homomorphism from H into X. This shows

$$\mathrm{Hom}(H, X) = \Phi(X).$$

Any W-algebra homomorphism $\xi : R \to R[X]$ with $\xi \mod X = \mathrm{id}_R$ can be aritten as $\xi = \mathrm{id}_R \oplus d_\xi$ with $d_\xi : R \to X$. Since $(r \oplus x)(r' \oplus x') = rr' \oplus rx' + r'x$ for $r, r' \in R$ and $x.x' \in X$, we have $d_\xi(rr') = rd_\xi(r') + r'd_\xi(r)$; so, $d_\xi \in Der_W(R, X)$. By universality of $(R, \boldsymbol{\rho})$, we have

$$\Phi(X) \cong \{\xi \in \mathrm{Hom}_{W\text{-alg}}(R, R[X]) | \xi \bmod X = \mathrm{id}\} = Der_W(R, X) = \mathrm{Hom}_R(\Omega_{R/W}, X).$$

Thus taking $X = K/W$, we have

$$\mathrm{Hom}_W(H \otimes_{\mathbb{Z}} W, K/W) = \mathrm{Hom}(H, K/W) = \mathrm{Hom}_R(\Omega_{R/W}, K/W) = \mathrm{Hom}_W(\Omega_{R/W} \otimes_{R,\pi} W, K/W).$$

By taking Pontryagin dual back, we have

$$H \cong \Omega_{R/W} \otimes_{R,\pi} W = C_1(\pi; W)$$

as desired. □

3.7. **Class group and Selmer group.** Let $\mathrm{Ind}_F^{\mathbb{Q}}\,\mathrm{id} = \mathrm{id} \oplus \chi$ and $H = C_F$. Then for Ω_F given basically by the regulator and some power of $(2\pi i)$,

$$|L(1, \chi)/\Omega_F|_p = \big||C_F|\big|_p.$$

We can identify $C_F^\vee = \mathrm{Hom}(C_F, \mathbb{Q}_p/\mathbb{Z}_p)$ with the Selmer group of χ given by

$$\mathrm{Sel}_{\mathbb{Q}}(\chi) := \mathrm{Ker}(H^1(\mathbb{Q}, V(\chi)^*) \to \prod_l H^1(I_l, V(\chi)^*))$$

for the inertia group $I_l \subset \mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$.

3.8. **Class number formula.**

Theorem 3.3 (Class number formula)**.** *Assume that $F/\mathbb{Q}$ is a Galois extension and $p \nmid [F : \mathbb{Q}]$. For the augmentation homomorphism $\pi : W[C_F] \to W$, we have, for $r(W) = \mathrm{rank}_{\mathbb{Z}_p} W$,*

$$\left|\frac{L(1, \chi)}{\Omega_F}\right|_p^{r(W)} = |C_1(\pi; W)|^{-1} = |C_0(\pi; W)|^{-1} = \big||\mathrm{Sel}_{\mathbb{Q}}(\chi)|\big|_p^{r(W)}$$

and $C_1(\pi; W) = C_F \otimes W$ and $C_0(\pi; W) = W/|C_F|W$.

4. Number of generators of adjoint Selmger griougs

The dimension d of the tangent space of a local ring R over $\mathbb{F}$ gives the number of generators of the ring R. We describe this fact. Using this fact, we prove that $\Omega_{R/W}$ is generated by d elements as R-modules. We fix a generator ϖ of the maximal ideal $\mathfrak{m}_W$ of W.

Hereafter, we fix a finite set S of rational primes (including infinite places), and we let $\mathfrak{G}_{\mathbb{Q}}$ denote the Galois group over $\mathbb{Q}$ of the maximal extension unramified outside S.

4.1. **Tangent spaces of local rings.** To study noetherian property of deformation ring, here is a useful lemma for an object R in CL_W:

Lemma 4.1. *If $t^*_{R/W} = \mathfrak{m}_R/(\mathfrak{m}_R^2 + \mathfrak{m}_W)$ is a finite dimensional vector space over $\mathbb{F}$, then $R \in CL_W$ is noetherian.*

The space $t^*_{R/W}$ is called the co-tangent space of R at $\mathfrak{m}_R = (\varpi) \in \mathrm{Spec}(R)$ over $\mathrm{Spec}(W)$. Define t^*_R by $\mathfrak{m}_R/\mathfrak{m}_R^2$, which is called the (absolute) co-tangent space of R at $\mathfrak{m}_R$.

Proof. Since we have an exact sequence:

$$\mathbb{F} \xrightarrow[a \mapsto a\varpi]{\sim} \mathfrak{m}_W/\mathfrak{m}_W^2 \longrightarrow t^*_R \longrightarrow t^*_{R/W} \longrightarrow 0,$$

we conclude that t^*_R is of finite dimension over $\mathbb{F}$ if $t^*_{R/W}$ is of finite dimensional.

First suppose that $\mathfrak{m}_R^N = 0$ for sufficiently large N. Let $\overline{x}_1, \ldots, \overline{x}_m$ be an $\mathbb{F}$–basis of t^*_R. Choose $x_j \in R$ so that $x_j \mod \mathfrak{m}_R^2 = \overline{x}_j$. and consider the ideal $\mathfrak{a}$ generated by x_j. We have $\mathfrak{a} = \sum_j Rx_j \hookrightarrow \mathfrak{m}_R$ (the inclusion).

After tensoring $R/\mathfrak{m}_R$, we have the surjectivity of the induced linear map: $\mathfrak{a}/\mathfrak{m}_R\mathfrak{a} \cong \mathfrak{a} \otimes_R R/\mathfrak{m}_R \to \mathfrak{m} \otimes_R R/\mathfrak{m}_R \cong \mathfrak{m}/\mathfrak{m}_R^2$ because $\{\overline{x}_1, \dots, \overline{x}_m\}$ is an $\mathbb{F}$–basis of t_R^*. This shows that $\mathfrak{m}_R = \mathfrak{a} = \sum_j Rx_j$ (NAK: Nakayama's lemma applied to the cokernel of $R^m \ni (a_1, \dots, a_m) \mapsto \sum_j a_j x_j \in \mathfrak{m}_R$). Therefore $\mathfrak{m}_R^k/\mathfrak{m}_R^{k+1}$ is generated by the monomials in x_j of degree k as an $\mathbb{F}$–vector space.

In particular, $\mathfrak{m}_R^{N-1}$ is generated by the monomials in $(x_0 := \varpi, x_1, \dots x_m)$ of degree $N-1$.

Inductive step: Define $\pi : B = W[[X_1, \dots, X_m]] \to R$ 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 $\mathfrak{m} = \mathfrak{m}_B = (\varpi, X_1, \cdots, X_m)$ be the maximal ideal of B. By definition,

$$\pi(\mathfrak{m}^{N-1}) = \mathfrak{m}_R^{N-1}.$$

Suppose now that $\pi(\mathfrak{m}^{N-j}) = \mathfrak{m}_R^{N-j}$, and try to prove the surjectivity of $\pi(\mathfrak{m}^{N-j-1}) = \mathfrak{m}_R^{N-j-1}$.

Since $\mathfrak{m}_R^{N-j-1}/\mathfrak{m}_R^{N-j}$ is generated by monomials of degree $N-j-1$ in x_j, for each $x \in \mathfrak{m}_R^{N-j-1}$, 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 $x - \pi(P) \in \mathfrak{m}_R^{N-j} = \pi(\mathfrak{m}^{N-j})$. This shows $\pi(\mathfrak{m}^{N-j-1}) = \mathfrak{m}_R^{N-j-1}$. Thus by induction on j, we get the surjectivity of π.

General case: Write $R = \varprojlim_i R_i$ for Artinian rings R_i. The projection maps are onto: $t_{R_{i+1}}^* \twoheadrightarrow t_{R_i}^*$. Since t_R^* is of finite dimensional, for sufficiently large i,

$$t_{R_{i+1}}^* \cong t_{R_i}^*.$$

Thus choosing x_j as above in R, we have its image $x_j^{(i)}$ in R_i.

Use $x_j^{(i)}$ to construct $\pi_i : W[[X_1, \dots, X_m]] \to R_i$ in place of x_j. Then π_i is surjective as already shown, and

$$\pi = \varprojlim_i \pi_i : W[[X_1, \dots, X_m]] \to R$$

remains surjective, because projective limit of continuous surjections, if all sets involved are compact sets, remain surjective; so, R is noetherian as profinite sets are compact. □

4.2. **Tangent space as adjoint cohomology group.** Let $R = R_{\overline{\rho}}$ be the universal ring for a mod p-Galois absolutely irreducible representation $\overline{\rho} : \mathfrak{G}_{\mathbb{Q}} \to GL_n(\mathbb{F})$.

We identify $t_{R/W}^*$ with a certain cohomology group $H^1(\mathfrak{G}_{\mathbb{Q}}, ad(\overline{\rho}))$ and in this way, we prove finite dimensionality: $\dim_{\mathbb{F}} t_{R/W}^* < \infty$ (and hence $R_{\overline{\rho}}$ is noetherian).

Let $M_n(\mathbb{F})$ be the space of $n \times n$ matrices with coefficients in $\mathbb{F}$. We let $\mathfrak{G}_{\mathbb{Q}}$ acts on $M_n(\mathbb{F})$ by $gv = \overline{\rho}(g)v\overline{\rho}(g)^{-1}$. This action is called the **adjoint** action of $\mathfrak{G}_{\mathbb{Q}}$, and this $\mathfrak{G}_{\mathbb{Q}}$–module will be written as $ad(\overline{\rho})$.

Write Z for the center of $M_n(\mathbb{F})$ and define $\mathfrak{sl}_n(\mathbb{F}) = \{X \in M_n(\mathbb{F}) | \mathrm{Tr}(X) = 0\}$. Since $\mathrm{Tr}(aXa^{-1}) = \mathrm{Tr}(X)$, $\mathfrak{sl}_n(\mathbb{F})$ is stable under the adjoint action. This Galois module will be written as $Ad(\overline{\rho})$.

If $p \nmid n$, $X \mapsto \frac{1}{n}\mathrm{Tr}(X) \oplus (X - \frac{1}{n}\mathrm{Tr}(X))$ gives rise to $M_n(\mathbb{F}) = Z \oplus \mathfrak{sl}_n(\mathbb{F})$ stable under the adjoint action. So we have $ad(\overline{\rho}) = \mathbf{1} \oplus Ad(\overline{\rho})$ if $p \nmid n$, where $\mathbf{1}$ is the trivial representation.

Lemma 4.2. *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 $\mathfrak{m}$. In the following proof of the lemma, we write $G = \mathfrak{G}_{\mathbb{Q}}$ and $R = R_{\overline{\rho}}$.

Proof. Step. 1, dual number. Let $A = \mathbb{F}[\varepsilon] = \mathbb{F}[X]/(X^2)$ with $X \leftrightarrow \varepsilon$. Then $\varepsilon^2 = 0$. We claim:

$$\mathrm{Hom}_{W\text{-alg}}(R, A) \cong t_{R/W}.$$

Construction of the map.

Start with a W-algebra homomorphism $\phi : R \to A$. Write

$$\phi(r) = \phi_0(r) + \phi_\varepsilon(r)\varepsilon \quad \text{with } \phi_0(r), \phi_\varepsilon(r) \in \mathbb{F}.$$

Then the map is $\phi \mapsto \ell_\phi = \phi_\varepsilon|_{\mathfrak{m}_R}$.

Step. 2, Well defined-ness of ℓ_ϕ. From $\phi(ab) = \phi(a)\phi(b)$, we get

$$\phi_0(ab) = \phi_0(a)\phi_0(b) \text{ and } \phi_\varepsilon(ab) = \phi_0(a)\phi_\varepsilon(b) + \phi_0(b)\phi_\varepsilon(a).$$

Thus $\phi_\varepsilon \in Der_W(R,\mathbb{F}) \cong \mathrm{Hom}_{\mathbb{F}}(\Omega_{R/W} \otimes_R \mathbb{F}, \mathbb{F})$. Since for any derivation $\delta \in Der_W(R,\mathbb{F})$, $\phi' = \phi_0 + \delta\varepsilon \in \mathrm{Hom}_{W\text{-alg}}(R,A)$, we find

$$\mathrm{Hom}_R(\Omega_{R/W} \otimes_R \mathbb{F}, \mathbb{F}) \cong Der_W(R,A) \cong \mathrm{Hom}_{W\text{-alg}}(R,A).$$

and $\mathrm{Ker}(\phi_0) = \mathfrak{m}_R$ because R is local. Since ϕ is W–linear, $\phi_0(a) = \overline{a} = a \mod \mathfrak{m}_R$.

Thus ϕ kills $\mathfrak{m}_R^2$ and takes $\mathfrak{m}_R$ W–linearly into $\mathfrak{m}_A = \mathbb{F}\varepsilon$; so, $\ell_\phi : t_R^* \to \mathbb{F}$. For $r \in W$, $\overline{r} = r\phi(1) = \phi(r) = \overline{r} + \phi_\varepsilon(r)\varepsilon$, and hence ϕ_ε kills W; so, $\ell_\phi \in t_{R/W}$.

Step. 3, injectivity of $\phi \mapsto \ell_\phi$. 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 ℓ_ϕ of ϕ_ε to $\mathfrak{m}_R$, which factors through $t_{R/W}^*$. Thus $\phi \mapsto \ell_\phi$ induces an injective linear map $\ell : \mathrm{Hom}_{W-alg}(R,A) \hookrightarrow \mathrm{Hom}_{\mathbb{F}}(t_{R/W}^*, \mathbb{F})$.

Note $R/(\mathfrak{m}_R^2 + \mathfrak{m}_W) = \mathbb{F} \oplus t_{R/W}^* = \mathbb{F}[t_{R/W}^*]$ with the projection $\pi : R \twoheadrightarrow t_{R/W}^*$ to the direct summand $t_{R/W}^*$. Indeed, writing $\overline{r} = (r \mod \mathfrak{m}_R)$, for the inclusion $\iota : \mathbb{F} = W/\mathfrak{m}_W \hookrightarrow R/(\mathfrak{m}_R^2 + m_W)$, $\pi(r) = r - \iota(\overline{r})$.

Step. 4, surjectivity of $\phi \mapsto \ell_\phi$. For any $\ell \in \mathrm{Hom}_{\mathbb{F}}(t_{R/W}^*, \mathbb{F})$, we extend ℓ to R by putting $\ell(r) = \ell(\pi(r))$. Then we define $\phi : R \to A$ by $\phi(r) = \overline{r} + \ell(\pi(r))\varepsilon$. Since $\varepsilon^2 = 0$ and $\pi(r)\pi(s) = 0$ in $\mathbb{F}[t_{R/W}^*]$, we have

$$rs = (\overline{r} + \pi(r))(\overline{s} + \pi(s)) = \overline{rs} + \overline{s}\pi(r) + \overline{r}\pi(s) \xrightarrow{\phi} \overline{rs} + \overline{s}\ell(\pi(r))\varepsilon + \overline{r}\ell(\pi(s))\varepsilon = \phi(r)\phi(s)$$

is an W–algebra homomorphism. In particular, $\ell(\phi) = \ell$, and hence ℓ is surjective.

By $\mathrm{Hom}_R(\Omega_{R/W} \otimes_R \mathbb{F}, \mathbb{F}) \cong \mathrm{Hom}_{W\text{-alg}}(R,A)$, we have

$$\mathrm{Hom}_R(\Omega_{R/W} \otimes_R \mathbb{F}, \mathbb{F}) \cong \mathrm{Hom}_{\mathbb{F}}(t_{R/W}^*, \mathbb{F});$$

so, if $t_{R/W}^*$ is finite dimensional, we get

$$\boxed{\Omega_{R/W} \otimes_R \mathbb{F} \cong t_{R/W}^*.} \tag{4.1}$$

Step. 5, use of universality. By the universality, we have

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

Write $\rho(g) = \overline{\rho}(g) + u'_\phi(g)\varepsilon$ for ρ corresponding to $\phi : R \to A$. From the mutiplicativity, we have

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

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

$$u'_\phi(gh) = \overline{\rho}(g)u'_\phi(h) + u'_\phi(g)\overline{\rho}(h). \tag{4.2}$$

Step. 6, Getting 1-cocycle. Define a map $u_\rho = u_\phi : G \to ad(\overline{\rho})$ by

$$u_\phi(g) = u'_\phi(g)\overline{\rho}(g)^{-1}.$$

Then by a simple computation, we have

$$gu_\phi(h) = \overline{\rho}(g)u_\phi(h)\overline{\rho}(g)^{-1}$$

from the definition of $ad(\overline{\rho})$. Then from the above formula (4.2), we conclude that

$$\boxed{u_\phi(gh) = gu_\phi(h) + u_\phi(g).}$$

Thus $u_\phi : G \to ad(\overline{\rho})$ is a 1–cocycle. Thus we get an $\mathbb{F}$-linear map

$$t_{R/W} \cong \mathrm{Hom}_{W\text{-alg}}(R,A) \to H^1(\mathfrak{G}_{\mathbb{Q}}, ad(\overline{\rho}))$$

by $\ell_\phi \mapsto [u_\phi]$

Step. 7, End of proof. By computation, for $x \in ad(\overline{\rho})$

$$\rho \sim \rho' \Leftrightarrow \overline{\rho}(g) + u'_\rho(g)\varepsilon = (1 + x\varepsilon)(\overline{\rho}(g) + u'_{\rho'}(g)\varepsilon)(1 - x\varepsilon)$$
$$\Leftrightarrow u'_\rho(g) = x\overline{\rho}(g) - \overline{\rho}(g)x + u'_{\rho'}(g) \Leftrightarrow u_\rho(g) = (1-g)x + u_{\rho'}(g).$$

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

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

In this way, we get a bijection between $\mathrm{Hom}_{\mathbb{F}}(t_{R/W}^*, \mathbb{F})$ and $H^1(G, ad(\overline{\rho}))$. □

4.3. **p-Frattini condition.** For each open subgroup H of a profinite group G, we write H_p for the maximal p–profinite quotient. Define p-Frattini quotient $\Phi(H_p)$ of H by $\Phi(H_p) = H_p/\overline{(H_p)^p(H_p, H_p)}$ for the the commutator subgroup (H_p, H_p) of H_p. We consider the following condition:

(Φ) *For any open subgroup H of G, $\Phi(H_p)$ is a finite group.*

Proposition 4.3 (Mazur)**.** *By class field theory, $\mathfrak{G}_{\mathbb{Q}}$ satisfies (Φ) , and $R_{\overline{\rho}}$ is a noetherian ring. In particular, $t^*_{R/W}$ is finite dimensional over $\mathbb{F}$ and is isomorphic to $\Omega_{R/W} \otimes_R \mathbb{F}$* (see (4.1)).

By this fact, hereafter we always assume that the deformation functor is defined over $CNL_{/W}$.

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

$$\dim_{\mathbb{F}} H^1(G, ad(\overline{\rho})) < \infty.$$

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 abelian extension M/F unramified outside p. By class field theory, $[M : F]$ is finite. □

Corollary 4.4. *$\Omega_{R/W}$ is an R-module of finite type, and its minimal number of generators over R is equal to*

$$\dim_{\mathbb{F}} \Omega_{R/W} \otimes_R \mathbb{F} = \dim_{\mathbb{F}} t_{R/W}.$$

Proof. For any R-module M, Nakayama's lemma tells us $M \otimes_R \mathbb{F} = 0 \Rightarrow M = 0$. Choose a basis $B = \{\overline{b}\}$ of $M/\mathfrak{m}_R M = M \otimes_R \mathbb{F}$ and suppose B is finite. Lift $\overline{b}$ to $b \in M$, and consider the R-linear map $\pi : \bigoplus_{g \in B} R \ni (a_{\overline{b}})_{\overline{b} \in B} \mapsto \sum_{\overline{b}} a_{\overline{b}} b \in M$. Tensoring $\mathbb{F}$ over R, we find $\mathrm{Coker}(\pi) \otimes_R \mathbb{F} = 0$; so, $\mathrm{Coker}(\pi) = 0$. This implies that $\{b | \overline{b} \in B\}$ is the minimal generators of M over R. Apply this to $M = \Omega_{R/W}$, we get the result by Proposition 4.3. □

5. Adjoint Selmer groups and differentials

We define $\mathrm{Sel}(Ad(\rho))$ for ordinary deformations ρ of an **absolutely irreducible** 2-dimensional Galois representation $\overline{\rho}$ and show that $\mathrm{Sel}(Ad(\overline{\rho})) = t_{R/W}$ and $\mathrm{Sel}(Ad(\boldsymbol{\rho})) \cong \Omega_{R/W}$ for the universal ordinary Galois representation $\boldsymbol{\rho}$ deforming $\overline{\rho}$.

We write I_p for the inertia group of $D_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

5.1. **p-Ordinarity condition.** Let $\rho : \mathfrak{G}_{\mathbb{Q}} \to \mathrm{GL}_2(A)$ $(A \in CL_{/W})$ be a deformation of $\overline{\rho} : \mathfrak{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ acting on $V(\rho)$. We say ρ is p-ordinary if

(ord_p) $\rho|_{D_p} \cong \left(\begin{smallmatrix} \epsilon & * \\ 0 & \delta \end{smallmatrix}\right)$ *for two characters $\epsilon, \delta : D_p \to A^\times$* **distinct** *modulo $\mathfrak{m}_A$ with δ unramified.*

So, $\overline{\rho} = \rho|_{D_p} \cong \left(\begin{smallmatrix} \overline{\epsilon} & * \\ 0 & \overline{\delta} \end{smallmatrix}\right)$ with $\delta \mod \mathfrak{m}_A = \overline{\delta}$ which is a requirement. We also consider a similar condition for $l \in S$ $(l \neq p)$:

(ord_l) *We have a non-trivial character $\epsilon_l : I_l \to W^\times$ of order prime to p such that $\rho|_{I_l} \cong \left(\begin{smallmatrix} \iota_A \circ \epsilon_l & 0 \\ 0 & \mathbf{1} \end{smallmatrix}\right)$, where $\iota_A : W \to A$ is the W-algebra structure morphism.*

We always impose these two conditions (ord_p) and (ord_l) for $l \in S$. In most cases, we fix a character $\chi : \mathfrak{G}_{\mathbb{Q}} \to W^\times$, we consider

(det) $$\det \rho = \iota_A \circ \chi.$$

5.2. **Ordinary deformation functor.** We consider the following functor for a fixed absolutely irreducible representation $\overline{\rho} : \mathfrak{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ satisfying (ord_p) and (ord_l). Then we consider $\mathcal{D}, \mathcal{D}_\chi : CL_{/W} \to SETS$ given by

$$\mathcal{D}(A) = \{\rho : \mathfrak{G}_{\mathbb{Q}} \to \mathrm{GL}_2(A) | \rho \mod \mathfrak{m}_A \cong \overline{\rho}, \rho \text{ satisfies } (\mathrm{ord}_p) \text{ and } (\mathrm{ord}_l)\}/\cong$$

and

$$\mathcal{D}_\chi(A) = \{\rho \in \mathcal{D}(A) | \det \rho = \iota_A \circ \chi\}.$$

Then

Theorem 5.1 (B. Mazur)**.** *There exists a universal couple $(R^{ord}, \boldsymbol{\rho} = \boldsymbol{\rho}^{ord})$ and $(R_\chi, \boldsymbol{\rho}_\chi)$ representing $\mathcal{D}$ and $\mathcal{D}_\chi$, respectively, so that $\mathcal{D}(A) \cong \mathrm{Hom}_{W\text{-}alg}(R^{ord}, A)$ by $\rho \mapsto \varphi$ with $\varphi \circ \boldsymbol{\rho}^{ord} = \rho$ (resp. $\mathcal{D}_\chi(A) \cong \mathrm{Hom}_{W\text{-}alg}(R_\chi, A)$ by $\rho \mapsto \varphi$ with $\varphi \circ \boldsymbol{\rho}_\chi = \rho$).*

For a proof, see [MFG, §2.3.2, §3.2.4].

5.3. **Fiber products.** Let $\mathcal{F} : CL_{/W} \to SETS$ be a covariant functor with $|\mathcal{F}(\mathbb{F})| = 1$. Let $\mathcal{C} = SETS$ or $CL_{/W}$. For morphisms $\phi' : S' \to S$ and $\phi'' : S'' \to S$ in $\mathcal{C}$,

$$S' \times_S S'' = \{(a', a'') \in S' \times S'' | \phi'(a') = \phi''(a'')\}$$

gives the fiber product of S' and S'' over S in $\mathcal{C}$. We assume that

$$|\mathcal{F}(\mathbb{F})| = 1 \text{ and } \mathcal{F}(\mathbb{F}[\varepsilon] \times_{\mathbb{F}} \mathbb{F}[\varepsilon]) = \mathcal{F}(\mathbb{F}[\varepsilon]) \times_{\mathcal{F}(\mathbb{F})} \mathcal{F}(\mathbb{F}[\varepsilon])$$

by two projections.

It is easy to see $\mathcal{F} = \mathcal{D}$ and $\mathcal{D}_\chi$ satisfies this condition. Indeed, noting that $\mathbb{F}[\varepsilon] \times_{\mathbb{F}} \mathbb{F}[\varepsilon] \cong \mathbb{F}[\varepsilon'] \times_{\mathbb{F}} \mathbb{F}[\varepsilon''] \cong \mathbb{F}[\varepsilon', \varepsilon'']$, if $\rho' \in \mathcal{F}(\mathbb{F}[\varepsilon'])$ and $\rho'' \in \mathcal{F}(\mathbb{F}[\varepsilon''])$, we have $\rho' \times \rho$ has values in $\mathrm{GL}_2(\mathbb{F}[\varepsilon', \varepsilon''])$ is an element in $\mathcal{F}(\mathbb{F}[\varepsilon'] \times_{\mathbb{F}} \mathbb{F}[\varepsilon''])$.

5.4. **Slight generalization.** For any $A \in CL_{/W}$ and an A-module X, suppose $|\mathcal{F}(A)| = 1$ and $\mathcal{F}(A[X] \times_A A[X]) = \mathcal{F}(A[X]) \times_{\mathcal{F}(A)} \mathcal{F}(A[X])$. Then $A[X] \times_A A[X] = A[X \oplus X]$. The addition on X and A-linear map $\alpha : X \to X$ induces in the same way $CL_{/W}$-morphisms $+_* : A[X \oplus X] \to A[X]$ by $a + (x \oplus y) \mapsto a + x + y$ and $\alpha_* : A[X] \to A[X]$ by $a + x \mapsto a + \alpha(x)$. Thus we have by functoriality. the "addition"

$$+ : \mathcal{F}(A[X]) \times_{\mathcal{F}(A)} \mathcal{F}(A[X]) = \mathcal{F}(A[X \oplus X]) \xrightarrow{\mathcal{F}(+_*)} \mathcal{F}(A[X])$$

and α-action

$$\alpha : \mathcal{F}(A[X]) \xrightarrow{\mathcal{F}(\alpha_*)} \mathcal{F}(A[X]).$$

With $\mathbf{0} = \mathrm{Im}(\mathcal{F}(A) \to \mathcal{F}(A[X])$ for the inclusion $A \hookrightarrow A[X]$, this makes $\mathcal{F}(A[X])$ as an A-module.

5.5. **Tangent space of deformation functors.** Identify $\mathbb{F}[\varepsilon] \times_{\mathbb{F}} \mathbb{F}[\varepsilon]$ with $\mathbb{F}[\varepsilon', \varepsilon'']$ ($\varepsilon'\varepsilon'' = 0$ and $\dim_{\mathbb{F}} \mathbb{F}[\varepsilon] \times_{\mathbb{F}} \mathbb{F}[\varepsilon] = 3$ but $\dim_{\mathbb{F}} \mathbb{F}[\varepsilon] \otimes_{\mathbb{F}} \mathbb{F}[\varepsilon] = 4$). It is easy to see that $a + b\varepsilon' + c\varepsilon'' \mapsto a + (a + c)\varepsilon$ gives an onto $CL_{/W}$-morphism $a : \mathbb{F}[\varepsilon] \times_{\mathbb{F}} \mathbb{F}[\varepsilon] \twoheadrightarrow \mathbb{F}[\varepsilon]$ which induces

$$+ : \mathcal{F}(\mathbb{F}[\varepsilon]) \times \mathcal{F}(\mathbb{F}[\varepsilon]) = \mathcal{F}(\mathbb{F}[\varepsilon] \times_{\mathbb{F}} \mathbb{F}[\varepsilon]) \xrightarrow{\mathcal{F}(a)} \mathcal{F}(\mathbb{F}[\varepsilon]).$$

Plainly this is associative and commutative, and for the inclusion $0 : \mathbb{F} \hookrightarrow \mathbb{F}[\varepsilon]$, we have $\mathbf{0} := \mathrm{Im}(\mathcal{F}(0)(\mathcal{F}(\mathbb{F}))) \in \mathcal{F}(\mathbb{F}[\varepsilon])$ gives the identity. Thus $\mathcal{F}(\mathbb{F}[\varepsilon])$ is an abelian group.

Similarly, for $\alpha \in \mathbb{F}$, $a + b\varepsilon \mapsto a + \alpha b\varepsilon$ is an automorphism of $\mathbb{F}[\varepsilon]$ in $CL_{/W}$. This induces a multiplication on $\mathcal{F}(\mathbb{F}[\varepsilon])$ by scalar in $\mathbb{F}$. We see that $\mathcal{F}(\mathbb{F}[\varepsilon])$ is an $\mathbb{F}$-vector space, and $\mathcal{F}(\mathbb{F}[\varepsilon])$ is called the **tangent space** of the functor $\mathcal{F}$.

5.6. **Tangent space of rings and deformation functor.**

Lemma 5.2. *Let $\mathcal{F} = \mathcal{D}$ or $\mathcal{D}_\chi$ and $R = R^{ord}$ or R_χ accordingly. Then $t_{R/W} \cong \mathcal{F}(\mathbb{F}[\varepsilon])$ as $\mathbb{F}$-vector spaces.*

Proof. Write $\mathcal{D}^\emptyset : CL_{/W} \to SETS$ for the deformation functor defined by $\mathcal{D}^\emptyset(A) = \{\rho : \mathfrak{G}_{\mathbb{Q}} \to \mathrm{GL}_2(A) | (\rho \bmod \mathfrak{m}_A) = \overline{\rho}\}/\sim$ without any extra properties. Let $R_{\overline{\rho}}$ be the universal ring for $\mathcal{D}^\emptyset$. We have got a canonical bijection in Lemma 5.2:

$$\mathcal{D}^\emptyset(\mathcal{F}[\varepsilon]) \xrightarrow[i_1]{\text{1-1 onto}} H^1(\mathfrak{G}_{\mathbb{Q}}, ad(\overline{\rho})) \xrightarrow[i]{\sim} t_{R_{\overline{\rho}}/W}$$

with a vector space isomorphism i. We have constructed a cocycle u_ρ from $\rho \in \mathcal{F}(\mathbb{F}[\varepsilon])$ writing $\rho = \overline{\rho} + u_\rho \overline{\rho} \varepsilon$. Regarding $(\rho, \rho') \in \mathcal{F}(\mathbb{F}[\varepsilon]) \times \mathcal{F}(\mathbb{F}[\varepsilon]) = \mathcal{F}(\mathbb{F}[\varepsilon] \times_{\mathbb{F}} \mathbb{F}[\varepsilon])$, we see that $+(\rho, \rho') = \overline{\rho} + (u_\rho \overline{\rho} + u_{\rho'} \overline{\rho})\varepsilon \in \mathcal{F}(\mathbb{F}[\varepsilon])$; so, i_1 is a homomorphism. Similarly, one can check that it is $\mathbb{F}$-linear. □

5.7. **Tangent space as cohomology group with local condition.** We identify $\mathcal{F}(\mathbb{F}[\varepsilon])$ with a $\mathbb{F}$-vector subspace of $H^1(\mathfrak{G}_{\mathbb{Q}}, ad(\overline{\rho}))$. We want to explicitly determine $\mathcal{F}(\mathbb{F}[\varepsilon])$. Since corresponding cohomology class corresponds to strict conjugacy class, we may choose by (ord_p) a basis (dependent on $l \in S \cup \{p\}$) of $V(\rho)$ for $\rho \in \mathcal{F}(\mathbb{F}[\varepsilon])$ so that $\rho|_{D_p}$ is upper triangular with quotient character δ congruent to $\overline{\delta}$ modulo $\mathfrak{m}_A$. Similarly by (ord_l), we choose the basis so that $\rho|_{I_l} = \epsilon_l \oplus \mathbf{1}$ in this order.

Theorem 5.3. *A 1-cocycle u gives rise to a class in $\mathcal{D}_\chi(\mathbb{F}[\varepsilon])$ if and only if $u(I_l) = 0$ for all prime $l \in S$ not equal to p, $u|_{D_p}$ is upper triangular, $u|_{I_p}$ is upper nilpotent and $\mathrm{Tr}(u) = 0$ over $\mathfrak{G}_{\mathbb{Q}}$, where $\overline{v} = v \mod (\epsilon)$.*

Note that the description of cocycles u is independent of χ; so, even if one changes χ, the tangent space $t_{R_\chi/W}$ is independent as a cohomology subgroup as long as $\mathbb{F}$ does not change.

Proof. By (det), $1 = \det(\rho\overline{\rho}^{-1}) = 1 + u_\rho\varepsilon = 1 + \mathrm{Tr}(u_\rho)\varepsilon$; so, (det) $\Leftrightarrow$ $\mathrm{Tr}(u) = 0$ over $\mathfrak{G}_{\mathbb{Q}}$. Thus we $t_{R_\chi/W} \subset H^1(\mathfrak{G}_{\mathbb{Q}}, Ad(\overline{\rho}))$.

Choose a generator $w \in V(\epsilon)$ over $\mathbb{F}[\varepsilon]$. Then (w, v) is a basis of $V(\rho)$ over $\mathbb{F}[\varepsilon]$. Let $(\overline{w}, \overline{v}) = (w, v)$ mod ε and identify $V(ad(\overline{\rho}))$ with $M_2(\mathbb{F})$ with this basis. Then defining $\overline{\rho}$ by $(\sigma\overline{w}, \sigma\overline{v}) = (\overline{w}, \overline{v})\overline{\rho}(\sigma)$, for $\sigma \in D_p$, we have $\overline{\rho}(\sigma) = \left(\begin{smallmatrix} \overline{\epsilon}(\sigma) & * \\ 0 & \overline{\delta}(\sigma) \end{smallmatrix}\right)$ (upper triangular). If $\sigma \in I_p$, $\rho\overline{\rho}^{-1} = 1 + u_\rho$ with lower right corner of u_ρ has to vanish as $\delta = 1$ on I_p, we have $u_\rho(\sigma) \in \{\left(\begin{smallmatrix} 0 & * \\ 0 & 0 \end{smallmatrix}\right)\}$.

Since ramification at $l \neq p$ is concentrated to $\overline{\rho}$ as $\rho(I_l)$ has order prime to p, $(\mathrm{ord}_l) \Leftrightarrow u_\rho(I_l) = 0$. (ord_p) is equivalent to u_ρ is of the form $\left(\begin{smallmatrix} * & * \\ 0 & 0 \end{smallmatrix}\right)$ but by $\mathrm{Tr}(u_\rho) = 0$, it has to be upper nilpotent. □

5.8. **Mod p adjoint Selmer group.** For $\mathcal{F} = \mathcal{D}$ or $\mathcal{D}_\chi$, we denote the corresponding local deformation functor by

$$\mathcal{D}_l(A) = \{\rho : \mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l) \to \mathrm{GL}_2(A) | \rho \mod \mathfrak{m}_A = \overline{\rho} \text{ and } \rho \text{ satisfies } (\mathrm{ord}_l)\},$$

and $\mathcal{D}_{\chi,l}(A) = \{\rho \in \mathcal{D}_l(A) | \det(\rho) = \iota_A \circ \chi\}$. Thus by the proof of Theorem 5.3, we find

$$\mathcal{D}_\chi(A) = \{\rho : \mathfrak{G}_{\mathbb{Q}} \to \mathrm{GL}_2(A) \in \mathcal{D}^\emptyset(A) : \rho|_{D_l} \in \mathcal{D}_{\chi,l}(A)\}.$$

Therefore, we have

$$\mathrm{Sel}(Ad(\overline{\rho})) := t_{R_\chi/W} = \mathrm{Ker}(H^1(\mathfrak{G}_{\mathbb{Q}}, Ad(\overline{\rho})) \to \prod_{l \in S \cup \{p\}} \frac{H^1(\mathbb{Q}_l, Ad(\overline{\rho}))}{\mathcal{D}_{\chi,l}(\mathbb{F}[\varepsilon])}),$$

and

$$\mathrm{Sel}(ad(\overline{\rho})) := t_{R^{ord}/W} = \mathrm{Ker}(H^1(\mathfrak{G}_{\mathbb{Q}}, ad(\overline{\rho})) \to \prod_{l \in S \cup \{p\}} \frac{H^1(\mathbb{Q}_l, ad(\overline{\rho}))}{\mathcal{D}_l(\mathbb{F}[\varepsilon])}).$$

5.9. **R^{ord} is an algebra over the Iwasawa algebra.** The finite order character $\det(\overline{\rho})$ factors through $\mathrm{Gal}(\mathbb{Q}[\mu_{N_0}]/\mathbb{Q})$ for some positive integer N_0. Let N_0 be the minimal such integer (called conductor of $\det(\overline{\rho})$). Write $N_0 = Np^\nu$ for N prime to p; so, N is the prime to p-conductor of $\det(\overline{\rho})$. Note that $\det(\boldsymbol{\rho}^{ord})$ factors through $\mathrm{Gal}(\mathbb{Q}[\mu_{Np^\infty}]/\mathbb{Q}) \cong \mathbb{Z}_p{}^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$. Write $\Gamma \cong 1 + p\mathbb{Z}_p$ be the maximal p-profinite quotient of $\mathrm{Gal}(\mathbb{Q}[\mu_{Np^\infty}]/\mathbb{Q})$. Supposing $\chi|_{I_l}$ has values in $W^\times$, consider the deformation functor

$$D(A) = \{\varphi : \mathfrak{G}_{\mathbb{Q}} \to A^\times | \varphi \mathrm{mod}\ \mathfrak{m}_A = \det(\overline{\rho}), \varphi|_{I_l} = \iota_A \circ \chi|_{I_l}\ \forall l \neq p\}$$

Plainly this functor is represented by $W[[\Gamma]]$ with universal character $\kappa(\sigma) = \chi_0(\sigma)[\sigma]$, where χ_0 is the restriction of χ to $(\mathbb{Z}/N\mathbb{Z})^\times$ and $[\sigma]$ is the restriction of σ to $\mathbb{Q}_\infty$ with $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \Gamma$ for a subfield $\mathbb{Q}_\infty \subset \mathbb{Q}[\mu_{p^\infty}]$. Since $\det \boldsymbol{\rho}^{ord} \in D(R^{ord})$, we have $i = i_{R^{ord}} : W[[\Gamma]] \to R^{ord}$ such that $\det \boldsymbol{\rho}^{ord} = i \circ \kappa$.

5.10. **Reinterpretation of $\mathcal{D}$.** Consider the following deformation functor $\mathcal{D}_\Lambda : CL_{/\Lambda} \to SETS$

$$\mathcal{D}_\kappa(A) = \{\rho : \mathfrak{G}_{\mathbb{Q}} \to \mathrm{GL}_2(A) | \rho \mod \mathfrak{m}_A \cong \overline{\rho}, \rho \text{ satisfies } (\mathrm{ord}_p), (\mathrm{ord}_l) \text{ and } (\det{}_\Lambda)\}/\cong,$$

where writing $i_A : \Lambda \to A$ for Λ-algebra structure of A,

$$(\det{}_\Lambda) \qquad \det(\rho) = i_A \circ \kappa.$$

Proposition 5.4. *We have $\mathcal{D}_\kappa(A) \cong \mathrm{Hom}_{\Lambda\text{-}alg}(R^{ord}, A)$ with universal representation $\boldsymbol{\rho}^{ord} \in \mathcal{D}(R^{ord})$; so,*

$$\mathrm{Sel}(Ad(\overline{\rho})) := t_{R^{ord}/\Lambda} = \mathrm{Ker}(H^1(\mathfrak{G}_{\mathbb{Q}}, Ad(\overline{\rho})) \to \prod_{l \in S \cup \{p\}} \frac{H^1(\mathbb{Q}_l, Ad(\overline{\rho}))}{\mathcal{D}_{\chi,l}(\mathbb{F}[\varepsilon])}).$$

Proof. For any $\rho \in \mathcal{D}_\Lambda(A)$, regard $\rho \in \mathcal{D}(A)$. Then we have $\varphi \in \mathrm{Hom}_{W\text{-alg}}(R^{ord}, A)$ such that $\varphi \circ \boldsymbol{\rho}^{ord} \cong \rho$. Thus $\varphi \circ \det(\boldsymbol{\rho}^{ord}) = \det(\rho)$. Since $\det(\rho) = i_A \circ \kappa$ and $\det(\boldsymbol{\rho}^{ord}) = i_{R^{ord}} \circ \kappa$, we find $\varphi \circ i_{R^{ord}} = i_A$, and hence $\varphi \in \mathrm{Hom}_{\Lambda\text{-alg}}(R^{ord}, A)$. This shows that R^{ord} also represents $\mathcal{D}_\kappa$ over Λ.

As we already remarked, $\mathcal{D}_\kappa(\mathbb{F}[\varepsilon]) = t_{R^{ord}/\Lambda} = \mathfrak{m}_{R^{ord}}/\mathfrak{m}^2_{R^{ord}} + \mathfrak{m}_\Lambda$ is independent as a subgroup of $H^1(\mathfrak{G}_{\mathbb{Q}}, Ad(\overline{\rho}))$; so, we get a new expression of $\mathrm{Sel}(Ad(\overline{\rho}))$. □

By the proof, $\Omega_{R^{ord}/\Lambda} \otimes_{R^{ord}} \mathbb{F} \cong \mathrm{Sel}(Ad(\overline{\rho})) \cong \Omega_{R_\chi/W} \otimes_{R_\chi} \mathbb{F}$, so the smallest number of generators of $\Omega_{R^{ord}/\Lambda}$ as R^{ord}-modules and $\Omega_{R_\chi/W}$ as R_χ modules is equal. In the same way, the number of generators of R^{ord} as Λ-algebras and R_χ as W-algebras is equal.

5.11. **Compatible basis of** $c \in \mathcal{F}(A)$**.** By (ord_l) for $l \in S \cup \{p\}$, the universal representation $\boldsymbol{\rho}_\chi$ is equipped with a basis $(\mathbf{v}_l, \mathbf{w}_l)$ so that the matrix representation with respect this basis satisfies (ord_l). By representability, each class $c \in \mathcal{F}(A)$ has ρ such that $V(\rho) = V(\boldsymbol{\rho}_\chi) \otimes_{R_\chi,\varphi} A$ for a unique $\varphi \in \mathrm{Hom}_{B\text{-alg}}(R_\chi, A)$, we can choose a unique $\rho \in c$ is equipped with a basis $\{(v_l = \mathbf{v}_l \otimes 1, w_l = \mathbf{w}_l \otimes 1\}_l$ satisfying $\{(\mathrm{ord}_l){:}l \in S \cup \{p\}\}$ compatible with specialization. We always choose such a specific representative ρ for each class $c \in \mathcal{F}(A)$ hereafter.

Take a finite A-module X and consider the ring $A[X] = A \oplus X$ with $X^2 = 0$. Then $A[X]$ is still p-profinite. Pick $\rho \in \mathcal{F}(A[X])$ such that $\rho \mod X \sim \rho_0$. By our choice of representative ρ and ρ_0 as above, we may (and do) assume $\rho \mod X = \rho_0$.

5.12. **General cocycle construction.** Here we allow $\chi = \kappa$ but if $\chi = \kappa$, we assume that $A \in CL_\Lambda$. Writing $B = W$ if χ has values in $W^\times$ and Λ if $\chi = \kappa$, the functor $\mathcal{F}$ is defined over $CL_{/B}$. Let ρ_0 act on $M_2(A)$ and $\mathfrak{sl}_2(A) = \{x \in M_2(A) | \mathrm{Tr}(x) = 0\}$ by conjugation. Write this representation $ad(\rho)$ and $Ad(\rho)$ as before. Let $ad(X) = ad(A) \otimes_A X$ and $Ad(X) = Ad(A) \otimes_A X$ and regard them as $\mathfrak{G}_\mathbb{Q}$-modules by the action on $ad(A)$ and $Ad(A)$. Then we define

$$\Phi(A[X]) = \frac{\{\rho : \mathfrak{G}_\mathbb{Q} \to \mathrm{GL}_2(A[X]) | (\rho \mod X) = \rho_0, [\rho] \in \mathcal{F}(A[X])\}}{1 + M_2(X)},$$

where $[\rho]$ is the isomorphism class in $\mathcal{F}(A)$ containing ρ and ρ is assumed to satisfy the lifting property described in §5.11.

Take X finite as above. For $\rho \in \Phi(X)$, we can write $\rho = \rho_0 \oplus u'_\rho$ letting ρ_0 acts on $M_2(X)$ by matrix multiplication from the right. Then as before

$$\rho_0(gh) \oplus u'_\rho(gh) = (\rho_0(g) \oplus u'_\rho(g))(\rho_0(h) \oplus u'_\rho(h)) = \rho_0(gh) \oplus (u'_\rho(g)\rho_0(h) + \rho_0(g)u'_\rho(h))$$

produces $u'_\rho(gh) = u'_\rho(g)\rho_0(h) + \rho_0(g)u'_\rho(h)$ and multiplying by $\rho_0(gh)^{-1}$ from the right, we get the cocycle relation for $u_\rho(g) = u'_\rho(g)\rho_0(g)^{-1}$:

$$u_\rho(gh) = u_\rho(g) + gu_\rho(h) \text{ for } gu_\rho(h) = \rho(g)u_\rho(h)\rho_0(g)^{-1},$$

getting the map $\Phi(A[X]) \to H^1(\mathfrak{G}_\mathbb{Q}, ad(X))$ which factors through $H^1(\mathfrak{G}_\mathbb{Q}, Ad(X))$. As before this map is injective A-linear map identifying $\Phi(A[X])$ with $\mathrm{Sel}(Ad(X))$.

5.13. **General adjoint Selmer group.** We see that $u_\rho : \mathfrak{G}_\mathbb{Q} \to Ad(X)$ is a 1-cocycle, and we get an embedding $\Phi(A[X]) \hookrightarrow H^1(\mathbb{Q}_l, Ad(X))$ for $l \in S \cup \{p\}$ by $\rho \mapsto [u_\rho]$. We consider local version of Φ replacing $\mathfrak{G}_\mathbb{Q}$ by D_l:

$$\Phi_l(A[X]) := \frac{\{\rho : D_l \to \mathrm{GL}_2(A[X]) | \widetilde{\rho} \mod X = \rho_0, [\rho] \in \mathcal{F}_l(A[X])\}}{1 + M_2(X)},$$

and we define

$$\mathrm{Sel}(Ad(X)) := \mathrm{Ker}(H^1(\mathfrak{G}_\mathbb{Q}, Ad(X)) \to \prod_{l \in S \cup \{p\}} \frac{H^1(\mathbb{Q}_l, Ad(\overline{\rho}))}{\Phi_l(A[X])}),$$

If $X = \varinjlim_i X_i$ for finite A-modules X_i, we just define

$$\mathrm{Sel}(Ad(X)) = \varinjlim_i \mathrm{Sel}(Ad(X_i)).$$

Then for finite X_i,

$$\Phi(A[X_i]) = \mathrm{Sel}(Ad(X_i)) \text{ and } \varinjlim_i \Phi(X_i) = \mathrm{Sel}(\varinjlim_i Ad(X_i)).$$

5.14. **Differentials and Selmer group.** For each $[\rho_0] \in \mathcal{F}(A)$, choose a representative $\rho_0 = \varphi \circ \boldsymbol{\rho}$ as in §5.11. Then we have a map $\Phi(A[X]) \to \mathcal{F}(A[X])$ for each finite A-module X sending $\rho \in \Phi(A[X])$ chosen as in §5.11 to the class $[\rho] \in \mathcal{F}(A[X])$. By our choice of ρ as in §5.11, this map is injective.

Conversely pick a class $c \in \mathcal{F}(A[X])$ over $[\rho_0] \in \mathcal{F}(A)$. Then for $\rho \in c$, we have $x \in 1 + M_2(\mathfrak{m}_{A[X]})$ such that $x\rho x^{-1} \mod X = \rho_0$. By replacing ρ by $x\rho x^{-1}$ and choosing the lifted base, we conclude $\Phi(A[X]) \cong \{[\rho] \in \mathcal{F}(A[X]) | \rho \mod X \sim \rho_0\}$; so, for finite X,

$$\begin{aligned}\mathrm{Sel}(Ad(X)) = \Phi(A[X]) &= \{\phi \in \mathrm{Hom}_{B\text{-alg}}(R_\chi, A[X]) : \phi \mathrm{mod}\ X = \varphi\} \\ &= Der_B(R_\chi, X) \xrightarrow[\sim]{\text{Corollary 2.3}} \mathrm{Hom}_A(\Omega_{R_\chi/B} \otimes_{R_\chi,\varphi} A, X).\end{aligned}$$

Thus

$$\boxed{\mathrm{Sel}(Ad(X)) \cong \mathrm{Hom}_A(\Omega_{R_\chi/B} \otimes_{R_\chi,\varphi} A, X)}. \tag{5.1}$$

Theorem 5.5. *We have a canonical isomorphism:* $\mathrm{Sel}(Ad(\rho_0))^\vee \cong \Omega_{R_\chi/B} \otimes_{R_\chi,\varphi} A$.

Proof. Take the Pontryagin dual

$$A^\vee := \mathrm{Hom}_B(A, B^\vee) = \mathrm{Hom}_{\mathbb{Z}_p}(A \otimes_B B, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p).$$

Since $A = \varprojlim_i A_i$ for finite i and $\mathbb{Q}_p/\mathbb{Z}_p = \varinjlim_j p^{-1}\mathbb{Z}/\mathbb{Z}$, $A^\vee = \varinjlim_i \mathrm{Hom}(A_i, \mathbb{Q}_p/\mathbb{Z}_p) = \varinjlim_i A_i^\vee$ is a union of the finite modules $A_i^\vee$. We define $\mathrm{Sel}(Ad(\rho_0)) := \varinjlim_j \mathrm{Sel}(Ad(A_i^\vee))$. Defining $\Phi(A[A^\vee]) = \varinjlim_i \Phi_l(A[A_i^\vee])$, we see from compatibility of cohomology with injective limit

$$\mathrm{Sel}(Ad(\rho_0)) = \varinjlim_i \mathrm{Sel}(Ad(A_i^\vee)) = \varinjlim_j \mathrm{Ker}(H^1(\mathfrak{G}_{\mathbb{Q}}, Ad(A_i^\vee)) \to \prod_{l \in S \cup \{p\}} \frac{H^1(\mathbb{Q}_l, Ad(A_i^\vee))}{\Phi_l(A[A_i^\vee])})$$

By the boxed formula (5.1),

$$\begin{aligned}\mathrm{Sel}(Ad(\rho_0)) &= \varinjlim_i \mathrm{Sel}(Ad(A_i^\vee)) = \varinjlim_i \mathrm{Hom}_{R_\chi}(\Omega_{R_\chi/B} \otimes_{R_\chi} A, A_i^\vee) \\ &= \mathrm{Hom}_A(\Omega_{R_\chi/B} \otimes_{R_\chi} A, A^\vee) = \mathrm{Hom}_A(\Omega_{R_\chi/B} \otimes_{R_\chi} A, \mathrm{Hom}_{\mathbb{Z}_p}(A, \mathbb{Z}_p)) \\ &= \mathrm{Hom}_{\mathbb{Z}_p}(\Omega_{R_\chi/B} \otimes_{R_\chi} A, \mathbb{Q}_p/\mathbb{Z}_p) = (\Omega_{R_\chi/B} \otimes_{R_\chi} A)^\vee.\end{aligned}$$

Taking Pontryagin dual back, we finally get

$$\boxed{\mathrm{Sel}(Ad(\rho_0))^\vee \cong \Omega_{R_\chi/B} \otimes_{R_\chi,\varphi} A \text{ and } \mathrm{Sel}(Ad(\overline{\rho}))^\vee \cong \Omega_{R_\chi/B} \otimes_{R_\chi} \mathbb{F}}$$

as desired. In particular, $\mathrm{Sel}(Ad(\boldsymbol{\rho}_\chi))^\vee = \Omega_{R_\chi/B}$ (with $\boldsymbol{\rho}_\kappa = \boldsymbol{\rho}^{ord}$ if $\chi = \kappa$). □

This is the generalization of the formula

$$Cl_F \otimes_{\mathbb{Z}} W \cong \Omega_{W[Cl_{F,p}]/W} \otimes_{W[Cl_{F,p}]} W.$$

5.15. **p-Local condition.** The submodule $\Phi_p(A[X])$ in the cohomology group $H^1(\mathbb{Q}_p, Ad(X))$ is made of classes of 1-cocycles u with $u|_{I_p}$ is upper nilpotent and $u|_{D_p}$ is upper triangular with respect to the compatible basis (v_p, w_p). Suppose we have $\sigma \in I_p$ such that $\rho_0(\sigma) = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ such that $\alpha \not\equiv \beta \mod \mathfrak{m}_A$. Suppose u is upper nilpotent over I_p. Then for $\tau \in D_p$, we have $Ad(\rho_0)(\tau)u(\tau^{-1}\sigma\tau) = (Ad(\rho_0)(\sigma) - 1)u(\tau) + u(\sigma)$. Writing $u(\tau) = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$, we find $(Ad(\rho_0)(\sigma) - 1)u(\tau) = \left(\begin{smallmatrix} 0 & (\alpha\beta^{-1}-1)b \\ (\alpha^{-1}\beta-1)c & 0 \end{smallmatrix}\right)$. Since $\rho_0(\tau)$ is upper triangular and $u(\tau^{-1}\sigma\tau)$ is upper nilpotent, $Ad(\rho_0)(\tau)u(\tau^{-1}\sigma\tau)$ is still upper nilpotent; so, $(\alpha^{-1}\beta - 1)c = 0$ and hence $c = 0$. Therefore u is forced to be upper triangular over D_p. Thus we get

Lemma 5.6. *If $\overline{\rho}(\sigma)$ for at least one $\sigma \in I_p$ has two distinct eigenvalues, $\Phi_p(A[X])$ gives rise to the subgroup of $H^1(\mathbb{Q}_p, Ad(X))$ made of classes containing a 1-cocycle whose restriction to I_p is upper nilpotent.*

6. Upper bound of the number of Selmer generators

By Kummer theory, we give an upper bound of the dimension $\dim t_{R^{ord}/\Lambda} = \dim t_{R_\chi/W}$ by the dimension of the dual Selmer group, which turns out to be often optimal.

6.1. **Local class field theory.** We summarize facts from local class field theory. Let $K_{/\mathbb{Q}_p}$ be a finite extension with algebraic closure $\overline{K}$ with integer ring O. Write $D := \mathrm{Gal}(\overline{K}/K)$ fixing an algebraic closure $\overline{K}/K$. Let $D \triangleright I$ be the inertia subgroup and D^{ab} be its maximal continuous abelian quotient.

- $x \mapsto [x, K] : K^\times \hookrightarrow D^{ab}$ (the local Artin symbol);
- $[\varpi, K]$ modulo the inertia subgroup $I_{ab} \subset D^{ab}$ is the Frobenius element Frob;
- For any integer $0 < m \in \mathbb{Z}$, $K^\times/(K^\times)^m = K^\times \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \cong D^{ab}/mD^{ab}$ by Artin symbol;
- $O^\times \cong I_{ab}$ by Artin symbol.

6.2. **Local cohomology.** We summarize facts from local cohomology.

- $inv : H^2(K, \mu_m(\overline{K})) \cong \mathbb{Z}/m\mathbb{Z}$ (the invariant map);
- $H^1(K, \mu_m) \cong K^\times/(K^\times)^m$ (Kummer theory valid for any field $K \supset \mathbb{Q}$).

This follows from the long exact sequence of $H^?(M) := H^?(K, M)$ associated to $\mu_m(\overline{K}) \hookrightarrow \overline{K}^\times \xrightarrow{x\mapsto x^m} \overline{K}^\times$:

$$\begin{array}{ccccccc} H^0(\overline{K}^\times) & \xrightarrow{x\mapsto x^m} & H^0(\overline{K}^\times) & \longrightarrow & H^1(\mu_m) & \longrightarrow & H^1(\overline{K}^\times) \overset{(*)}{=} 0 \\ \wr\downarrow & & \wr\downarrow & & \wr\downarrow & & \\ K^\times & \xrightarrow[x\mapsto x^m]{} & K^\times & \longrightarrow & K^\times/(K^\times)^m, & & \end{array}$$

where the vanishing $(*)$ follows from Hilbert theorem 90.

6.3. **Local Tate duality.** For any finite (continuous) D-module M killed by $0 < m \in \mathbb{Z}$, let

$$M^*(1) := \mathrm{Hom}(M, \mu_m(\overline{K}))$$

as Galois module acting by $\sigma \cdot \phi(x) = \sigma(\phi(\sigma^{-1}x))$ (called Tate dual). Then

$$M^*(1) \otimes_{\mathbb{Z}/m\mathbb{Z}} M \ni \phi \otimes x \mapsto \phi(x) \in \mu_m$$

is a $\mathbb{Z}[D]$-morphism inducing a cup product pairing $H^r(M^*(1)) \times H^{2-r}(M) \to H^2(\mu_m) \xrightarrow{inv} \mathbb{Z}/m\mathbb{Z}$.

Theorem 6.1 (J. Tate)**.** *Cohomological dimension of D is equal to 2 and the above pairing is perfect for $r = 0, 1, 2$.*

If $M = \mu_m(\overline{K})$, by definition $\mu_m = (\mathbb{Z}/m\mathbb{Z})^*(1)$. We know $H^1(\mu_m) = K^\times/(K^\times)^m$ and $H^1(\mathbb{Z}/m\mathbb{Z}) = \mathrm{Hom}(D^{ab}/mD^{ab}, \mathbb{Z}/m\mathbb{Z})$. By local class field theory, $D^{ab}/mD^{ab} \cong K^\times/(K^\times)^m$; so, the duality in this case follows. One can deduce the proof of the duality in this special case basically by restricting to $\mathrm{Gal}(\overline{K}/K(M))$ for the splitting field $K(M)$ of M (see [MFG, Theorem 4.43]).

6.4. **Another example of local Tate duality.** Consider $\mathrm{Hom}(\mathrm{Frob}^{\widehat{\mathbb{Z}}}, M) \subset H^1(K, M)$ for a finite $\mathbb{Z}/m\mathbb{Z}$-module M on which D acts trivially. Here Frob is the Frobenius element in D/I.

Lemma 6.2. *The orthogonal complement of* $\mathrm{Hom}(\mathrm{Frob}^{\widehat{\mathbb{Z}}}, M) \subset H^1(K, M)$ *in the dual* $H^1(K, M^*(1)) = K^\times \otimes_{\mathbb{Z}} M$ *is given by* $O^\times \otimes_{\mathbb{Z}} M$*. In particular, the Tate duality between* $H^1(K, \mu_m)$ *and* $H^1(K, \mathbb{Z}/m\mathbb{Z})$ *gives rise to the tautological duality between* $\mathrm{Frob}^{\widehat{\mathbb{Z}}}/m\mathrm{Frob}^{\widehat{\mathbb{Z}}}$ *and* $\mathrm{Hom}(\mathrm{Frob}^{\widehat{\mathbb{Z}}}, \mathbb{Z}/m\mathbb{Z})$.

The result for general M follows from extending scalar to M; so, we may assume $M = \mathbb{Z}/m\mathbb{Z}$.

6.5. **Inflation-restriction.** To prove the lemma, we recall the inflation-restriction sequence. Let G be a profinite group and H is an open normal subgroup (so, G/H is finite). If M is a G-module, for a 1-cocycle $u : H \to M$, $g \cdot u := gu(g^{-1}hg)$ can be easily checked to be a one cocycle. If $u(h) = (h-1)m$, we see $g \cdot u(h) = g(g^{-1}hg - 1)m = (hg - g)m = (h-1)(gm)$; so, this preserves coboundaries, and hence G/H acts on $H^1(H, M)$.

Since H fixes $M^H = H^0(H, M)$, M^H is a G/H-module. The inflation restriction **exact** sequence is

$$0 \to H^1(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^1(G, M) \xrightarrow{\mathrm{Res}} H^1(H, M)^{G/H} \to H^2(G/H, M),$$

where $\mathrm{Inf}(u)(g) = u(g \mod H)$ and $\mathrm{Res}(u) = u|_H$ for cocycles. For a proof of this, see [MFG, Theorem 4.33].

6.6. **Proof of Lemma 6.2.** The last statement follows from the construction of pairing between $H^1(K, \mu_m)$ and $H^1(K, \mathbb{Z}/m\mathbb{Z})$ described in §5.2.

By the inflation-restriction sequence, we have an exact sequence

$$0 \to \mathrm{Hom}(D/I, \mathbb{Z}/m\mathbb{Z}) \to \mathrm{Hom}(D, \mathbb{Z}/m\mathbb{Z}) \to \mathrm{Hom}(I, \mathbb{Z}/m\mathbb{Z}) \to 0$$

for the inertia group $I \triangleright D$. Since $D/I = \mathrm{Frob}^{\widehat{\mathbb{Z}}}$, we have the following commutative diagram with exact rows:

$$\begin{array}{ccccc} (O^\times/(O^\times)^m) & \xrightarrow{\hookrightarrow} & (K^\times/(K^\times)^m) & \xrightarrow{\twoheadrightarrow} & \mathrm{Frob}^{\widehat{\mathbb{Z}}}/\mathrm{Frob}^{m\widehat{\mathbb{Z}}} \\ \wr\downarrow & & \wr\downarrow & & \wr\downarrow \\ H^1(I, \mathbb{Z}/m\mathbb{Z})^\vee & \xrightarrow[\hookrightarrow]{} & H^1(K, \mathbb{Z}/m\mathbb{Z})^\vee & \xrightarrow[\twoheadrightarrow]{} & H^1(D/I, \mathbb{Z}/m\mathbb{Z})^\vee. \end{array}$$

Since the image of I in D^{ab} is given by $O^\times$, the result follows. □

6.7. **Dual Selmer group.** By trace pairing $(x,y)=\mathrm{Tr}(xy)$ the Galois modules $ad(\overline{\rho})$ and $Ad(\overline{\rho})$ are self dual; so, $ad(\overline{\rho})^*(1)=ad(\overline{\rho})(1)$ and $Ad(\overline{\rho})^*(1)=Ad(\overline{\rho})(1)$. The dual Selmer group of $ad(\overline{\rho})$ and $Ad(\overline{\rho})$ is defined as follows:

$$\mathrm{Sel}^{\perp}(Ad(\overline{\rho})(1)):=\mathrm{Ker}(H^1(\mathfrak{G}_{\mathbb{Q}},Ad(\overline{\rho})(1))\to\prod_{l\in S\cup\{p\}}\frac{H^1(\mathbb{Q}_l,Ad(\overline{\rho})(1))}{\mathcal{D}_{\chi,l}(\mathbb{F}[\varepsilon])^{\perp}}),$$

$$\mathrm{Sel}^{\perp}(ad(\overline{\rho})(1)):=\mathrm{Ker}(H^1(\mathfrak{G}_{\mathbb{Q}},ad(\overline{\rho})(1))\to\prod_{l\in S\cup\{p\}}\frac{H^1(\mathbb{Q}_l,ad(\overline{\rho})(1))}{\mathcal{D}_{l}(\mathbb{F}[\varepsilon])^{\perp}}).$$

Here "$\perp$" indicates the orthogonal complement under the Tate duality. We have the following bound due to R. Greenberg and A. Wiles:

Lemma 6.3. $\dim_{\mathbb{F}}\mathrm{Sel}(Ad(\overline{\rho}))\le\dim_{\mathbb{F}}\mathrm{Sel}^{\perp}(Ad(\overline{\rho})(1))$.

This we admit. For a proof, see [MFG, Proposition 3.40] or [HMI, Proposition 3.29].

6.8. **Details of $H^1(K,\mu_p)\cong K^\times\otimes_{\mathbb{Z}}\mathbb{F}_p$.** Here K is any field. The connection map δ of the long exact sequence $H^0(K,M)\to H^0(N)\xrightarrow{\delta}H^1(L)$ of a short exact sequence $L\hookrightarrow M\twoheadrightarrow N$ is given as follows: Pick $n\in H^0(K,N)$ and lift it to $m\in M$. Then for $\sigma\in\mathrm{Gal}(\overline{K}/K)$, $(\sigma-1)m$ is sent to $(\sigma-1)n=0$ as n is fixed by σ. Thus we may regard $u_m:\sigma\mapsto(\sigma-1)m$ is a 1-cocycle with values in L. If we choose another lift m', then $m'-m=l\in L$ and hence $u_{m'}-u_m=(\sigma-1)l$ which is a coboundary. Thus we get the map δ sending m to the class $[u_m]$.

Applying this, the cocycle u_α corresponding $\alpha\in K^\times/(K^\times)^p=K^\times\otimes\mathbb{F}_p$ is given by

$$\boxed{u_\alpha(\sigma)={}^{\sigma-1}(\sqrt[p]{\alpha}).}$$

6.9. **Unramifiedness of u_α at a prime $\mathfrak{l}\neq p$.** Let K be an $\mathfrak{l}$-adic field which is a finite extension of $\mathbb{Q}_l$ for a prime $l\neq p$. If $\alpha\notin(K^\times)^p$, $\alpha':=l^{p^N}\alpha\notin(K^\times)^p$ with $K[\sqrt[p]{\alpha}]=K[\sqrt[p]{\alpha'}]$ and $u_\alpha=u_{\alpha'}$. Replacing α by α' for a sufficiently large N, we may assume that $\alpha\in O\cap K^\times$.

The minimal equation of $\sqrt[p]{\alpha}$ is $f(X)=X^p-\alpha$. Since the derivative $f'(X)=pX^{p-1}$, the different of $K[\sqrt[p]{\alpha}]/K$ is a factor of $p\sqrt[p]{\alpha}^{p-1}$. Thus we find

$$\boxed{u_\alpha\text{ is unramified}\Leftrightarrow\alpha\in O^\times}$$

choosing $\alpha\in O\cap K^\times$. This can be also shown by noting that all conjugates of $\sqrt[p]{\alpha}$ is given by $\{\zeta\sqrt[p]{\alpha}|\zeta\in\mu_p\}$ which has p distinct elements modulo $\mathfrak{l}$ if and only if $\alpha\in O^\times$.

6.10. **Restriction to the splitting field of $Ad:=Ad(\overline{\rho})$.** Let F be the splitting field of $Ad:=Ad(\overline{\rho})$; so, $F=\overline{\mathbb{Q}}^{\mathrm{Ker}(Ad)}$, and $K:=F[\mu_p]$ is the splitting field of $Ad(1)$. Write $G:=\mathrm{Gal}(F/\mathbb{Q})$. Let $\mathfrak{G}_F=\mathrm{Ker}(Ad|_{\mathfrak{G}_{\mathbb{Q}}})$. We realize $\mathrm{Sel}^{\perp}(Ad(1))$ inside $H^1(F,Ad(1))=F^\times\otimes_{\mathbb{Z}}Ad$. Assume

$$H^j(F/\mathbb{Q},Ad(1)^{\mathfrak{G}_K})=0\ \text{ for }j=1,2,\qquad\text{(CV)}$$

which follows if $K=F[\mu_p]\neq F$ or $p\nmid[F:\mathbb{Q}]$. If $F[\mu_p]\neq F$, we see $Ad(1)^{\mathfrak{G}_F}=0$ as Ad is trivial over $\mathfrak{G}_F$. If $p\nmid[F:\mathbb{Q}]=|G|$, we note $H^q(G,M)=0$ for any $\mathbb{F}[G]$-module M [MFG, Prop. 4.21]. Again by inflation-restriction,

$$H^1(G,Ad(1)^{\mathfrak{G}_F})\hookrightarrow H^1(\mathbb{Q},Ad(1))\to H^1(F,Ad(1))^G\to H^2(G,Ad(1)^{\mathfrak{G}_F}).$$

is exact. So

$$H^1(\mathbb{Q},Ad(1))\cong(F^\times\otimes_{\mathbb{Z}}Ad)^G.$$

6.11. **Kummer theory.** We analyze how G acts on $F^\times\otimes_{\mathbb{F}_p}Ad$. The action of $\tau\in G$ is given by ${}^\tau u(g)=\tau u(\tau^{-1}g\tau)=Ad(\tau)u(\tau^{-1}g\tau)$ $(\tau\in G)$ for cocycle u giving rise to a class in $H^1(F,Ad(1))$. For a basis (v_1,v_2,v_3) of Ad giving an identification $Ad=\mathbb{F}^3$, and write $u=v\underline{u}$ for $\underline{u}:={}^t(u_1,u_2,u_3)$ (column vector) for $v=(v_1,v_2,v_3)$ (row vector) as a $\mathbb{F}^3$ valued cocycle; so, $\tau v=(\tau v_1,\tau v_2,\tau v_3)=v^tAd(\tau)$. Since $u_j(g)=u_{\alpha_j}(g)={}^{g-1}\sqrt[p]{\alpha}_j$ for $\alpha_j\in F^\times\otimes_{\mathbb{Z}}\mathbb{F}$, rewriting $u_\alpha:=\underline{u}$, we have $\tau(v^\tau u_\alpha(\tau^{-1}g\tau))=v^tAd(\tau)u_{\tau_\alpha}(g)$. Thus τ-invariance implies

$$u_{\tau_\alpha}:={}^t(u_{\tau_{\alpha_1}},u_{\tau_{\alpha_2}},u_{\tau_{\alpha_3}})={}^tAd(\tau)^{-1}u_\alpha\Leftrightarrow v^tAd(\tau)u_{\tau_\alpha}(g)=vu_\alpha.$$

Therefore inside $F^\times \otimes_{\mathbb{Z}} \mathbb{F}$, α_js span an $\mathbb{F}$-vector space on which G acts by a factor of $Ad \cong {}^t Ad^{-1}$. Thus we get

$$H^1(\mathbb{Q}, Ad \otimes \overline{\omega}) \cong \mathrm{Hom}_{\mathbb{F}[G]}(Ad, F^\times \otimes_{\mathbb{Z}} \mathbb{F}) =: (F^\times \otimes_{\mathbb{Z}} \mathbb{F})[Ad]. \tag{6.1}$$

6.12. **Selmer group as a subgroup of $F^\times \otimes_{\mathbb{Z}} \mathbb{F}$.**

Theorem 6.4. *Let O be the integer ring of F. If $p \nmid h_F = |Cl_F|$, we have the following inclusion*

$$\mathrm{Sel}^\perp(Ad(\overline{\rho})(1)) \hookrightarrow O^\times \otimes_{\mathbb{Z}} \mathbb{F}[Ad(\overline{\rho})].$$

We start the proof of the theorem which ends in §6.15. Let $[u] \in \mathrm{Sel}^\perp(Ad(\overline{\rho})(1))$ for a cocycle $u : \mathfrak{G}_{\mathbb{Q}} \to Ad(\overline{\rho})(1)$. Thus $u|_{\mathfrak{G}_F}$ gives rise to u_α for $\alpha \in F^\times \otimes_{\mathbb{Z}} \mathbb{F}[Ad(\overline{\rho})]$ by Kummer theory. Consider the fractional ideal $(\alpha) = \alpha O[\frac{1}{p}]$. Make a prime decomposition $(\alpha) = \prod_{\mathfrak{l}} \mathfrak{l}^{e(\mathfrak{l})}$ in $O[\frac{1}{p}]$. Since u_α is unramified at all $l \neq p$, we find $\boxed{p|e(\mathfrak{l})}$ as otherwise, $\mathfrak{l}$ ramifies in $F[\sqrt[p]{\alpha}]$. So $(\alpha) = \mathfrak{a}^p$ for $\mathfrak{a} = \prod_{\mathfrak{l}} \mathfrak{l}^{e(\mathfrak{l})/p}$

6.13. **l-integrality ($l \neq p$).** If a local Kummer cocycle u_α associated to $\alpha \in F_v^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ for $v \nmid p$ is unramified, then α vanishes in $(F_v^\times/O_v^\times) \otimes_{\mathbb{Z}} \mathbb{F}_p$. The local cocycle is trivial if and only if α vanishes in $F_v^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$. If a global Kummer cocycle u_α for $\alpha \in F^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ is trivial at $v|N$ and unramified outside p, then the principal ideal $\alpha O[\frac{1}{p}]$ is a p-power $\mathfrak{a}^p$.

If $p \nmid h := h_F = |Cl_F|$, replacing α by α^h does not change the Kummer cocycle up to non-zero scalar. We do this replacement and write α instead of α^h. Then $\mathfrak{a}$ is replaced by the principal ideal $\mathfrak{a}^h = (\alpha')$, and we find that $\alpha = \varepsilon \alpha'^p$ for $\varepsilon \in O[\frac{1}{p}]^\times$. Thus $u_\alpha = u_\varepsilon$. Therefore

$$\boxed{\mathrm{Sel}^\perp(Ad(1)) \subset (O[\frac{1}{p}]^\times \otimes_{\mathbb{Z}} \mathbb{F})[Ad].}$$

6.14. **Case where $\overline{\rho}|_D$ is indecomposable for $D = \mathrm{Gal}(F_{\mathfrak{p}}/\mathbb{Q}_p)$.** By indecomposability, the matrix form of $Ad(\sigma)$ if $\overline{\rho}(\sigma) = \left(\begin{smallmatrix} \overline{\epsilon} & a \\ 0 & \overline{\delta} \end{smallmatrix}\right)$ $(a \neq 0)$ with respect to the basis $\{\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\}$ is

$$\begin{pmatrix} \overline{\epsilon}\overline{\delta}^{-1} & -2\overline{\delta}^{-1}a & -(\overline{\epsilon}\overline{\delta})^{-1}a^2 \\ 0 & 1 & \overline{\epsilon}^{-1}a \\ 0 & 0 & \overline{\epsilon}^{-1}\overline{\delta} \end{pmatrix},$$

in short, Ad is also an indecomposable D-module without trivial quotient. We have an exact sequence of D-modules:

$$O^\times \otimes_{\mathbb{Z}} \mathbb{F} \hookrightarrow O[\frac{1}{p}]^\times \otimes_{\mathbb{Z}} \mathbb{F} \xrightarrow[\twoheadrightarrow]{\xi \mapsto (\xi)} \oplus_{\sigma \in G/D} \mathbb{F}\mathfrak{p}^{e\sigma} \cong \mathrm{Ind}_D^G \mathbf{1},$$

where e is the order of the class of $\mathfrak{p}$ in Cl_F. By Shapiro's lemma [MFG, Lemma 4.20, (4.27)], $\mathrm{Ind}_D^G \mathbf{1}[Ad] = \mathrm{Hom}_{\mathbb{F}[G]}(Ad, \mathrm{Ind}_D^G \mathbf{1}) = \mathrm{Hom}_D(Ad|_D, \mathbf{1}) = 0$ by indecomposability; so, $\mathrm{Sel}^\perp(Ad(1)) \subset (O^\times \otimes \mathbb{F})[Ad]$.

6.15. **Case where $\overline{\rho}|_D$ is completely reducible.** In this case, we have

$$\mathrm{Ind}_D^G \mathbf{1}[Ad] = \mathrm{Hom}_{\mathbb{F}[G]}(Ad, \mathrm{Ind}_D^G \mathbf{1}) = \mathrm{Hom}_D(Ad|_D, \mathbf{1}) = \mathbb{F}.$$

If a cocycle $u : D_{\mathfrak{p}} \to Ad(1)$ restricted to the decomposition group $D_{\mathfrak{p}} = \mathrm{Gal}(\overline{\mathbb{Q}}/F_{\mathfrak{p}})$ at $\mathfrak{p}$ project down non-trivially to $F_{\mathfrak{p}}^\times \otimes \mathbb{F}[\mathbf{1}]$ (i.e., $u \in H^1(\mathbb{Q}_p, \mu_p \otimes \mathbb{F})$), by the lemma in §5.4, if u is a dual Selmer cocycle it corresponds to an element in $O_{\mathfrak{p}}^\times \otimes \mathbb{F}$. Since $\mathfrak{p}|p$ is arbitrary, we conclude again

$$\boxed{\mathrm{Sel}^\perp(Ad(1)) \subset (O^\times \otimes_{\mathbb{Z}} \mathbb{F})[Ad].}$$

This finishes the proof of the theorem. □

6.16. **Dirichlet's unit theorem.** Fix a complex conjugation $c \in G$ and C be the subgroup generated by c. Let ∞ be the set of complex places of F. Dirichlet's unit theorem is proven by considering

$$O^\times \xrightarrow{Log} \mathbb{R}^\infty := \prod_\infty \mathbb{R}$$

given by $Log(\varepsilon) = (\log |\varepsilon|_v)_{v \in \infty}$ and showing $\mathrm{Im}(Log) \otimes_{\mathbb{Z}} \mathbb{R} = \mathrm{Ker}(\mathbb{R}^\infty \xrightarrow{\mathrm{Tr}} \mathbb{R})$ for $\mathrm{Tr}(x_v)_v = \sum_v x_v$. The Galois group G acts by permutation on $\infty \cong G/C$. Therefore $\mathbb{R}^\infty \cong \mathrm{Ind}_C^G \mathbf{1}$. Thus $(O^\times \otimes \mathbb{Q}) \oplus \mathbf{1} \cong \mathrm{Ind}_C^G \mathbb{Q}\mathbf{1}$.

If $p \nmid |G|$, any $\mathbb{F}[G]$-module over $\mathbb{F}$ is semi-simple; so, characterized by its trace. Therefore this descends to $O^\times/\mu_p(F) \otimes_{\mathbb{Z}} \mathbb{F}$ and

$$\boxed{\mathrm{Ind}_C^G \mathbb{F}\mathbf{1} \cong (O^\times/\mu_p(F) \otimes_{\mathbb{Z}} \mathbb{F}) \oplus \mathbb{F}\mathbf{1}.}$$

Theorem 6.5. *We have* $\dim_{\mathbb{F}} \mathrm{Sel}^\perp(Ad(1)) \leq 1$ *if* $p \nmid |G|h_F$.

Proof. By Shapiro's lemma, we have

$$\begin{aligned}(O^\times/\mu_p(F) \otimes_{\mathbb{Z}} \mathbb{F})[Ad] &= \mathrm{Hom}_G(Ad, (O^\times/\mu_p(F)) \otimes_{\mathbb{Z}} \mathbb{F}) \\ &\cong \mathrm{Hom}_G(Ad, \mathrm{Ind}_C^G \mathbb{F}\mathbf{1}) \cong \mathrm{Hom}_C(Ad|_C, \mathbb{F}\mathbf{1}) \cong \mathbb{F},\end{aligned}$$

since $Ad(c) \sim \mathrm{diag}[-1, 1, -1]$. By irreducibility, $\mu_p(F)[Ad] = 0$; so, $(O^\times \otimes_{\mathbb{Z}} \mathbb{F})[Ad] \cong \mathbb{F}$. By §5.12, we have

$$\mathrm{Sel}^\perp(Ad(1)) \hookrightarrow (O^\times \otimes_{\mathbb{Z}} \mathbb{F})[Ad] \cong \mathbb{F},$$

we conclude $\boxed{\dim_{\mathbb{F}} \mathrm{Sel}^\perp(Ad(1)) \leq 1}$. □

Corollary 6.6. *If* $p \nmid |G|h_F$*, then for any deformation* $\rho \in \mathcal{D}_\chi(A)$*,* $\mathrm{Sel}(Ad(\rho))$ *is generated by at most one element over* A.

7. Selmer group of induced Galois representation

Assuming that $\rho_0 = \mathrm{Ind}_K^{\mathbb{Q}} \varphi$ for a quadratic field $K = \mathbb{Q}[\sqrt{D}]$ (with discriminant D) and a character $\varphi : \mathfrak{G}_K \to W^\times$ of order prime to p, we explore the meaning of the cyclicity of $\mathrm{Sel}(\rho_0)^\vee$ in terms of Iwasawa theory over K. Write $\overline{\varphi} := (\varphi \bmod \mathfrak{m}_W)$ and $\overline{\rho} = \mathrm{Ind}_K^{\mathbb{Q}} \overline{\varphi}$. We denote by O the integer ring of K.

7.1. **Induced representation.** Let $A \in CL_{/W}$ and G be a profinite group with a subgroup H of index 2. Put $\Delta := G/H$. Let H be a character $\varphi : G \to A$. Let $A(\varphi) \cong A$ on which H acts by φ. Regard the group algebra $A[G]$ as a left and right $A[G]$-module by multiplication. Define $A(\mathrm{Ind}_H^G \varphi) := A[G] \otimes_{A[H]} A(\varphi)$ (so, $\xi h \otimes a = \xi \otimes ha = \xi \otimes \varphi(h)a = \varphi(a)(\xi \otimes a))$ for $h \in H$. and let G acts on $A(\mathrm{Ind}_H^G \varphi)$ by $g(\xi \otimes a) := (g\xi) \otimes a$. The resulted G-module $A(\mathrm{Ind}_G^H \varphi)$ is the induced module.

Similarly we can think of $A(\mathrm{ind}_G^H \varphi) := \mathrm{Hom}_{A[H]}(A[G], A(\varphi))$ (so, $\phi(h\xi) = h\phi(\xi) = \varphi(h)\phi(\xi))$ on which $g \in G$ acts by $g\phi(\xi) = \phi(\xi g)$.

7.2. **Matrix form of** $\mathrm{Ind}_H^G \varphi$**.** Suppose that φ has order prime to p. Then for $\sigma \in G$ generating G over H, $\varphi_\sigma(h) = \varphi(\sigma^{-1}h\sigma)$ is again a character of H. The module $\mathrm{Ind}_H^G \varphi$ has a basis $1_G \otimes 1$ and $\sigma \otimes 1$ for the identity element 1_G of G and $1 \in A \cong A(\varphi)$.

We have

$$\begin{aligned}g(1_G \otimes 1, \sigma \otimes 1) &= (g \otimes 1, g\sigma \otimes 1) \\ &= \begin{cases} (1_G \otimes g, \sigma \otimes \sigma^{-1}g\sigma) = (1_G \otimes 1, \sigma \otimes 1)\begin{pmatrix} \varphi(g) & 0 \\ 0 & \varphi_\sigma(g)\end{pmatrix} & \text{if } g \in H, \\ (\sigma \otimes \sigma^{-1}g, 1_G \otimes g\sigma) = (1_G \otimes 1, \sigma \otimes 1)\begin{pmatrix} 0 & \varphi(g\sigma) \\ \varphi(\sigma^{-1}g) & 0\end{pmatrix} & \text{if } g\sigma \in H,\end{cases}\end{aligned}$$

Thus extending φ to G by 0 outside H, we get

$$\boxed{\mathrm{Ind}_H^G \varphi(g) = \begin{pmatrix} \varphi(g) & \varphi(g\sigma) \\ \varphi(\sigma^{-1}g) & \varphi(\sigma^{-1}g\sigma)\end{pmatrix}.} \tag{7.1}$$

7.3. **Two inductions are equal.** The induction $\mathrm{ind}_H^G \varphi$ has basis (ϕ_1, ϕ_σ) given by $\phi_1(\xi + \xi'\sigma) = \varphi(\xi) \in A = A(\varphi)$ and $\phi_\sigma(\xi + \xi'\sigma^{-1}) = \varphi(\xi') \in A = A(\varphi)$ for $\xi \in A[H]$; so, $(*)$ $\phi_1(\xi' + \xi\sigma^{-1}) = \phi_\sigma(\xi + \xi'\sigma^{-1})$. Then we have

$$\begin{aligned}&g(\phi_1(\xi + \xi'\sigma^{-1}), \phi_\sigma(\xi + \xi'\sigma^{-1})) \\ &= (\phi_1(\xi g + \xi'\sigma^{-1}g\sigma\sigma^{-1}), \phi_\sigma(\xi g + \xi'\sigma^{-1}g\sigma\sigma^{-1})) \\ &= \begin{cases} (\phi_1(\xi), \varphi_\sigma(\xi'))\begin{pmatrix} \varphi(g) & 0 \\ 0 & \varphi_\sigma(g)\end{pmatrix} & (g \in H), \\ (\phi_1(\xi'\sigma^{-1}g), \phi_\sigma(\xi g\sigma)) \overset{(*)}{=} (\phi_1(\xi), \phi_\sigma(\xi'))\begin{pmatrix} 0 & \varphi(g\sigma) \\ \varphi(\sigma^{-1}g) & 0\end{pmatrix} & (g\sigma \in H).\end{cases}\end{aligned}$$

Thus we get

$$\boxed{\mathrm{Ind}_H^G \varphi \cong \mathrm{ind}_H^G \varphi.} \tag{7.2}$$

7.4. **Tensoring $\alpha : \Delta \cong \mu_2$.** Let $J = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Extending φ to G by 0 outside H, we find

$$\mathrm{Ind}_H^G \varphi \otimes \alpha(g)$$
$$= \begin{cases} \begin{pmatrix} \varphi(g) & 0 \\ 0 & \varphi(\sigma^{-1}g\sigma) \end{pmatrix} = J \begin{pmatrix} \varphi(g) & 0 \\ 0 & \varphi(\sigma^{-1}g\sigma) \end{pmatrix} J^{-1} & (g \in H), \\ -\begin{pmatrix} 0 & \varphi(g\sigma) \\ \varphi(\sigma^{-1}g) & 0 \end{pmatrix} = J \begin{pmatrix} 0 & \varphi(g\sigma) \\ \varphi(\sigma^{-1}g) & 0 \end{pmatrix} J^{-1} & (g\sigma \in H). \end{cases}$$

Thus we get

$$\boxed{(\mathrm{Ind}_H^G \varphi) \otimes \alpha = J(\mathrm{Ind}_H^G \varphi)J^{-1} \xrightarrow[i_\alpha]{\sim} \mathrm{Ind}_H^G \varphi.} \tag{7.3}$$

Thus $Ad(\mathrm{Ind}_H^G) = \{x \in \mathrm{End}_A(\mathrm{Ind}_H^G \varphi))|\mathrm{Tr}(x) = 0\}$ contains i_α as $\mathrm{Tr}(J) = 0$.

7.5. **Characterization of self-twist.** Let $\overline{\varphi} := (\varphi \bmod \mathfrak{m}_A)$. Suppose $\overline{\varphi}_\sigma \neq \overline{\varphi}$. Since $\mathrm{Ind}_H^G \overline{\varphi}(H)$ contains a diagonal matrices with distinct eigenvalues, its normalizer is $\mathrm{Ind}_H^G \overline{\varphi}(G)$. Thus the centralizer $Z(\mathrm{Ind}_H^G \overline{\varphi}) = \mathbb{F}^\times$ (scalar matrices). Since $\mathrm{Ind}_H^G \overline{\varphi}(\sigma)$ interchanges $\overline{\varphi}$ and $\overline{\varphi}_\sigma$, $\mathrm{Ind}_H^G \overline{\varphi}$ is **irreducible**. Since $\mathrm{Aut}(\overline{\rho}) = \mathbb{F}^\times$, i_α for $\overline{\rho}$ is unique up to scalars.

Let $\rho : G \to \mathrm{GL}_2(A)$ be a deformation of $\mathrm{Ind}_H^G \overline{\varphi}$ with $\rho \otimes \alpha \cong \rho$. Write $j\rho j^{-1} = \rho \otimes \alpha$. Since $\alpha^2 = 1$, j^2 is scalar. We may normalize $j \equiv J \mod \mathfrak{m}_A$ as $j \mod \mathfrak{m}_A = zJ$ for a scalar $z \in A^\times$. Thus j has two eigenvalues $\epsilon_\pm$ with $\epsilon_\pm \equiv \pm z \mod \mathfrak{m}_A$. Let $A_\pm$ be $\epsilon_\pm$-eigenspace of j. Since $j\rho|_H = \rho|_H j$, $A_\pm \cong A$ is stable under H. Thus we find a character $\varphi : H \to A^\times$ acting on A_+. Plainly H acts on A_- by φ_σ. This shows $\rho \cong \mathrm{Ind}_H^G \varphi$ as $V(\rho) = A_+ \oplus \rho(\sigma)A_+$.

7.6. **Decomposition of adjoint representation.**

Theorem 7.1. *We have $Ad(\mathrm{Ind}_H^G \varphi) \cong \alpha \oplus \mathrm{Ind}_H^G \varphi^-$ as representation of G.*

Here $\varphi^-(g) = \varphi(g)\varphi_\sigma^{-1}(g) = \varphi(\sigma^{-1}g^{-1}\sigma g)$ and $\mathrm{Ind}_H^G \varphi^-$ is irreducible if $\varphi^- \neq \varphi_\sigma^- = (\varphi^-)^{-1}$ (i.e., φ^- has order ≥ 3).

Proof. On H, $\rho := \mathrm{Ind}_H^G \varphi = \left(\begin{smallmatrix} \varphi & 0 \\ 0 & \varphi_\sigma \end{smallmatrix}\right)$. Therefore

$$Ad(\mathrm{Ind}_H^G \varphi)(h) \left(\begin{smallmatrix} x & y \\ z & -x \end{smallmatrix}\right) = \rho(h) \left(\begin{smallmatrix} x & y \\ z & -x \end{smallmatrix}\right) \rho^{-1}(h) = \begin{pmatrix} x & \varphi^-(h)y \\ (\varphi^-)^{-1}(h)z & -x \end{pmatrix},$$

and

$$Ad(\mathrm{Ind}_H^G \varphi)(\sigma) \left(\begin{smallmatrix} x & y \\ z & -x \end{smallmatrix}\right) = \begin{pmatrix} 0 & \varphi(\sigma^2) \\ 1 & 0 \end{pmatrix} \left(\begin{smallmatrix} x & y \\ z & -x \end{smallmatrix}\right) \begin{pmatrix} 0 & 1 \\ \varphi(\sigma^{-2}) & 0 \end{pmatrix} = \begin{pmatrix} \alpha(\sigma)x & \varphi(\sigma)^2 z \\ \varphi(\sigma)^{-2}y & -\alpha(\sigma)x \end{pmatrix}.$$

Thus α is realized on diagonal matrices, and $\mathrm{Ind}_H^G \varphi^-$ is realized on the anti-diagonal matrices. □

7.7. **Irreducibility of $\mathrm{Ind}_H^G \overline{\varphi}^-$.**

Lemma 7.2. $\mathrm{Ind}_H^G \overline{\varphi}^-$ *is irreducible if and only if $\overline{\varphi}^- \neq \overline{\varphi}_\sigma^- = (\overline{\varphi}^-)^{-1}$ (i.e., $\overline{\varphi}^-$ has order ≥ 3). If $\overline{\varphi}^-$ has order ≤ 2, then $\overline{\varphi}^-$ extends to a character $\overline{\phi} : G \to \mathbb{F}^\times$ and* $\mathrm{Ind}_H^G \varphi^- \cong \overline{\phi} \oplus \overline{\phi}\alpha$.

Proof. Note $\varphi^-(\sigma^2) = \varphi(\sigma^2)\varphi(\sigma^{-1}\sigma^2\sigma)^{-1} = \varphi(1) = 1$. The irreducibility of $\mathrm{Ind}_H^G \overline{\varphi}^-$ under $\overline{\varphi}^- \neq \overline{\varphi}_\sigma^-$ follows from the argument proving irreducibility of $\mathrm{Ind}_H^G \overline{\varphi}$ under $\overline{\varphi} \neq \overline{\varphi}_\sigma$ in §7.5. Suppose $\overline{\varphi}^-$ has order ≤ 2 (so, $\overline{\varphi}^- = \overline{\varphi}_\sigma^-$). Choose a root $\zeta = \pm 1$ of $X^2 - \varphi_\sigma^-(\sigma^2) = X^2 - 1$ in $\mathbb{F}$. Define $\overline{\phi} = \overline{\varphi}_-$ on H and $\overline{\phi}(\sigma h) = \zeta\overline{\varphi}^-(h)$. For $h, h' \in H$,

$$\overline{\phi}(\sigma h \sigma h') = \overline{\phi}(\sigma^2\sigma^{-1}h\sigma h') = \overline{\varphi}^-(\sigma^2))\overline{\varphi}_\sigma^-(h)\overline{\varphi}^-(h') = \zeta^2\overline{\varphi}^-(hh') = \overline{\varphi}^-(\sigma h)\overline{\varphi}^-(\sigma h').$$

Similarly $\overline{\phi}(h\sigma h') = \overline{\phi}(\sigma\sigma^{-1}hch') = \zeta\overline{\varphi}_\sigma(h)\overline{\varphi}(h') = \overline{\phi}(h)\overline{\phi}(\sigma h')$; so, $\overline{\phi}$ is a character. Then $\mathbb{F}[\zeta][G] \otimes_{\mathbb{F}[H]} \mathbb{F}[\zeta](\overline{\varphi}^-) \cong \mathbb{F}[\zeta](\overline{\phi})$ as G-modules by $a \otimes b \mapsto \overline{\phi}(a)b$. □

7.8. **Ordinarity for residual induced representation.** Let $\sigma \in \mathfrak{G}_{\mathbb{Q}}$ induce a non-trivial field automorphism of $K_{/\mathbb{Q}}$. Let $\overline{\rho} := \mathrm{Ind}_K^{\mathbb{Q}} \overline{\varphi} = \mathrm{Ind}_{\mathfrak{G}_K}^{\mathfrak{G}_{\mathbb{Q}}} \overline{\varphi}$ and assume that $p = \mathfrak{p}\mathfrak{p}^\sigma$ in O (fixing the factor $\mathfrak{p}$ so that $\overline{\varphi}$ is unramified at $\mathfrak{p}^\sigma$). Let $\mathfrak{c}$ be the conductor of $\overline{\varphi}$; so, the ray class field $H_{\mathfrak{c}/K}$ of conductor $\mathfrak{c}$ is the smallest ray class field such that $\overline{\varphi}$ factors through $\mathrm{Gal}(H_{\mathfrak{c}}/K)$. Suppose

$$\text{(sp)} \qquad \mathfrak{c} + \mathfrak{c}^\sigma = O.$$

Pick a prime factor $\mathfrak{l}|\mathfrak{c}$. Then $\mathfrak{l} + \mathfrak{l}^\sigma = O$; so, $\mathfrak{l}$ splits in K. In particular, $I_l = I_{\mathfrak{l}} \subset \mathfrak{G}_K$ (for $(l) = \mathfrak{l} \cap \mathbb{Z}$), and $\overline{\varphi}|_{I_{\mathfrak{l}}}$ ramifies while $\overline{\varphi}$ is unramified at $\mathfrak{l}^\sigma$. Thus $\overline{\rho}|_{I_{\mathfrak{l}}} \cong \left(\begin{smallmatrix} \overline{\epsilon}_{\mathfrak{l}} & 0 \\ 0 & \delta_{\mathfrak{l}} \end{smallmatrix}\right)$ with $\overline{\epsilon}_{\mathfrak{l}} = \overline{\varphi}|_{\mathfrak{l}}$ and $\overline{\delta}_{\mathfrak{l}} = \overline{\varphi}_\sigma$ which is unramified.

Suppose $\mathfrak{l}|D$; so, $I_{\mathfrak{l}}$ is of index 2 in I_l. Then $\overline{\varphi}|_{I_{\mathfrak{l}}} = \overline{\varphi}_\sigma|_{I_{\mathfrak{l}}} = \mathbf{1}$. Similarly to §7.7, we find $\mathrm{Ind}_K^{\mathbb{Q}} \overline{\varphi}|_{I_l} = \mathrm{Ind}_{I_{\mathfrak{l}}}^{I_l} \overline{\varphi}|_{I_{\mathfrak{l}}} = \left(\begin{smallmatrix} \overline{\epsilon}_{\mathfrak{l}} & 0 \\ 0 & \delta_{\mathfrak{l}} \end{smallmatrix}\right)$ with $\overline{\epsilon}_{\mathfrak{l}} = \alpha|_{I_l}$ and $\overline{\delta}_{\mathfrak{l}} = \mathbf{1}$. In short, $\overline{\rho}$ satisfies (ord$_l$) for $l \in S := \{l|DN(\mathfrak{c})p\}$.

7.9. **Identity of two deformation functors.** Let χ be the Teichmüller lift of $\det(\overline{\rho})$. For any Galois representation ρ, let $K(\rho)$ be the solitting field $\overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$ of ρ. Let $K(\overline{\rho})^{(p)}/K(\overline{\rho})$ be the maximal p-profinite extension unramified outside p. Put $G = \mathrm{Gal}(K(\overline{\rho})^{(p)}/\mathbb{Q})$ and $H = \mathrm{Gal}(K(\overline{\rho})^{(p)}/K)$. Consider the deformation functor $\mathcal{D}_? : CL_{/B} \to SETS$ for χ and κ. Since any deformation factors through G, we regard $\rho \in \mathcal{D}_?(A)$ is defined over G. Let

$$\mathcal{F}_H(A) = \{\varphi : H \to A^\times | \varphi \bmod \mathfrak{m}_A = \overline{\varphi} \ \text{ unramified outside } \mathfrak{c}\}$$

and $\mathcal{D}_?^{\widehat{\Delta}}(A) = \{\rho \in \mathcal{D}_?(A) | \rho \otimes \alpha \cong \rho, \det \rho = ?\}/\mathrm{GL}_2(A)$. Recall $\Delta = G/H$ and write $\widehat{\Delta} = \{\alpha, \mathbf{1}\}$ for its character group.

Lemma 7.3. *Let $\widehat{\Delta}$ act on $\mathcal{F}$ by $\rho \mapsto \rho \otimes \alpha$. Then $\mathcal{F}_H(A) \ni \varphi \mapsto \mathrm{Ind}_H^G \varphi \in \mathcal{D}(A)^{\widehat{\Delta}}$ induces an isomorphism: $\mathcal{F}_H \cong \mathcal{D}_?^{\widehat{\Delta}}$ of the functors if $\overline{\varphi} \neq \overline{\varphi}_c$.*

Proof. Note $\mathcal{D}_?^{\widehat{\Delta}}(A) = \{\rho \in \mathcal{D}_?(A) | J(\rho \otimes \alpha)J^{-1} \sim \rho\}/(1 + M_2(\mathfrak{m}_A))$ (realizing $\mathcal{D}_?$ under strict equivalence and choosing $\mathrm{Ind}_H^G \varphi$ specified (7.1)) as $J(\overline{\rho} \otimes \alpha)J^{-1} = \overline{\rho}$ (see §7.4). By the characterization in §7.5, we find a character $\varphi : H \to A^\times$ such that $\mathrm{Ind}_H^G \varphi \cong \rho$.

We choose $j \in \mathrm{GL}_2(A)$ with $j \equiv J \mod \mathfrak{m}_A$ as in §7.5. Then $A_+ = A(\varphi)$ for a character $\varphi : H \to A^\times$. Note that $\varphi \bmod \mathfrak{m}_A = \overline{\varphi}$ by the construction in §7.5. By (ord$_l$) for $l \in S$, $\overline{\varphi}_\sigma$ acting on A_- is unramified at $\mathfrak{l}|\mathfrak{c}\mathfrak{p}$. Thus we conclude $\mathcal{F}_H \cong \mathcal{D}_?^{\widehat{\Delta}}$. □

By $\rho \mapsto \rho \otimes \alpha$, $\widehat{\Delta}$ acts on $\mathcal{D}_?$. For the universal representation $\boldsymbol{\rho}_? \in \mathcal{D}_?(R_?)$, therefore, we have an involution $[\alpha] \in \mathrm{Aut}_{B\text{-alg}}(R_?)$ such that $[\alpha] \circ \boldsymbol{\rho}_? \cong \boldsymbol{\rho}_? \otimes \alpha$. Define $R_?^{\pm} := \{x \in R_? | [\alpha](x) = \pm x\}$.

7.10. **Induced Selmer groups.** For a character $\phi : H \to \mathbb{F}^\times$, Let $K^{(\mathfrak{p})}$ be the maximal p-abelian extension of K unramified outside $\mathfrak{p}$. Let $\Gamma_{\mathfrak{p}} = \mathrm{Gal}(K^{(\mathfrak{p})}/K)$ which is a p-profinite abelian group.

Corollary 7.4. *We have a canonical isomorphism $R_\kappa/R_\kappa([\alpha]-1)R_\kappa \cong W[[\Gamma_{\mathfrak{p}}]]$, where $R_\kappa([\alpha]-1)R_\kappa$ is the R_κ-ideal generated by $[\alpha](x) - x$ for all $x \in R_\kappa$.*

If a finite group $\langle\gamma\rangle$ acts on $R \in CL_{/B}$ fixing B, then

$$\boxed{\mathrm{Hom}_{B\text{-alg}}(R, A)^{\langle\gamma\rangle} = \mathrm{Hom}_{B\text{-alg}}(R/R(\gamma-1)R, A).}$$

Indeed, $f \in \mathrm{Hom}_{B\text{-alg}}(R, A)^\gamma$, then $f \circ \gamma = f$; so, $f(R(\gamma-1)R) = 0$. Thus $\mathrm{Hom}_{B\text{-alg}}(R, A)^\gamma \hookrightarrow \mathrm{Hom}_{B\text{-alg}}(R/R(\gamma-1)R, A)$. Surjectivity is plain.

Proof. Since $\mathcal{F}_H = \mathcal{D}_\kappa^{\widehat{\Delta}}$, we find

$$\mathcal{F}_H(A) = \mathrm{Hom}_{\Lambda\text{-alg}}(R_\kappa, A)^{\widehat{\Delta}} = \mathrm{Hom}_{\Lambda\text{-alg}}(R_\kappa/(R_\kappa([\alpha]-1)R_\kappa), A).$$

Thus $\mathcal{F}_H$ is represented by $R_\kappa/(R_\kappa([\alpha]-1)R_\kappa)$.

Let $\varphi_0 : H \to W^\times$ be the Teichmüller lift of $\overline{\varphi}$. Define $\boldsymbol{\varphi} : H \to W[[\Gamma_{\mathfrak{p}}]]^\times$ by $\boldsymbol{\varphi}(h) = \varphi_0(h)h|_{K^{(\mathfrak{p})}} \in W[[\Gamma_{\mathfrak{p}}]]$. We show that $(W[[\Gamma_{\mathfrak{p}}]], \boldsymbol{\varphi})$ is a universal couple for $\mathcal{F}_H$, which implies the identity of the corollary. Pick a deformation $\varphi \in \mathcal{F}_H(A)$. Then $(\iota_A \circ \varphi_0)^{-1}\varphi$ has values in $1 + \mathfrak{m}_A$ unramified outside $\mathfrak{p}$ as the ramification at $l \in S$ different from p is absorbed by that of $\overline{\varphi}$ by the fact that the inertia group at l in H is isomorphihc to the inertia group at l of $\mathrm{Gal}(K(\overline{\varphi})/K)$. Thus $(\iota_A \circ \varphi_0)^{-1}\varphi$ factors through $\Gamma_{\mathfrak{p}}$, and induces a unique W-algebra homomorphism $W[[\Gamma_{\mathfrak{p}}]] \xrightarrow{\phi} A$ with $\varphi = \phi \circ \boldsymbol{\varphi}$. □

7.11. **What is $\Gamma_{\mathfrak{p}}$?**

Proposition 7.5. *If $p > 2$, we have an exact sequence*

$$1 \to (1+p\mathbb{Z}_p)/\varepsilon^{(p-1)\mathbb{Z}_p} \to \Gamma_{\mathfrak{p}} \to Cl_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \to 1,$$

where $\varepsilon = 1$ if K is imaginary, and ε is a fundamental unit of K if K is real. Thus $\Gamma_{\mathfrak{p}}$ is finite if K is real.

Proof. Since $\Gamma_{\mathfrak{p}} = Cl_K(\mathfrak{p}^\infty) \otimes_{\mathbb{Z}} \mathbb{Z}_p$, the exact sequence is the p-primary part of the exact sequence of the class field theory:

$$1 \to O_{\mathfrak{p}}^\times/\overline{O}^\times \to Cl_K(\mathfrak{p}^\infty) \to Cl_K \to 1.$$

Thus tensoring $\mathbb{Z}_p$ over $\mathbb{Z}$, we get the desired exact sequence, since $O_{\mathfrak{p}} \cong \mathbb{Z}_p$ canonically. Note here $\varepsilon^{p-1} \in 1 + p\mathbb{Z}_p = 1 + \mathfrak{p}O_{\mathfrak{p}}$. □

7.12. **Iwasawa theoretic interpretation of** $\mathrm{Sel}(Ad(\mathrm{Ind}_K^{\mathbb{Q}}\varphi))$**.** Pick a deformation $\varphi \in \mathcal{F}_H(A)$. By $Ad(\mathrm{Ind}_K^{\mathbb{Q}}\varphi) = \alpha \oplus \mathrm{Ind}_K^{\mathbb{Q}}\varphi^-$, the cohomology is decomposed accordingly:

$$H^1(G, Ad(\mathrm{Ind}_K^{\mathbb{Q}}\varphi)) = H^1(G,\alpha) \oplus H^1(G, \mathrm{Ind}_K^{\mathbb{Q}}\varphi^-).$$

Since Selmer cocycles are upper triangular over D_p and upper nilpotent over I_p, noting the fact that $\alpha \subset Ad(\mathrm{Ind}_H^G\varphi)$ is realized on diagonal matrices, and $\mathrm{Ind}_H^G\varphi^-$ is realized on anti-diagonal matrices, the Selmer condition is compatible with the above factorization; so, we have

Theorem 7.6. *We have* $\mathrm{Sel}(Ad(\mathrm{Ind}_H^G\varphi)) = \mathrm{Sel}(\alpha) \oplus \mathrm{Sel}(\mathrm{Ind}_H^G\varphi^-))$*, where* $\mathrm{Sel}(\alpha)$ *is made of classes in $H^1(G,\alpha)$ unramified everywhere and* $\mathrm{Sel}(\mathrm{Ind}_H^G\varphi^-)$ *is isomorphic to the subgroup* $\mathrm{Sel}(\varphi^-)$ *of $H^1(H,\varphi^-)$ made of classes unramified outside $\mathfrak{p}$ and vanishes over $D_{\mathfrak{p}^\sigma}$. In particular,*

$$\mathrm{Sel}(\alpha) = \mathrm{Hom}(Cl_K, A^\vee) = \mathrm{Hom}(Cl_K \otimes_{\mathbb{Z}} A, \mathbb{Q}_p/\mathbb{Z}_p).$$

Proof. Pick a Selmer cocycle $u : G \to Ad(\rho_0)^*$. Projecting down to α, it has diagonal form; so, the projection u_α restricted to D_p is unramified. Therefore u_α factors through Cl_K. Starting with an unramified homomorphism $u : Cl_K \to A^\vee$ and regard it as having values in diagonal matrices in $Ad(\rho_0)^*$, its class falls in $\mathrm{Sel}(Ad(\rho_0))$.

Similarly, the projection u^{Ind} of u to the factor $\mathrm{Ind}_H^G\varphi^-$ is anti-diagonal of the form $\left(\begin{smallmatrix} 0 & u^+ \\ u^- & 0\end{smallmatrix}\right)$. Noting $H^j(\Delta, ((\mathrm{Ind}_H^G\varphi^-)^*)^H) = 0$ $(j = 1, 2)$, by inflation-restriction sequence,

$$H^1(G, (\mathrm{Ind}_H^G\varphi^-)^*) \cong (H^1(H,(\varphi^-)^*) \oplus H^1(H,(\varphi^-_\sigma)^*))^\Delta.$$

So $u^-(\sigma^{-1}g\sigma) = u^+(g)$ as $\sigma \in \Delta$ interchanges $H^1(H,(\varphi^-)^*)$ and $H^1(H,(\varphi^-_\sigma)^*)$. Moreover u^+ is unramified outside $\mathfrak{p}$ as an element of $H^1(H,(\varphi^-)^*)$. Since $u^-|_{D_{\mathfrak{p}}} = 0$, u^+ vanishes on $D_{\mathfrak{p}^\sigma}$ by $u^-(\sigma^{-1}g\sigma) = u^+(g)$. □

7.13. **Anti-cyclotomic p-abelian extension.** Regard $\boldsymbol{\varphi} : G \to W[[\Gamma_{\mathfrak{p}}]]^\times$. Define $K^-_{/K}$ by the maximal p-abelian anticyclotomic extension unramified outside p (so, $\sigma\gamma\sigma^{-1} = \gamma^{-1}$). The the fixed subfield of $K(\overline{\rho})^{(p)}$ by $\mathrm{Ker}(\boldsymbol{\varphi}^-)$ is given by $K(\varphi^-)K^-$. So $\Gamma^- = \mathrm{Gal}(K^-/K)$ is the maximal p-abelian quotient of $\mathrm{Im}(\boldsymbol{\varphi}^-)$; i.e., $\mathrm{Gal}(K^-/K) \cong \Gamma^- \times \mathrm{Gal}(K(\overline{\varphi}_0^-)/K)$. Note that $\boldsymbol{\varphi}^-(h) = \boldsymbol{\varphi}(h)\boldsymbol{\varphi}(\sigma^{-1}h\sigma)^{-1} \in \Gamma_{\mathfrak{p}}$ if $h \in \Gamma^-$. Thus we have an exotic homomorphism $\Gamma^- \to \Gamma_{\mathfrak{p}}$. We have an exact sequence for $\widehat{Cl}_K := Cl_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$:

$$1 \to ((1+pO_p)/\varepsilon^{(p-1)\mathbb{Z}_p})^{\sigma=-1} \to \Gamma^- \to \widehat{Cl}_K \to 1,$$

which is the "$-$"-eigenspaces of the action of σ on the exact sequence with $\widehat{Cl}_K(p^\infty) := Cl_K(p^\infty) \otimes_{\mathbb{Z}} \mathbb{Z}_p$:

$$1 \to (1+pO_p)/\varepsilon^{(p-1)\mathbb{Z}_p} \to \widehat{Cl}_K(p^\infty) \to \widehat{Cl}_K \to 1.$$

Therefore the above homomorphism induces an isomorphism $\Gamma^- \cong \Gamma_{\mathfrak{p}}$, and in this way, we identify $W[[\Gamma^-]]$ with $W[[\Gamma_{\mathfrak{p}}]]$.

7.14. **Iwasawa modules.** Let L/K^- (resp. $L'/K(\varphi^-)$) be the maximal p-abelian extension unramified outside $\mathfrak{p}$ totally split at $\mathfrak{p}^\sigma$ (so $L' \subset L$). Put $\mathcal{Y} := \mathrm{Gal}(L/K^-)$ and $\Delta := \mathrm{Gal}(K(\varphi_0^-)/K)$. By conjugation, $\Delta \times \Gamma_- = \mathrm{Gal}(K^-/K)$ acts on $\mathcal{Y}$; so, we put $\mathcal{Y}(\varphi_0^-) = \mathcal{Y} \otimes_{\mathbb{Z}_p[\mathrm{Gal}(K(\varphi^-)/K]} \varphi_0^-$ (the maximal quotient of $\mathcal{Y}$ on which $\Delta \subset \mathrm{Gal}(K^-/K)$ acts by φ_0^-). Then $\mathcal{Y}(\varphi_0)$ is a module over $W[[\Gamma_-]]$ (an Iwasawa module). The Galois group $\mathrm{Gal}(L'/K(\varphi^-))$ (resp. $\mathrm{Gal}(L'/K(\varphi^-)(\varphi_0^-) = \mathrm{Gal}(L'/K(\varphi^-) \otimes_{\mathbb{Z}_p[\Delta]} \varphi_0^-)$ is a quotient of $\mathcal{Y}$ (resp. $\mathcal{Y}(\varphi_0)$), and if $W[[\Gamma^-]] \twoheadrightarrow A$, $\mathrm{Gal}(L'/K(\varphi^-)(\varphi_0^-) = \mathcal{Y}(\varphi_0^-) \otimes_{W[[\Gamma^-]],\varphi^-} A$.

We have an inflation-restriction exact sequence:

$$H^1(K(\varphi^-)/K, (\varphi^-)^*) \hookrightarrow H^1(H, (\varphi^-)^*) \to \mathrm{Hom}_{\mathrm{Gal}(K(\varphi^-)/K)}(\mathrm{Gal}(K(\overline{\rho})^{(p)}/K(\varphi^-)), (\varphi^-)^*) \to H^2(K(\varphi^-)/K, (\varphi^-)^*).$$

Lemma 7.7. *Assume that* $\overline{\varphi}^- \neq 1$. *If* Γ^- *is cyclic, we have* $H^j(K(\varphi^-)/K, (\varphi^-)^*) = 0$ *for* $j = 1, 2$.

Proof. For a finite cyclic group C generated by γ

$$H^1(C, M) = \mathrm{Ker}(\mathrm{Tr})/\mathrm{Im}(\gamma - 1),\ H^2(C, M) = \mathrm{Ker}(\gamma - 1)/\mathrm{Im}(\mathrm{Tr}),$$

where $\mathrm{Tr}(x) = \sum_{c \in C} cx$ and $(\gamma - 1)(x) = \gamma x - x$ for $x \in M$. If C is infinite with M discrete, $H^q(C, M) = \varinjlim_{C' \subset C} H^q(C/C', M^{C'})$. Thus if $\overline{\varphi}^-(\gamma) \neq 1$ for a generator of Γ^-, we find

$$H^j(K(\varphi^-)/K, (\varphi^-)^*) = 0$$

as $\gamma - 1 : (\varphi^-)^* \to (\varphi^-)^*$ is a bijection. □

By Lemma 7.7, from inflation-restriction sequence, we get

$$H^1(H, (\varphi^-)^*) \cong \mathrm{Hom}_{\mathrm{Gal}(K(\varphi^-)/K)}(\mathrm{Gal}(K(\overline{\rho})^{(p)}/K(\varphi^-)), (\varphi^-)^*).$$

Then Selmer cocycles factor through $\mathcal{Y}$; so, for $\mathcal{G} := \mathrm{Gal}(K(\varphi^-)/K)$,

$$\mathrm{Sel}(\varphi^-) = \mathrm{Hom}_{\mathcal{G}}(\mathcal{Y}, (\varphi^-)^*) \cong \mathrm{Hom}_{W[[\Gamma_-]]}(\mathcal{Y}(\varphi_0^-), (\varphi^-)^*) \cong \mathrm{Hom}_W(\mathcal{Y}(\varphi_0^-) \otimes_{W[[\Gamma_-]],\varphi^-} A, \mathbb{Q}_p/\mathbb{Z}_p).$$

7.15. **Cyclicity of Iwasawa module $\mathcal{Y}(\varphi_0^-)$.** Since $R_\kappa/R_\kappa([\alpha]-1)R_\kappa \cong W[[\Gamma_\mathfrak{p}]] = W[[\Gamma^-]]$, we write this morphism as $\theta : R_\kappa \to W[[\Gamma^-]]$.

Theorem 7.8. *If* Γ^- *is cyclic, we have*

$$\mathrm{Sel}(\varphi^-) \cong \mathrm{Hom}_{W[[\Gamma_-]]}(\mathcal{Y}(\varphi_0^-), (\varphi^-)^*),\ \Omega_{R_\kappa/\Lambda} \otimes_{R_\kappa,\lambda} W[[\Gamma^-]] \cong \mathcal{Y}(\varphi_0^-)$$

as $W[[\Gamma^-]]$*-modules.*

This follows from Lemma 7.7.

Since $p \nmid [K(\varphi_0^-) : K]$, the p-Hilbert class field H/K and $K(\varphi_0^-)$ is linearly disjoint over K; so, we have $[H : K] = [HF, F]$; so, $p \nmid h_F$ implies $p \nmid h_K$. Thus combining the above theorem with the cyclicity result in Theorem 6.5, we get

Corollary 7.9. *If* $p \nmid h_F$, $\mathcal{Y}(\varphi_0^-)$ *is a cyclic module over* $W[[\Gamma^-]]$ *if* $\overline{\varphi}_0 \neq 1$.

8. Selmer group of Artin representation

Assuming that $\overline{\rho}$ comes from an Artin representation $\rho : \mathfrak{G}_\mathbb{Q} \to \mathrm{GL}_2(W)$, we explore a way to describe the size of its adjoint Selmer group in terms of a global unit of the splitting field F. Let $G = \mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{Im}(Ad(\overline{\rho}))$. Assume $p \nmid |G|$ and irreducibility of $\overline{\rho}$ throughout this section. Then $G \cong \mathrm{Im}(Ad(\rho)) = \mathrm{Im}(Ad(\overline{\rho}))$. We write $\mathbb{F}$ for the minimal field of rationality of $Ad(\overline{\rho})$. Noting that $Ad(\overline{\rho})$ factors through $\mathrm{PGL}_2(\mathbb{F})$, $\mathbb{F}$ is the minimal subfield of $\overline{\mathbb{F}}_p$ with $\mathrm{Im}(Ad(\rho)) \subset \mathrm{PGL}_2(\mathbb{F})$. Then we take W to be the unramified extension of $\mathbb{Z}_p$ with $W/\mathfrak{m}_W = \mathbb{F}$; so, $W = W(\mathbb{F})$ (the ring of Witt vectors with coefficients in $\mathbb{F}$). We write O for the integer ring F. Fix a prime $\mathfrak{p}|p$ in O. We write $D \subset G$ for the decomposition group of $\mathfrak{p}$ and choose basis so that $\rho|_D = \left(\begin{smallmatrix}\epsilon & 0\\ 0 & \delta\end{smallmatrix}\right)$ with δ unramified.

8.1. **Classification of Artin representations.** Identify G with the subgroup $\mathrm{Im}(Ad(\overline{\rho}))$ of $\mathrm{PGL}_2(\mathbb{F})$. Dickson (in [LGF, §260]; see also [W2, §3]) gave a classification of $G \subset \mathrm{PGL}_2(\mathbb{F})$:

Case G: If $p||G|$, G is conjugate to $\mathrm{PGL}_2(k)$ or $\mathrm{PSL}_2(k)$ for a subfield $k \subset \mathbb{F}$ as long as $p > 3$ (when $p = 3$, G can be A_5). Suppose $p \nmid |G|$ (so, $p \geq 5$). Then G is given as follows.

Case C: G is cyclic ($\Rightarrow \mathrm{Im}(\overline{\rho})$ is abelian).

Case D: G is isomorphic to a dihedral group D_a of order $2a$ (so, $\overline{\rho} = \mathrm{Ind}_K^{\mathbb{Q}} \overline{\varphi}$ for a quadratic field), and $\mathbb{F} = \mathbb{F}_p[\overline{\varphi}^-]$ (the field generated by the values of $\overline{\varphi}^-$)

Case E: G is either isomorphic to A_4, S_4 ($\mathbb{F} = \mathbb{F}_p$ and $W = \mathbb{Z}_p$), or A_5 ($\mathbb{F} \cong \mathbb{Z}_p[\sqrt{5}]/\mathfrak{p}$ for a prime $\mathfrak{p}|p$ by the character table of A_5; so, $\mathbb{F} = \mathbb{F}_p$ or $\mathbb{F}_{p^2}$). These groups does not have quotient isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z}$ for $p \geq 5$ (Serre's book on linear group representation: §5.7-8 and §18.6).

In this section, we study Case E but until §8.8 (except for §8.2), we do not suppose that we are in case E.

8.2. $Ad(\overline{\rho})$ **is absolutely irreducible in Case E.** If $Ad(\overline{\rho})$ is reducible, it contain a 1-dimensional subspace or quotient stable under G-action. We regard $\overline{\rho}$ has values in the algebraic closure $\overline{\mathbb{F}}_p$. Since $Ad(\overline{\rho})$ is self dual, the dual of the quotient is a subspace; so, always it contains subspace of dimension 1 spanned by $0 \neq i \in \mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{\rho})$ with $\mathrm{Tr}(i) = 0$. Thus G acts on i by a character α: $\overline{\rho}(g) \circ i \circ \overline{\rho}(g)^{-1} = \alpha(g)i$ ($\Leftrightarrow \overline{\rho} \circ i = i \circ (\overline{\rho} \otimes \alpha)$). This implies that i gives an isomorphism $\overline{\rho} \cong \overline{\rho} \otimes \alpha$ as $\overline{\rho}$ is irreducible. Taking determinant of this identity, $\det(\overline{\rho}) = \det(\overline{\rho})\alpha^2$; so, $\alpha^2 = 1$. If $\alpha = 1$, i commutes with absolutley irreducible $\overline{\rho}$; so, by Schur's lemma, i is a non-zero scalar multiplication, contradicting $\mathrm{Tr}(i) = 0$ (by $p > 2$). Thus α is quadratic, and as seen in §6.5, $\overline{\rho} = \mathrm{Ind}_K^{\mathbb{Q}} \varphi$ for a quadratic extension $K/\mathbb{Q}$ fixed by $\mathrm{Ker}(\alpha)$. This means we are in Case D or case C. Thus $Ad(\overline{\rho})$ is absolutely irreducible in Case E.

8.3. **Lifting $\overline{\rho}$.** Since $p \nmid |G|$, $\mathcal{G} := \mathrm{Gal}(F(\overline{\rho})/\mathbb{Q}) \cong \mathrm{Im}(\overline{\rho})$ fits into an exact sequence for the center Z (scalar matrices) of GL_2:

$$1 \to Z(\mathbb{F}) \cap \mathcal{G} \to \mathcal{G} \to G \to 1.$$

Since $|Z(\mathbb{F})| = |\mathbb{F}^\times|$ is prime to p, we find $p \nmid |\mathcal{G}|$. Under this circumstance, the set of irreducible representations of $\mathcal{G}$ with coefficients in $\mathbb{F}$ is in bijection to representations with coefficients in W irreducible over $\mathrm{Frac}(W)$ by reduction modulo $\mathfrak{m}_W$ (cf. [MFG,Corollary 2.7].

Writing $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(W)$ (factoring through $\mathcal{G}$) for the lifted representation, we have $\mathrm{Im}(Ad(\rho)) = \mathrm{Im}(Ad(\overline{\rho})) \cong G$. Recall the splitting field F of $Ad(\overline{\rho})$; so, $G = \mathrm{Gal}(F/\mathbb{Q})$. In Case E, G has no abelian cyclic quotient of order $p-1$; so, $\mu_p(F) = \{1\}$.

8.4. **Minkowski unit.** Let $O_f^\times := O^\times/\mu_p(F)$. We have shown in §5.16 that $(O_f^\times \otimes_{\mathbb{Z}} \mathbb{F}) \oplus \mathbb{F}\mathbf{1} \cong \mathrm{Ind}_C^G \mathbf{1} \cong \mathbb{F}[G/C]$ by (the proof of) Dirichlet's unit theorem. Here C is the subgroup of G generated by the fixed complex conjugation c. By the same argument, we find $(O_f^\times \otimes_{\mathbb{Z}} \mathfrak{m}_W^n/\mathfrak{m}_W^{n+1}) \oplus \mathfrak{m}_W^n/\mathfrak{m}_W^{n+1}\mathbf{1} \cong \mathfrak{m}_W^n/\mathfrak{m}^{n+1}[G/C]$; so, $(O_f^\times \otimes_{\mathbb{Z}} W/\mathfrak{m}_W^n) \oplus W/\mathfrak{m}_W^n\mathbf{1} \cong W/\mathfrak{m}_W^n[G/C]$. Passing to the (projective) limit, we get

$$(O_f^\times \otimes_{\mathbb{Z}} W) \oplus W\mathbf{1} \cong W[G/C]$$

as G-module. Take $W = \mathbb{Z}_p$. Since $\mathbb{Z}_p[G/C]/\mathbb{Z}_p\mathbf{1}$ is a cyclic $\mathbb{Z}_p[G]$-module, there is a generator $\varepsilon \otimes 1 \in O_f^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$ ($\varepsilon \in O_f^\times$) over $\mathbb{Z}_p[G]$. This unit ε is called a **Minkowski unit**, and we fix one. By our choice, $\{\varepsilon^\sigma|\sigma \in G/C\}$ has a unique relation $\prod_{\sigma \in G/C} \varepsilon^\sigma = 1$ and generates a subgroup of $O_f^\times$ of finite index prime to p. For each general $W_{/\mathbb{Z}_p}$, $\varepsilon \otimes 1$ is a generator of $O_f^\times \otimes_{\mathbb{Z}} W$ over $W[G]$.

8.5. **Ray class groups.** Recall $Cl_F(p^\infty) = \varprojlim_n Cl_F(p^n)$, and we have an exact sequence

$$O^\times \to (O/p^nO)^\times \to Cl_F(p^n) \to Cl_F \to 1.$$

Passing to the limit, we get

$$1 \to \overline{O^\times} \to O_p^\times \to Cl_F(p^\infty) \to Cl_F \to 1,$$

where $O_p = \varprojlim_n O/p^nO$ and $\overline{O^\times} = \varprojlim_n \mathrm{Im}(O^\times \to (O/p^nO)^\times)$.

Adding "$\widehat{\ }$", we denote the p-profinite part of each groups in the sequence, getting another exact sequence

$$1 \to \widehat{O^\times} \to \widehat{O_p^\times} \to \widehat{Cl}_F(p^\infty) \to \widehat{Cl}_F \to 1,$$

where we have written simply $\widehat{O^\times}$ for $\widehat{\overline{O^\times}}$. Except for Case E, we could have p-torsion in $\widehat{O^\times}$ (i.e., $\mu_p(F) \neq 1$) and in $\widehat{O_p^\times}$ (i.e., $\epsilon/\delta = \omega$ is the Teichmüller character).

8.6. **Selmer group revisited.** We often write simply Ad for $Ad(\rho)$. Let $k^{(p)}$ be the maximal p-profinite extension of a number field k unramified outside p and put $\mathfrak{G} = \mathrm{Gal}(F^{(p)}/\mathbb{Q})$, $\mathfrak{H} = \mathrm{Gal}(F^{(p)}/F)$, $\mathfrak{G}' = \mathrm{Gal}(F(\overline{\rho})^{(p)}/\mathbb{Q})$, $\mathfrak{H}' = \mathrm{Gal}(F(\overline{\rho})^{(p)}/F)$. Recall

$$\mathrm{Sel}(Ad(\rho)) := \mathrm{Ker}(H^1(\mathfrak{G}', Ad^*) \to \frac{H^1(\mathbb{Q}_l, Ad^*)}{F_-^+(Ad^*)} \times \prod_{l\in S} H^1(I_l, Ad^*),$$

where $F_-^+Ad^*$ is a subgroup of $H^1(\mathbb{Q}_l, Ad^*)$ made of classes of cocycles upper triangular over the p-decomposition group and upper nilpotent over the p-inertia group.

Lemma 8.1. *We have a canonical inclusion*

$$\mathrm{Sel}(Ad(\rho)) \subset \mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{Cl}_F(p^\infty), Ad(\rho)^*).$$

Proof. For a topological group X, write X^{ab} for the maximal continuous abelian quotient of X. Let $u : \mathfrak{G}' \to Ad^*$ be a Selmer cocycle. Let $u' = u|_{\mathfrak{H}'} : \mathfrak{H}' \to Ad^*$, which is a homomorphism. By inflation-restriction, through $u \mapsto u'$,

$$\mathrm{Sel}(Ad(\rho)) \hookrightarrow H^1(\mathfrak{G}', Ad^*) \cong \mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathfrak{H}'^{ab}, Ad^*),$$

since $H^q(G, Ad(\rho)^*) = 0$ for $q > 0$ by $p \nmid [F : \mathbb{Q}]$.

Since the ramification of a prime $\mathfrak{l}$ of O outside p is concentrated in $\mathrm{Gal}(F(\overline{\rho})/F)$, the inertia group $I_{\mathfrak{l}}$ injects into $\mathrm{Gal}(F(\overline{\rho})/F)$; so, $\boxed{I_{\mathfrak{l}} \text{ is finite of order prime to } p.}$ This implies $u'(I_{\mathfrak{l}}) = 0$ as Ad^* is p-torsion. Thus u' factors through $\mathfrak{H}'^{ab} \twoheadrightarrow \mathfrak{H}^{ab}$ as $\mathfrak{H}$ is the Galois group over F of the maximal p-profinite extension $F^{(p)}$ of F unramified outside p. By class field theory, we know $\mathfrak{H}^{ab} \cong \widehat{Cl}_F(p^\infty)$. □

8.7. **Galois module structure of p-decomposition groups.** Essential part of $\widehat{Cl}_F(p^\infty)$ comes from $\widehat{O}_p^\times$ which is the product of p-inertia subgroup of $\mathfrak{H}^{ab}$; so, we study decomposition group in $\mathfrak{H}^{ab}$ as D-modules. Recall the fixed prime factor $\mathfrak{p}|p$ in O with its decomposition subgroup $D \subset G$. Write simply $M_{\mathfrak{p}} := F_{\mathfrak{p}}^\times \otimes_{\mathbb{Z}} W$ and $U_{\mathfrak{p}} := \widehat{O_{\mathfrak{p}}^\times} \otimes_{\mathbb{Z}_p} W = O_{\mathfrak{p}}^\times \otimes_{\mathbb{Z}} W$. Then for each character $\xi : D \to W^\times$, $M_{\mathfrak{p}}$ contains as a direct factor the ξ-eigenspace $M_{\mathfrak{p}}[\xi] = 1_\xi M_{\mathfrak{p}}$ for $1_\xi = |D|^{-1}\sum_{g\in D}\xi^{-1}(g)g \in W[D]$. Then

- A canonical exact sequence $U_{\mathfrak{p}}[\mathbf{1}] \hookrightarrow M_{\mathfrak{p}}[\mathbf{1}] \xrightarrow[\twoheadrightarrow]{\mathrm{ord}_{\mathfrak{p}}} W$ induced by the valuation $\mathrm{ord}_{\mathfrak{p}} : F_{\mathfrak{p}}^\times \twoheadrightarrow \mathbb{Z}$ at $\mathfrak{p}$, and $U_{\mathfrak{p}}[\mathbf{1}] \cong W$ as $\mu_p(F_{\mathfrak{p}})[\mathbf{1}] = 0$.
- $M_{\mathfrak{p}}[\xi]$ is a direct summand of $U_{\mathfrak{p}}$ if $\xi \neq \mathbf{1}$. Since all other prime factor of p is of the form $\sigma(\mathfrak{p})$ for $\sigma \in G/D$, we have $M_p := F_p^\times \otimes_{\mathbb{Z}} W \cong \mathrm{Ind}_D^G M_{\mathfrak{p}}$ as G-modules (for $F_p = F \otimes_{\mathbb{Q}} \mathbb{Q}_p$). Put $U_p := \widehat{O_p^\times} \otimes_{\mathbb{Z}_p} W = O_p^\times \otimes_{\mathbb{Z}} W$.

8.8. **Structure of $M_p[Ad]$ as a G-module in Case E..** Hereafter we suppose to be in Case E (so, M_p is p-torsion-free). For the idempotent 1_{Ad} of $W[G]$ corresponding to $Ad(\rho)$ and a W-free $W[G]$-module X, we consider the Ad-isotypical component $X[Ad] = 1_{Ad}X$. Since $M_p = \mathrm{Ind}_D^G M_{\mathfrak{p}}$, by Shapiro's lemma, we have for $\xi = \epsilon\delta^{-1}$

$$\mathrm{Hom}_G(M_p, Ad^*) = \mathrm{Hom}_D(M_{\mathfrak{p}}, Ad^*|_D) = \mathrm{Hom}_D(M_{\mathfrak{p}}, \xi^* \oplus \mathbf{1}^* \oplus (\xi^{-1})^*).$$

Since $M_{\mathfrak{p}}[\xi^{\pm 1}] = U_{\mathfrak{p}}[\xi^{\pm 1}]$ (by $\xi \neq \mathbf{1}$),

$$(\mathrm{Ind}_D^G U_{\mathfrak{p}}[\xi] \oplus \mathrm{Ind}_D^G U_{\mathfrak{p}}[\mathbf{1}] \oplus \mathrm{Ind}_D^G U_{\mathfrak{p}}[\xi^{-1}])[Ad] = Ad_\xi \oplus Ad_{\mathbf{1}} \oplus Ad_{\xi^{-1}},$$

where $Ad_? = \mathrm{Ind}_D^G ?[Ad]$. This fits into the following exact sequence of G-modules:

$$0 \to \overbrace{Ad_\xi \oplus Ad_{\mathbf{1}} \oplus Ad_{\xi^{-1}}}^{\text{inertia part}} \to M_p[Ad] \xrightarrow{\prod_{\sigma\in G/D} \mathrm{ord}_{\sigma(\mathfrak{p})}} \overbrace{(\mathrm{Ind}_D^G W\mathbf{1})[Ad]}^{\text{Frobenius part}} \to 0.$$

8.9. **Selmer group as a subgroup of $\mathrm{Hom}_G(\widehat{Cl}_F(p^\infty), Ad(\rho)^*)$.** Let $Cl_F^{(p)}$ be the subgroup of Cl_F generated by $\sigma(\mathfrak{p})$ for $\sigma \in G$. We the define $C_F := Cl_F/Cl_F^{(p)}$.

Theorem 8.2. *Assume that we are in Case E. Then we have an exact sequence*

$$\mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{C}_F, Ad(\rho)^*) \hookrightarrow \mathrm{Sel}(Ad(\rho))$$
$$\twoheadrightarrow \mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{Cl}_F^{(p)}, Ad(\rho)^*) \oplus \mathrm{Hom}_{W[D]}(U_{\mathfrak{p}}[\epsilon\delta^{-1}]/\overline{\langle\varepsilon_{\epsilon\delta^{-1}}\rangle}, W^\vee),$$

where ε is the fixed Minkowski unit with $\widehat{O}^\times = \mathbb{Z}_p[G]\varepsilon$, $\varepsilon_{\epsilon\delta^{-1}}$ is the projection of ε in the direct summand $U_\mathfrak{p}[\epsilon_\mathfrak{p}\delta_\mathfrak{p}^{-1}]$ under $O^\times \to U_p \twoheadrightarrow U_\mathfrak{p}[\epsilon\delta^{-1}]$, and $\overline{\langle\varepsilon_{\epsilon\delta^{-1}}\rangle}$ is the p-adic closure of the subgroup $\varepsilon_{\epsilon\delta^{-1}}^{\mathbb{Z}}$ generated by $\varepsilon_{\epsilon\delta^{-1}}$.

Corollary 8.3. *Suppose we are in Case E. Then we have*

$$|\mathrm{Sel}(Ad(\rho))| = |\widehat{Cl}_F \otimes_{\mathbb{Z}_p[G]} Ad(\rho)||(U_\mathfrak{p}[\epsilon\delta^{-1}]/\overline{\langle\varepsilon_{\epsilon\delta^{-1}}\rangle})|,$$

which is finite.

We start the proof of Theorem 8.2 which ends in §8.14. After finishing the proof of the theorem, we prove the corollary.

8.10. **Proof of** $\mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{C}_F, Ad^*) \hookrightarrow \mathrm{Sel}(Ad(\rho))$**.** Elements in $\mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{C}_F, Ad^*)$ are everywhere unramified and trivial at p; so, they gives rise to a subgroup of $\mathrm{Sel}(Ad(\rho))$ of classes everywhere unramified and trivial at p. Indeed, by $H^1(\mathfrak{G}, Ad^*) \cong \mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathfrak{H}^{ab}, Ad^*)$, any $u \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{C}_F, Ad^*)$ extends uniquely the cocycle $u : \mathfrak{G} \to Ad^*$ unramified everywhere over $\mathfrak{H}$. Since the inertia group $I_l \subset G$ of any prime $l \in S$ has order prime to p, $u|_{I_l} = 0$, and hence $[u] \in \mathrm{Sel}(Ad(\rho))$.

Let $D_\mathfrak{p}$ be the decomposition group at $\mathfrak{p}$ of $\mathfrak{H}^{ab}$ with inertia subgroup $I_\mathfrak{p}$. Then

$$\prod_{\sigma\in G/D} \sigma D_\mathfrak{p}\sigma^{-1} \cong M_p \quad\text{and}\quad \prod_{\sigma\in G/D} \sigma I_\mathfrak{p}\sigma^{-1} \cong U_p.$$

Elements of $\mathrm{Sel}(Ad(\rho))$ modulo $\mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{C}_F, Ad^*)$ is determined by its restriction to M_p as they are unramified outside p as they factor through $\widehat{Cl}_F(p^\infty)$ and $p \nmid |I_l|$.

8.11. **Restriction to** $D_\mathfrak{p}$**.** Recall $\xi = \epsilon\delta^{-1}$. We study

$$u_\mathfrak{p} = u|_{D_\mathfrak{p}} \in \mathrm{Hom}_{\mathbb{Z}_p[D]}(D_\mathfrak{p}, Ad^*) = \mathrm{Hom}_{\mathbb{Z}_p[D]}(M_\mathfrak{p}, Ad^*)$$

for cocycle $u : \mathfrak{G} \to Ad^*$. Since $Ad = Ad[\xi] \oplus Ad[\mathbf{1}] \oplus Ad[\xi^{-1}]$, we have a decomposition:

$$\mathrm{Hom}_{\mathbb{Z}_p[D]}(M_\mathfrak{p}, Ad^*) = \overbrace{\mathrm{Hom}_{\mathbb{Z}_p[D]}(U_\mathfrak{p}[\xi], Ad[\xi]^*)}^{\text{upper nilpotent}} \oplus \overbrace{\mathrm{Hom}_{\mathbb{Z}_p[D]}(M_\mathfrak{p}[\mathbf{1}], Ad[\mathbf{1}]^*)}^{\text{diagonal}} \oplus \overbrace{\mathrm{Hom}_{\mathbb{Z}_p[D]}(U_\mathfrak{p}[\xi^{-1}], Ad[\xi^{-1}]^*)}^{\text{lower nilpotent}}.$$

Thus a Selmer cocycle u projects down to the first two factors:

$$\overbrace{\mathrm{Hom}_{\mathbb{Z}_p[D]}(U_\mathfrak{p}[\xi], Ad[\xi]^*)}^{\text{upper nilpotent}} \oplus \overbrace{\mathrm{Hom}_{\mathbb{Z}_p[D]}(M_\mathfrak{p}[\mathbf{1}], Ad[\mathbf{1}]^*)}^{\text{diagonal}}.$$

Write $u_\mathfrak{p}^+$ (resp. $u_\mathfrak{p}^0$) for the upper nilpotent projection (resp. the diagonal projection) of u.

8.12. **Inertia part** u_+**.** We have $u_\mathfrak{p}^+ : I_\mathfrak{p}[\xi] = U_\mathfrak{p}[\xi] \to Ad[\xi]^*$ and $u_{\sigma(\mathfrak{p})}^+ : U_{\sigma(\mathfrak{p})}[\xi_\sigma] \to Ad[\xi_\sigma]^*$ for $D_{\sigma(\mathfrak{p})} = \sigma D\sigma^{-1} \xrightarrow{\xi_\sigma} A^\times$ given by $\xi_\sigma(h) = \xi(\sigma^{-1}h\sigma)$. Note $Ad[\xi_\sigma]^* = \sigma(Ad[\xi]^*)$ and $U_{\sigma(\mathfrak{p})}[\xi_\sigma] = \sigma(U_\mathfrak{p}[\xi])$ and $u_{\sigma(\mathfrak{p})}(h) = u_\mathfrak{p}(\sigma^{-1}h\sigma)$. Since u is a cocycle over $\mathfrak{G}$, out of each restriction $u_{\sigma(\mathfrak{p})}^+$, we create the map

$$u_+ := (u_{\sigma(\mathfrak{p})}^+)_\sigma : \prod_{\sigma\in G/D} \sigma(U_\mathfrak{p}[\xi]) \to \prod_{\sigma\in G/D} \sigma(Ad[\xi])^*.$$

Note $\prod_\sigma \sigma(U_\mathfrak{p}[\xi]) = \mathrm{Ind}_D^G U_\mathfrak{p}[\xi]$ and $\prod_\sigma \sigma(Ad[\xi])^* \cong \mathrm{Ind}_D^G Ad[\xi]^*$ as G-modules. Since u is a cocycle defined over $\mathfrak{G}$, we get a G-equivariant commutative diagram:

$$\begin{array}{ccc} \mathrm{Ind}_D^G U_\mathfrak{p}[\xi] & \xrightarrow{u_+} & \mathrm{Ind}_D^G Ad[\xi]^* \\ \big\downarrow & & \big\downarrow \\ U_p[Ad] & \xrightarrow{u|_{U_p}} & Ad^*. \end{array}$$

8.13. **Determination of inertia part $u|_{U_p}$.** By the above argument, the restriction $u|_{U_p}$ falls into $\mathrm{Hom}_{\mathbb{Z}_p[G]}(Ad_\xi, Ad^*)$ induced from u_+. Though $U_p[Ad] \cong Ad^m$ for $m = 3$ if ξ has order 3 and $m = 2$ if ξ has order 2, as Shapiro's isomorphism

$$S : \mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathrm{Ind}_D^G U_{\mathfrak{p}}[\xi], Ad) \cong \mathrm{Hom}_D(\xi, \xi_+ \oplus \mathbf{1} \oplus \xi_-^{-1})$$

with $\xi_+ = \xi$ realized on upper nilpotent matrices and $\xi_- = \xi$ realized on lower nilpotent matrices. The restriction $u|_{U_p}$ only has values in ξ_+; so, ξ_-^{-1}-component does not show up as $u|_{U_{\mathfrak{p}}}$ is upper nilpotent, we have $S(u|_{U_p}) \in \mathrm{Hom}_{W[D]}(U_{\mathfrak{p}}[\xi], \xi_+^*)$. Since u factors through $O_p^\times/\overline{O^\times}$,

$$S(u|_{U_p}) \textit{ factors through } U_{\mathfrak{p}}[\xi]/\overline{\langle \varepsilon_\xi \rangle}.$$

Starting from $u_{\mathfrak{p}} \in \mathrm{Hom}(U_{\mathfrak{p}}[\xi]/\overline{\langle \varepsilon_\xi \rangle}, \xi^*)$, we recreate $u = S^{-1}(u_{\mathfrak{p}}) : U_p/\widehat{O}^\times[Ad] \to Ad^*$; so, we have $\mathrm{Sel}(Ad) \twoheadrightarrow \mathrm{Hom}(U_{\mathfrak{p}}[\xi]/\overline{\langle \varepsilon_\xi \rangle}, \xi_+^*)$.

8.14. **Frobenius part.** Note $M_p/U_p = \mathrm{Ind}_D^G W\mathbf{1} \cong \bigoplus_{\sigma(\mathfrak{p}):\sigma \in G/D} W\sigma(\mathfrak{p})$ as $W[G]$-modules with projection $\pi : \mathrm{Ind}_D^G W\mathbf{1} \twoheadrightarrow \widehat{Cl}_F^{(p)} \otimes_{\mathbb{Z}_p} W$. If $\mathfrak{p}$ has order p^h in $\widehat{Cl}_F^{(p)}$, this induces a surjection $\mathrm{Ind}_D^G W/p^hW\mathbf{1} \to \widehat{Cl}_F^{(p)} \otimes_{\mathbb{Z}_p} W$, which gives rise to an isomorphism:

$$(*) \qquad (\mathrm{Ind}_D^G W/p^hW\mathbf{1})[Ad] \cong (\widehat{Cl}_F^{(p)} \otimes_{\mathbb{Z}_p} W)[Ad] =: \widehat{Cl}_F^{(p)}[Ad]$$

by the irreducibility of $Ad(\overline{\rho})$. Therefore

$$u_0 \in \mathrm{Hom}_{W[G]}(\widehat{Cl}_F^{(p)}[Ad], Ad^*) \overset{(*)}{=} \mathrm{Hom}_{W[G]}(\mathrm{Ind}_D^G W/p^hW\mathbf{1}, Ad^*)$$
$$\overset{\text{Shapiro's lemma}}{=} \mathrm{Hom}_D(W/p^hW\mathbf{1}, Ad^*|_D) = W/p^hW.$$

Reversing the argument, the Frobenius part is given by

$$\mathrm{Hom}_{W[G]}(\widehat{Cl}_F^{(p)}[Ad], Ad^*) \cong \mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{Cl}_F^{(p)}, Ad^*).$$

This finishes the proof of the theorem. □

8.15. **Proof of the formula in the corollary.** Since $Ad^* = Ad(\rho) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \cong \mathrm{Hom}_{\mathbb{Z}_p}(Ad, \mathbb{Q}_p/\mathbb{Z}_p)$ and $\otimes$-Hom adjunction formula, we have

$$\mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{Cl}_F^{(p)}, Ad^*) \cong \mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{Cl}_F^{(p)}, \mathrm{Hom}_{\mathbb{Z}_p}(Ad, \mathbb{Q}_p/\mathbb{Z}_p)) \cong \mathrm{Hom}_{\mathbb{Z}_p}(\widehat{Cl}_F^{(p)} \otimes_{\mathbb{Z}_p[G]} Ad, \mathbb{Q}_p/\mathbb{Z}_p).$$

Similarly we have

$$\mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{C}_F, Ad^*)) \cong \mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{C}_F, \mathrm{Hom}_{\mathbb{Z}_p}(Ad, \mathbb{Q}_p/\mathbb{Z}_p)) \cong \mathrm{Hom}_{\mathbb{Z}_p}(\widehat{C}_F \otimes_{\mathbb{Z}_p[G]} Ad, \mathbb{Q}_p/\mathbb{Z}_p).$$

The W-corank of the Selmer group is positive when $\varepsilon_{\epsilon\delta^{-1}} = 1$. If this happens, it is equal to $\mathrm{rank}_W U_{\mathfrak{p}}[\epsilon\delta^{-1}]$. Since $U_{\mathfrak{p}}[\epsilon\delta^{-1}] = O_{\mathfrak{p}}^\times \otimes_{\mathbb{Z}} W[\epsilon\delta^{-1}]$ has the same rank with $O_{\mathfrak{p}} \otimes_{\mathbb{Z}_p} W[\epsilon\delta^{-1}]$ by D-equivariance of logarithm, we get $\mathrm{rank}_W(O_{\mathfrak{p}} \otimes_{\mathbb{Z}_p} W)[\epsilon\delta^{-1}] = 1$, since $F_{\mathfrak{p}}$ has normal basis over $\mathbb{Q}_p$.

8.16. **Galois action on global units.** Recall $(O^\times \otimes_{\mathbb{Z}} W) \oplus W\mathbf{1} \cong \mathrm{Ind}_C^G W\mathbf{1} \cong W[G/C]$ (as $\mu_p(F) = \{1\}$). Here C is the subgroup of G generated by the fixed complex conjugation c. The following lemma finishes the proof.

Lemma 8.4. *We have a $W[G]$-linear surjective homomorphism*

$$\phi : O^\times \otimes_{\mathbb{Z}} W \twoheadrightarrow Ad$$

and $\varepsilon_{\epsilon\delta^{-1}} \neq 1$.

Since $Ad(\overline{\rho})$ is irreducible over $\mathbb{F}$, if a $W[G]$-linear map $M \to Ad$ for a $W[G]$-module M is non-trivial modulo $\mathfrak{m}_W$, the map is surjective modulo $\mathfrak{m}_W$, and by Nakayama's lemma, the original map is surjective.

Proof. Since Ad is irreducible of dimension 3 over $\mathrm{Frac}(W)$, non-zero homomorphism

$$\phi \in \mathrm{Hom}_{W[G]}(O^\times \otimes_{\mathbb{Z}} W \oplus W\mathbf{1}, Ad)$$

has to factors through $O^\times \otimes_{\mathbb{Z}} W = W[G]\varepsilon$. By Shapiro's lemma, we have, for $\chi : C \cong \{\pm 1\}$,

$$\mathrm{Hom}_{W[G]}(O^\times \otimes_{\mathbb{Z}} W, Ad) = \mathrm{Hom}_{W[G]}(\mathrm{Ind}_C^G W\mathbf{1}, Ad)$$
$$= \mathrm{Hom}_{W[C]}(W\mathbf{1}, Ad|_C) = \mathrm{Hom}_{W[C]}(W\mathbf{1}, \chi \oplus \mathbf{1} \oplus \chi) = W.$$

Thus we have a $W[G]$-linear homomorphiosm $\phi : O^\times \otimes_{\mathbb{Z}} W \to Ad$ non-zero modulo $\mathfrak{m}_W$. Therefore, the $W[G]$-linear homomorphism $\phi : O^\times \otimes_{\mathbb{Z}} W \to Ad$ is onto, and Ad is generated over $W[G]$ by the image of ε. Since $Ad|_D = \xi \oplus \mathbf{1} \oplus \xi^{-1}$, the composed ξ-projection $O^\times \otimes_{\mathbb{Z}} W \xrightarrow{\phi} Ad \twoheadrightarrow Ad[\xi] = W\xi$ is onto producing a non-zero multiple of $\varepsilon_{\epsilon\delta^{-1}}$ as its image. □

9. Iwasawa theory over quadratic fields

Assuming that $\overline{\rho} = \mathrm{Ind}_K^{\mathbb{Q}} \overline{\varphi}$ for a character $\overline{\varphi} : \mathfrak{G}_{\mathbb{Q}} \to \mathbb{F}^\times$, we describe the size of its adjoint Selmer group in Case D in terms of a Minkowski unit. Let $G = \mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{Im}(Ad(\overline{\rho}))$. Let φ be the Teichmüller lift of $\overline{\varphi}$, and put $\rho = \mathrm{Ind}_K^{\mathbb{Q}} \varphi$. Then $G \cong \mathrm{Im}(Ad(\rho)) = \mathrm{Im}(Ad(\overline{\rho}))$. We write $\mathbb{F}$ for the field generated by the values of $\overline{\varphi}$. As seen in §6.6, $Ad(\rho) \cong \alpha \oplus \mathrm{Ind}_K^{\mathbb{Q}} \varphi^-$ for $\alpha = \left(\frac{K/\mathbb{Q}}{}\right)$. Then we take W to be the unramified extension of $\mathbb{Z}_p$ with $W/\mathfrak{m}_W = \mathbb{F}$. We write O (resp. O_K) for the integer ring F (resp. K). Fix a prime $\mathfrak{p}|p$ in O and a prime $\mathfrak{P}|\mathfrak{p}$ in $F(\varphi) = F(\overline{\rho})$. We write $D \subset G$ (resp. D') for the decomposition group of $\mathfrak{p}$ (resp. $\mathfrak{P}$) such that $\rho|_{D'} = \left(\begin{smallmatrix} \epsilon & 0 \\ 0 & \delta \end{smallmatrix}\right)$ with $\delta = \varphi_\sigma|_{D'}$ unramified. Since G is dihedral and p splits in K, $\mu_p(F) = \{1\}$ for $p \geq 3$.

9.1. **Galois action on global units.** Recall $(O^\times \otimes_{\mathbb{Z}} W) \oplus W\mathbf{1} \cong \mathrm{Ind}_C^G W\mathbf{1} \cong W[G/C]$. Here C is the subgroup of G generated by the fixed complex conjugation c.

Proposition 9.1. *We have*

$$\mathrm{Hom}_{W[G]}(\mathrm{Ind}_K^{\mathbb{Q}} \varphi^-, O^\times \otimes_{\mathbb{Z}} W) = \begin{cases} 0 & \text{if } K \text{ is real,} \\ W & \text{if } K \text{ is imaginary,} \end{cases}$$

$$\mathrm{Hom}_{\mathbb{Z}_p[G]}(\alpha, O^\times \otimes_{\mathbb{Z}} W) = \begin{cases} W & \text{if } K \text{ is real,} \\ 0 & \text{if } K \text{ is imaginary.} \end{cases}$$

If K is imaginary, $\varepsilon_{\varphi^-} \neq 1$ and $\varepsilon_\alpha = 1$ and if K is real, $\varepsilon_\alpha \neq 1$ and $\varepsilon_{\varphi^-} = 1$.

We have $\mathrm{Hom}_{W[G]}(\mathrm{Ind}_K^{\mathbb{Q}} \varphi^-, \mathrm{Ind}_C^G W\mathbf{1}) = \mathrm{Hom}_{W[C]}(\mathrm{Ind}_K^{\mathbb{Q}} \varphi^-|_C, W\mathbf{1})$ and $\mathrm{Hom}_{\mathbb{Z}_p[G]}(\alpha, \mathrm{Ind}_C^G \mathbf{1}) = \mathrm{Hom}_{\mathbb{Z}_p[C]}(\alpha|_C, \mathbf{1})$. The second assertion is clear from the second identity.

Proof. Pick $\sigma \in G$ such that $\sigma|K$ is non-trivial. If K is imaginary, $\mathrm{Ind}_K^{\mathbb{Q}} \varphi^-|_C = \mathbf{1} \oplus \alpha$ as $\mathrm{Tr}(\mathrm{Ind}_K^{\mathbb{Q}} \varphi^-)(c)) = 0$. Therefore

$$\mathrm{Hom}_{W[C]}(\mathrm{Ind}_K^{\mathbb{Q}} \varphi^-|_C, W\mathbf{1}) = \mathrm{Hom}_{W[C]}(\mathbf{1} \oplus \alpha, \mathbf{1}) = W.$$

Suppose that K is real. Since

$$Ad(\overline{\rho})(c) \sim \mathrm{diag}[-1, 1, -1] \sim \mathrm{diag}[\varphi^-(c), \alpha(c), (\varphi^-)^{-1}(c)],$$

$\alpha(c) = 1$ implies $\varphi^-(c) = \varphi^-_\sigma(c) = -1$. Therefore

$$\mathrm{Hom}_{W[C]}(\mathrm{Ind}_K^{\mathbb{Q}} \varphi^-|_C, W\mathbf{1}) = \mathrm{Hom}_{W[C]}(\chi \oplus \chi, \mathbf{1}) = 0$$

for $\chi : C \cong \{\pm 1\}$. □

9.2. **Selmer group and ray class group.** Recall Lemma 8.1:

Lemma 9.2. *We have a canonical inclusion*

$$\mathrm{Sel}(Ad(\rho)) \subset \mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{Cl}_F(p^\infty), Ad(\rho)^*).$$

As before, we put $\mathfrak{H} = \mathrm{Gal}(F^{(p)}/F)$, and we study decomposition group in $\mathfrak{H}^{ab}$ as D-modules. Recall the fixed prime factor $\mathfrak{p}|p$ in O with its decomposition subgroup $D \subset G$. Write simply $M_\mathfrak{p} := F_\mathfrak{p}^\times \otimes_{\mathbb{Z}} W$ and $U_\mathfrak{p} := \widehat{O_\mathfrak{p}^\times} \otimes_{\mathbb{Z}_p} W = O_\mathfrak{p}^\times \otimes_{\mathbb{Z}} W$. Then for each character $\xi : D \to W^\times$, $M_\mathfrak{p}$ contains as a direct factor the ξ-eigenspace $M_\mathfrak{p}[\xi]$. Then writing $\mu_p(F_\mathfrak{p})_{/\mathbb{F}} = \mu_p(F_\mathfrak{p}) \otimes_{\mathbb{Z}} \mathbb{F}$

(U) $M_\mathfrak{p}[\xi] = U_\mathfrak{p}[\xi] \cong \begin{cases} W & \text{if } \xi \notin \{\mathbf{1}, \omega\}, \\ W \oplus \mu_p(F_\mathfrak{p})_{/\mathbb{F}} & \text{if } \xi = \omega. \end{cases}$

(M) We have an exact sequence $0 \to U_\mathfrak{p}[\mathbf{1}] \to M_\mathfrak{p}[\mathbf{1}] \xrightarrow{\mathrm{ord}_\mathfrak{p}} W \to 0$ induced by the valuation $\mathrm{ord}_\mathfrak{p} : F_\mathfrak{p}^\times \twoheadrightarrow \mathbb{Z}$ at $\mathfrak{p}$, and $U_\mathfrak{p}[\mathbf{1}] \cong W$.

9.3. **Structure of $M_p[Ad]$ as a G-module in Case D..** For each irreducible factor ϕ of Ad, we consider the ϕ-isotypical component $X[\phi]$, and write $\mu_p(F_{\mathfrak{p}})_{/\mathbb{F}} = \mu_p(F_{\mathfrak{p}}) \otimes_{\mathbb{Z}} \mathbb{F}$.

Lemma 9.3. *Assume $\varphi^-|_D \neq 1$ and $p \geq 5$.*

$$\mathrm{Hom}_G(M_p, \phi^*) = \begin{cases} \mathrm{Hom}_D(U_{\mathfrak{p}}[\varphi^-] \oplus U_{\mathfrak{p}}[\varphi^-_\sigma], (\phi|_D)^*) \cong W^2 \oplus \mu_p(F_{\mathfrak{p}})_{/\mathbb{F}}[\xi^{\pm 1}] & \dim \phi = 2, \\ \mathrm{Hom}_D(U_{\mathfrak{p}}[\phi], \phi^*) \cong W & \phi \subsetneq \mathrm{Ind}_K^{\mathbb{Q}} \varphi^-, \\ \mathrm{Hom}_D(M_{\mathfrak{p}}[\mathbf{1}], \mathbf{1}^*) \cong W^2 & \phi = \alpha, \end{cases}$$

where $\xi = \varphi^-$ in the first case.

Proof. Since $M_p = \mathrm{Ind}_D^G M_{\mathfrak{p}}$, we have $\mathrm{Hom}_G(M_p, \phi^*) = \mathrm{Hom}_D(M_{\mathfrak{p}}, \phi^*|_D)$ by Shapiro's lemma. If $\varphi^-|_D \neq \mathbf{1}$, $\phi|_D$ is

- $(\varphi^- \oplus \varphi^-_\sigma)|_D$ when $\phi = \mathrm{Ind}_K^{\mathbb{Q}} \varphi^-$ is irreducible ($\mathrm{ord}(\varphi^-) \geq 3$),
- $\varphi^-|_D$ when $\phi \subsetneq \mathrm{Ind}_K^{\mathbb{Q}} \varphi^-$ ($\mathrm{ord}(\varphi^-) = 2$),
- $\mathbf{1}$ when $\phi = \alpha$.

Let $\xi = \varphi^-|_D$. Since $M_{\mathfrak{p}}[\xi^{\pm 1}] = U_{\mathfrak{p}}[\xi^{\pm 1}]$ (by $\xi \neq \mathbf{1}$),

$$(\mathrm{Ind}_D^G U_{\mathfrak{p}}[\xi^{\pm 1}])[Ad] = \begin{cases} \phi \oplus \mathrm{Ind}_D^G \mu_p(F_{\mathfrak{p}})[\phi] & \text{if } \xi \neq \xi^{-1} \text{ and } \dim \phi = 2, \\ \phi \oplus \phi\alpha & \text{if } \phi \subsetneq \mathrm{Ind}_K^{\mathbb{Q}} \varphi^-, \\ 0 & \text{if } \phi = \alpha, \end{cases}$$

$$(\mathrm{Ind}_D^G M_{\mathfrak{p}}[\mathbf{1}])[Ad] = \begin{cases} 0 & \text{if } \phi \subset \mathrm{Ind}_K^{\mathbb{Q}} \varphi^-, \\ \alpha \oplus \alpha & \text{if } \phi = \alpha. \end{cases}$$

This is because $M_{\mathfrak{p}}[\xi^{\pm 1}] = U_{\mathfrak{p}}[\xi^{\pm 1}] \cong W \oplus \mu_p(F_{\mathfrak{p}})_{/\mathbb{F}}$ by (U) and by Shapiro's lemma

$$\begin{aligned} \mathrm{Hom}_G(\mathrm{Ind}_K^{\mathbb{Q}} \varphi^-, \mathrm{Ind}_D^G U_{\mathfrak{p}}[\xi]) &= \mathrm{Hom}_D(\mathrm{Ind}_K^{\mathbb{Q}} \varphi^-|_D, \xi \oplus (\mu_p(F_{\mathfrak{p}}) \otimes_{\mathbb{Z}} \mathbb{F})) \\ &= \mathrm{Hom}_D(\xi \oplus \xi^{-1}, \xi \oplus (\mu_p(F_{\mathfrak{p}}) \otimes_{\mathbb{Z}} \mathbb{F})) \end{aligned}$$

as $D \subset \mathrm{Gal}(F/K)$. The second formula follows from (M). □

9.4. **Theorem for** $\mathrm{Sel}(\mathrm{Ind}_K^{\mathbb{Q}} \varphi^-)$**.** The representations $\Phi := \mathrm{Ind}_K^{\mathbb{Q}} \varphi^-$ and α in $Ad(\rho)$ fits into the following exact sequence of G-modules:

$$0 \to \overbrace{\Phi \oplus \mathrm{Ind}_D^G(\mu_p(F_{\mathfrak{p}}) \otimes_{\mathbb{Z}} \mathbb{F})[\Phi] \oplus \alpha \oplus \Phi}^{\text{inertia part}} \to M_p[Ad] \to \alpha \to 0.$$

Here Φ can be reducible.

Theorem 9.4. *Assume that we are in Case D with irreducible $\mathrm{Ind}_K^{\mathbb{Q}} \overline{\varphi}$. Then we have an exact sequence*

$$\mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{Cl}_F, \Phi^*) \hookrightarrow \mathrm{Sel}(\Phi) \twoheadrightarrow \mathrm{Hom}_{W[D]}(U_{\mathfrak{p}}[\varphi^-]/\overline{\langle \varepsilon_{\varphi^-} \rangle}, W^\vee),$$

where ε is a Minkowski unit, ε_{φ^-} is the projection of ε in the direct summand $U_{\mathfrak{p}}[\varphi^-]$ under $O^\times \to U_p \twoheadrightarrow U_{\mathfrak{p}}[\varphi^-]$, and $\overline{\langle \varepsilon_{\varphi^-} \rangle}$ is the p-adic closure of the subgroup $\varepsilon_{\varphi^-}^{\mathbb{Z}}$ generated by ε_{φ^-}.

Proof. Proof of $\mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{Cl}_F, \Phi^*) \hookrightarrow \mathrm{Sel}(\Phi)$. We proceed as in Case E (in §8.10) replacing Ad by Φ. Since $\widehat{Cl}_F^{(p)}$ (surjective image of $\mathrm{Ind}_D^G \mathbf{1}$) does not contain $\Phi = \mathrm{Ind}_K^{\mathbb{Q}} \varphi^-$, we can ignore it and can work with the entire $\widehat{Cl}_F$. Elements in $\mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{Cl}_F, \Phi^*)$ are everywhere unramified and trivial at p; so, they gives rise to a subgroup of $\mathrm{Sel}(\Phi)$ of classes everywhere unramified and trivial at p. Indeed, by $H^1(\mathfrak{G}, \Phi^*) \cong \mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathfrak{H}^{ab}, \Phi^*)$, any $u \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{Cl}_F, \Phi^*)$ extends uniquely the cocycle $u : \mathfrak{G} \to \Phi^*$ unramified everywhere over $\mathfrak{H}$. Since the inertia group $I_l \subset G$ of any prime $l \in S$ has order prime to p, $u|_{I_l} = 0$, and hence $[u] \in \mathrm{Sel}(\Phi)$.

Elements of $\mathrm{Sel}(\Phi)$ modulo $\mathrm{Hom}_{\mathbb{Z}_p[G]}(\widehat{Cl}_F, \Phi^*)$ is determined by its restriction to M_p as they are unramified outside p as they factor through $\widehat{Cl}_F(p^\infty)$ and $p \nmid |I_l|$.

Inertia part. Recall $\xi = \epsilon\delta^{-1} = \varphi^-$. A Selmer cocycle $u|_{\mathfrak{H}^{ab}}$ regarded as a $W[\Gamma^-]]$-linear homomorphism in $\mathrm{Hom}_{W[[\Gamma^-]]}(\mathcal{Y}(\varphi^-), (\varphi^-)^*)$ has values in $(\varphi^-)^*$ over U_p. Since $M_p/U_p \cong \mathrm{Ind}_D^G W\mathbf{1}$ does not contain Φ, we can ignore M_p/U_p. By its G-equivariance,

$$u|_{U_p} \in \mathrm{Hom}_{W[G]}(U_p, \Phi^*).$$

By Shapiro's lemma,

$$\mathrm{Hom}_{W[G]}(U_p, \Phi^*) \cong \mathrm{Hom}_{W[D]}(U_{\mathfrak{p}}[\varphi^-], (\varphi^-)^*).$$

Since u factors through $O_p^\times/\overline{O^\times}$, u factors through $U_{\mathfrak{p}}[\varphi^-]/\overline{\langle\varepsilon_{\varphi^-}\rangle}$. □

Corollary 9.5. *If K is imaginary, we have*

$$|\mathrm{Sel}(\mathrm{Ind}_K^{\mathbb{Q}} \varphi^-)| = |\widehat{Cl}_F \otimes_{\mathbb{Z}_p[\mathrm{Gal}(F/K)]} \varphi^-||(U_{\mathfrak{p}}[\varphi^-]/\overline{\langle\varepsilon_{\varphi^-}\rangle})|$$

which is finite, otherwise it has W-corank 1 (up to finite W-torsion).

Proof. By Proposition 9.1, $\varepsilon_{\varphi^-} \neq 1$ only when K is imaginary. Thus the finiteness of the Selmer group follows. When K is real, we have $U_{\mathfrak{p}}[\varphi^-] \cong W$, and therefore from Theorem 9.4, the Selmer group has corank 1. □

10. "$R = \mathbb{T}$" theorem and adjoint Selmer groups

On the way to prove FLT, Wiles and Taylor identified the universal ring R for the deformation functor $\mathcal{D}_\kappa$ with a p-adic Hecke algebra $\mathbb{T}$. The algebra $\mathbb{T}$ is known to be free of finite rank over the Iwasawa algebra, and they also showed that $R = \mathbb{T}$ is a local complete intersection over Λ. We explore consequences of these result in our study of the adjoint Selmer groups of modular Galois representations.

10.1. **Local complete intersection ring.** Let $B \in CL_{/W}$ be the base ring which is an integral domain. An object $A \in CL_{/B}$ is called a (relative) local complete intersection over B if A is free of finite rank over B with a presentation $A \cong B[[X_1, \dots, X_r]]/(f_1, \dots, f_r)$ for a positive integer r. Then the following facts are known

- $\mathrm{Hom}_B(A, B)$ is free of rank 1 over B (i.e., A is a Gorenstein ring over B);
- $x \mapsto f_j x$ is an injection over $A/(f_1, \dots, f_{j-1})$ for all $j = 1, \dots r$ (i.e., $(f_1, \dots, f_r)$ is a regular sequence;
- If A is generated over B by m elements, the minimal choice of r is m.

For these facts, see [CRT, §21].

Theorem 10.1 (J. Tate)**.** *If B is normal noetherian and $P : A \to B$ is a B-algebra homomorphism with $A \otimes_B \mathrm{Frac}(B) = \mathrm{Frac}(B) \oplus (\mathrm{Ker}(P) \otimes_B \mathrm{Frac}(B))$ as an algebra direct summand, we have*

$$\mathrm{char}(C_0) = \mathrm{char}(C_1),$$

where $C_0 = C_0(P) = A \otimes_A S$ for the image S of A in the algebra $\mathrm{Ker}(P) \otimes_B \mathrm{Frac}(B)$ and $C_1 = C_1(P) = \Omega_{A/B} \otimes_{A,P} B$.

Tate actually proved a finer equality $\mathrm{Fitt}(C_0) = \mathrm{Fitt}(C_1)$ of Fitting B-ideals for any commutative algebra B with identity. For Tate's proof, see the appendix to the paper by Mazur–Robert [MR70].

10.2. **Homological dimension.** For a noetherian local ring A in $CL_{/W}$, we define the homological dimension $\mathrm{hdim}_B M$ of a finitely generated B-module M is the minimum length h of exact sequence $0 \to F_h \to F_{h-1} \to \cdots \to F_0 \to M \to 0$ made of R-free module F_j of finite rank. If $R_{A/B}$ is a local complete intersection free of finite rank over B, we have a presentation $A = B[[T_1, \dots, T_r]/(f_1, \dots, f_r)$ for a regular sequence $f_1, \dots, f_r$. Then the 2nd fundamental exact sequence (Corollary 2.2) gives an exact sequence

$$(f_1, \dots, f_r)/(f_1, \dots, f_r)^2 \xrightarrow{i} \Omega_{B[[T_1,\dots,T_r]]/B} \otimes_{B[[T_1,\dots,T_r]]} A \twoheadrightarrow \Omega_{A/B}.$$

If further B is a domain of characteristic 0 and A is reduced, $\Omega_{A/B}$ is a torsion A-module (as the extension $\mathrm{Frac}(A)/\mathrm{Frac}(B)$ is a finite semi-simple extension). Since $(f_1, \dots, f_r)/(f_1, \dots, f_r)^2 \cong A^r$ as $(f_1, \dots, f_r)$ is a regular sequence, torsion-property of $\Omega_{A/B}$ tells us that i is injective; so, we get from $\Omega_{B[[T_1,\dots,T_r]]/B} \otimes_{B[[T_1,\dots,T_r]]} A \cong \bigoplus_j AdT_j$

$$\boxed{\mathrm{hdim}\,\Omega_{A/B} = 1} \text{ if } A \text{ is local complete intersection over } B.$$

10.3. **Taylor-Wiles theorem.** Taylor and Wiles proved

Theorem 10.2. *Under* (ord$_l$) *for* $l \in S \cup \{p\}$, R_χ/B *is a local complete intersection with presentation* $R_\chi = B[[T_1, \dots, T_r]]/(f_1, \dots, f_r)$ *for* $r = \dim_{\mathbb{F}} \mathrm{Sel}(Ad(\overline{\rho}))$, *where* $B = W$ *if* χ *has values in* $W^\times$ *and* $B = \Lambda$ *if* $\chi = \kappa$. *In particular, we have* $\mathrm{hdim}_B\, \Omega_{R_\chi/B} \le 1$.

What Taylor–Wiles proved is a bit different from this theorem for the number of variables. There presentation has the number of variables r_0 possibly slightly bigger than $\dim_{\mathbb{F}} \mathrm{Sel}(Ad(\overline{\rho})(1)) \ge r = \dim_{\mathbb{F}} \mathrm{Sel}(Ad(\overline{\rho}))$. Since R_χ is generated by r elements over B as seen in Lecture No.3, by [CRT, Theorem 21.2 (ii)], we can change Taylor–Wiles presentation so that it is valid for r. For a proof, see [TW] and [HMI, §3.2].

10.4. **Existence of p-adic L..** Let $\rho : \mathfrak{G}_{\mathbb{Q}} \to \mathrm{GL}_2(A)$ be a deformation of $\overline{\rho}$ such that $\rho \cong P \circ \boldsymbol{\rho}_\chi$. If $r = 1$, $R_\chi = B[[T_1]]/(f_1)$ and we have an exact sequence for $(P : R_\chi \to A) \in \mathrm{Hom}_{B\text{-alg}}(R_\chi, A)$

$$\begin{array}{ccccc} A = (f_1)/(f_1^2) \otimes_{R_\chi} A & \longrightarrow & A \cdot dT_1 & \overset{\twoheadrightarrow}{\longrightarrow} & \Omega_{R_\chi/B} \otimes_{R_\chi} A \\ \| \big\uparrow L_\rho \mapsto f_1 & & \| \big\uparrow 1 \mapsto dT_1 & & \wr \big\uparrow \\ A \cdot L_\rho & \longrightarrow & A & \underset{\twoheadrightarrow}{\longrightarrow} & \mathrm{Sel}(Ad(\rho))^\vee. \end{array}$$

If $B = W$, $|L_\rho|_p^{-1} = |\mathrm{Sel}(Ad(\rho)|$ and $L_{\boldsymbol{\rho}}(P) := P(L_{\boldsymbol{\rho}}) = L_\rho$. If $B = \Lambda$ ($\chi = \kappa$), $L_{\boldsymbol{\rho}}$ gives rise to a p-adic L-function with

$$\mathrm{Spec}(R_\kappa)(W) \ni P \mapsto |L_{\boldsymbol{\rho}}(P)|_p^{-1} = |\mathrm{Sel}(Ad(P \circ \boldsymbol{\rho}))|.$$

If $r > 1$, we define

$$L_{\boldsymbol{\rho}} := \det((f_1, \dots, f_r)/(f_1, \dots, f_r)^2 \to \bigoplus_{j=1}^{r} R_\kappa \cdot dT_j),$$

and the outcome is the same.

10.5. **Universal modular deformation.** Let N be the prime-to-p Artin conductor of $\overline{\rho}$ with $\det \overline{\rho}(c) = -1$. By the solution of Serre's mod p modularity conjecture, we have Hecke eigenforms f (actually infinitely many) whose p-adic Galois representation ρ_f is in $\mathcal{D}_\kappa(A_f)$ for a finite extension A_f of W generated by $\mathrm{Tr}(\rho_f)$. We can define the p-adic Hecke algebra $\mathbb{T}$ interpolating all modular Galois representation $\rho_f \in \mathcal{D}_\kappa(A_f)$ as follows: The algebra $\mathbb{T} \subset \prod_f A_f$ topologically generated by $\prod_f \mathrm{Tr}(\rho_f(g))$ for all $g \in \mathfrak{G}_{\mathbb{Q}}$. Then by my old result in 1986, we have a Galois representation $\rho_{\mathbb{T}} : \mathfrak{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$ such that $\rho_{\mathbb{T}} \in \mathcal{D}_\kappa(\mathbb{T})$ (in particular $\mathbb{T} \in CL_{/\Lambda}$). The proof of Theorem 10.2 actually produces the following

Corollary 10.3. *Suppose* (ord$_l$) *in* §5.1 *for* $l \in S \cup \{p\}$. *Then we have* $\iota : R_\kappa \cong \mathbb{T}$ *such that* $\iota \circ \boldsymbol{\rho} \cong \rho_{\mathbb{T}}$.

See [TW] and [HMI, §3.2].

10.6. **Lifting to an extension $\mathbb{I}$ of Λ.** Let $\lambda : R_\kappa = \mathbb{T} \twoheadrightarrow \mathbb{I}$ be a Λ-algebra surjective homomorphism for an integral domain $\mathbb{I}$ finite torsion-free over Λ. Let $\mathbb{T}_{\mathbb{I}} := \mathbb{T} \otimes_\Lambda \mathbb{I}$ and $\widetilde{\lambda}$ be the composite $\mathbb{T}_{\mathbb{I}} \twoheadrightarrow \mathbb{I} \otimes_\Lambda \mathbb{I} \xrightarrow[\twoheadrightarrow]{a \otimes b \mapsto ab} \mathbb{I}$. Then for each $P \in \mathrm{Spec}(\mathbb{I})(W) = \mathrm{Hom}_{W\text{-alg}}(\mathbb{I}, W)$, $\widetilde{\lambda}$ induces $\Lambda \hookrightarrow \mathbb{T}_{\mathbb{I}} \xrightarrow{\widetilde{\lambda}} \mathbb{I} \xrightarrow{P} W$ by composition.

Writing $\rho_P := P \circ \lambda \circ \boldsymbol{\rho}$. Then $\det \rho_P$ is a deformation of $\det \overline{\rho}$; so, we have a unique morphism $\iota_P : \Lambda \to W$ such that $\iota_P \circ \kappa = \det(\rho_P)$. Since the Λ-algebra structure $\iota : \Lambda \to \mathbb{T}$ of $\mathbb{T} = R_\kappa$ is given by $\det(\boldsymbol{\rho}) = \det(\rho_{\mathbb{T}}) = \iota \circ \kappa$, we find out that the above composite is just ι_P.

Let $\mathbb{T}_P = \mathbb{T}_{\mathbb{I}} \otimes_{\mathbb{I},P} W$ under the above algebra homomorphism. Note that

$$\mathbb{T}_P = \mathbb{T} \otimes_\Lambda \mathbb{I} \otimes_{\mathbb{I},P} W \cong \mathbb{T} \otimes_{\Lambda,\iota_P} W$$

by associativity of tensor product.

10.7. **Modular and admissible points.** By construction, we have $\lambda_P : \mathbb{T}_P \to W$ induced by λ. Even if $\iota_P = \iota_{P'}$, λ_P may be different from $\lambda_{P'}$. If λ_P is associated to a Hecke eigenform of weight ≥ 2, we call P a **modular** point. If $\mathbb{T}_P \otimes_W \mathrm{Frac}(W) = \mathrm{Frac}(W) \oplus (\mathrm{Ker}(\lambda_P) \otimes_W \mathrm{Frac}(W))$ as algebra direct sum, we call P **admissible**. If P is admissible, $C_0(\lambda_P)$ is well defined. If P is modular, it is admissible.

If $\rho \in \mathcal{D}_\chi(A)$ for W-valued $\chi = \det(\rho_P)$, then $\rho \in \mathcal{D}_\kappa(A)$ and hence $\rho = \phi \circ \boldsymbol{\rho}$ for $\phi : R_\kappa \to A$. By definition, ϕ factors through

$$R_\kappa / R(\det(\boldsymbol{\rho})(g) - \chi(g))_g R = R_\kappa / R(\kappa(g) - \chi(g))_g R = R \otimes_{\Lambda,\chi} W.$$

This shows that $R_\chi = R \otimes_{\Lambda,\chi} W$ for $\chi : \Lambda = W[[\Gamma]] \to W$ induced by χ. Applying this to $\mathbb{T}_P$, we get $R_{\det(\rho_P)} = \mathbb{T}_P$.

10.8. **Modular adjoint p-adic L: L^{mod}.** Suppose (ord_l) in §5.1 for $l \in S \cup \{p\}$. Here is a theorem I proved long ago (e.g., [MFG, §5.3.6]) for canonical periods $\Omega_{f,\pm}$ of f:

Theorem 10.4. *Let $\lambda : \mathbb{T} \twoheadrightarrow \mathbb{I}$ be a surjective Λ-algebra homomorphism for a domain $\mathbb{I}$ containing Λ and $\widetilde{\lambda} : \mathbb{T}_{\mathbb{I}} \to \mathbb{I}$ be its scalar extension to $\mathbb{I}$ as in §10.6. Then there exists $L^{mod} \in \mathbb{I}$ such that $C_0(\lambda) = \mathbb{I}/(L^{mod})$ and for each admissible $P \in \mathrm{Spec}(\mathbb{I})$, $C_0(\lambda_P) = W/P(\lambda(L^{mod}))$ and if $P \circ \lambda \circ \rho_{\mathbb{T}} \cong \rho_f$ for a modular form of weight ≥ 2, we have $|C_0(\lambda_P)| = |W/P(\lambda(L^{mod}))| = |\frac{L(1,Ad(\rho_f))}{\Omega_{f,+}\Omega_{f,-}}|_p^{-1}$* (see [MFG, Corollary 5.31]).

If f is of weight 2 on a modular curve X, for $\mathcal{W} = W \cap \overline{\mathbb{Q}}$, we have $H^1(X, \mathcal{W})[\lambda_P] = \mathcal{W}\omega_+(f) \oplus \mathcal{W}\omega_-(f)$ ($\pm$-eigenspace under the pull-back action of $z \mapsto -\overline{z}$ on the upper half complex plane) and $H^1(X, \mathbb{C}) = \mathbb{C}\delta_+(f) + \mathbb{C}\delta_-(f)$ for $\delta_\pm f = f(z)dz \mp f(-\overline{z})d\overline{z}$. Then $\Omega_{f,\pm}\omega_\pm(f) = \delta_\pm(f)$. We use Eichler-Shimura isomorphism to define $\Omega_{f,\pm}$ for higher weight.

10.9. **Sketch of Proof of the existence of L^{mod}.** Write $X^* := \mathrm{Hom}_{\mathbb{I}}(X, \mathbb{I})$ for an $\mathbb{I}$-module X. Let S be the image of $\mathbb{T}_{\mathbb{I}}$ in $\mathfrak{B} \otimes_{\mathbb{I}} \mathrm{Frac}(\mathbb{I})$ for $\mathfrak{B} = \mathrm{Ker}(\widetilde{\lambda})$ in the decomposition $\mathbb{T} \otimes_\Lambda \mathrm{Frac}(\mathbb{I}) = \mathrm{Frac}(\mathbb{I}) \oplus (\mathfrak{B} \otimes_{\mathbb{I}} \mathrm{Frac}(\mathbb{I}))$. Let $\mu : \mathbb{T}_{\mathbb{I}} \to S$ be the projection and put $\mathfrak{A} = \mathrm{Ker}(\mu)$. So we have a split exact sequence $\mathfrak{B} \hookrightarrow \mathbb{T}_{\mathbb{I}} \twoheadrightarrow \mathbb{I}$. A local complete intersection $\mathbb{T}_{\mathbb{I}}$ over $\mathbb{I}$ has such a self-dual pairing $(\cdot,\cdot)$ with values in $\mathbb{I}$ such that $(xy, z) = (x, yz)$ for $x, y, z \in \mathbb{T}_{\mathbb{I}}$. Thus $\mathfrak{B}^* \cong \mathbb{T}_{\mathbb{I}}^*/\mathbb{I}^*$, and $\mathbb{I}^* \subset \mathbb{T}_{\mathbb{I}} = \mathbb{T}_{\mathbb{I}}^*$ is a maximal submodule of $\mathbb{T}_{\mathbb{I}}$ on which $\mathbb{T}_{\mathbb{I}}$ acts through $\widetilde{\lambda}$; so, $\mathbb{I}^* = \mathfrak{A}$ inside $\mathbb{T}_{\mathbb{I}}$. This implies $\mathfrak{B}^* \cong S$; so, S is $\mathbb{I}$-free. In other words, applying $\mathbb{I}$-dual, we get a reverse exact sequence

$$\begin{array}{ccccc} \mathbb{I}^* & \xrightarrow{\hookrightarrow} & \mathbb{T}_{\mathbb{I}}^* & \xrightarrow{\twoheadrightarrow} & \mathfrak{B}^* \\ \wr\downarrow & & \wr\downarrow & & \wr\downarrow \\ ? & \longrightarrow & \mathbb{T}_{\mathbb{I}} & \longrightarrow & S \end{array}$$

This shows $? = \mathfrak{A} \cong \mathbb{I}^* \cong \mathbb{I}$; so, $\mathfrak{A}$ is principal to have $L^{mod} \in \mathbb{I}$ such that $\mathfrak{A} = (L^{mod})$. Note that $C_0(\widetilde{\lambda}) = \mathbb{I}/\mathfrak{A}$ (see §2.6).

10.10. **Specialization property.** We have $\mathfrak{B}^* = S$ and a split exact sequence $\mathfrak{B} \to \mathbb{T}_{\mathbb{I}} \to \mathbb{I}$; so, $\mathfrak{B}$ is an $\mathbb{I}$-direct summand of $\mathbb{T}_{\mathbb{I}}$. Tensoring W over $\mathbb{I}$ via P, $\mathfrak{B} \otimes_{\mathbb{I},P} W \to \mathbb{T}_P \to W$ is exact, and we get $\mathfrak{B}_P = \mathfrak{B} \otimes_{\mathbb{I},P} W = \mathrm{Ker}(\lambda_P)$. Since $\mathbb{T}$ is Λ-free of finite rank, $\mathbb{T}_{\mathbb{I}}$ is $\mathbb{I}$-free of finite rank. Thus $\mathfrak{B}$ is $\mathbb{I}$-projective and hence $\mathbb{I}$-free; so, $S \cong \mathfrak{B}^*$ is $\mathbb{I}$-free. Tensoring W over $\mathbb{I}$ via P, we get

$$0 \to \mathfrak{A} \otimes_{\mathbb{I},P} W \to \mathbb{T}_P \to S \otimes_{\mathbb{I},P} W \to 0.$$

Thus if P is admissible, $S_P := S \otimes_{\mathbb{I},\lambda_P} W$ gives rise to the decomposition: $\mathbb{T}_P \otimes_W \mathrm{Frac}(W) = \mathrm{Frac}(W) \oplus (S_P \otimes_W \mathrm{Frac}(W))$. By $\mathfrak{B}_P = \mathfrak{B}_P \otimes_{\mathbb{I},P} W = \mathrm{Ker}(\lambda_P)$, we get $C_0(\lambda_P) = S_P/\mathfrak{B}_P = (S/\mathfrak{B}) \otimes_{\mathbb{I},P} W = C_0(\widetilde{\lambda}) \otimes_{\mathbb{I},P} W$, as desired. □

10.11. **Relation between $L_{\boldsymbol{\rho}}$ and L^{mod}.** Tensoring $\mathbb{I}$ with the exact sequence of $\mathbb{T}$-modules:

$$(f_1, \ldots, f_r)/(f_1, \ldots, f_r)^2 \xrightarrow{f \mapsto df} \Omega_{\Lambda[[T_1,\ldots,T_r]]/\Lambda} \otimes_{\Lambda[[T_1,\ldots,T_r]]} \mathbb{T} \twoheadrightarrow \Omega_{\mathbb{T}/\Lambda}$$

over $\mathbb{T}$, we get an exact sequence

$$\bigoplus_j \mathbb{I}df_j \xrightarrow{d \otimes 1 = \lambda(d)} \bigoplus_j \mathbb{I}dT_j \to \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T},\lambda} \mathbb{I} \to 0.$$

Since $\mathbb{T}_{\mathbb{I}} = \mathbb{I}[[T_1, \ldots, T_r]]/(f_1, \ldots, f_r)_{\mathbb{I}}$, we have

$$\Omega_{\mathbb{T}_{\mathbb{I}}/\mathbb{I}} \otimes_{\mathbb{T}_{\mathbb{I}},\widetilde{\lambda}} \mathbb{I} = \bigoplus_j \mathbb{I}dT_j / \bigoplus_j \mathbb{I}df_j = \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T},\lambda} \mathbb{I}.$$

They have the same characteristic ideals (and Fitting ideals) by Tate's theorem. Thus in general, we get

$$\begin{aligned}(\lambda(L_{\boldsymbol{\rho}})) &= (\lambda(\det(d))) = (\det(d \otimes 1)) \\ &= \mathrm{char}(C_1(\widetilde{\lambda})) \overset{\text{Tate}}{=} \mathrm{char}(C_0(\widetilde{\lambda})) = (L^{mod}).\end{aligned}$$

10.12. **Conclusion.** Thus we obtain

Corollary 10.5. *Let the notation and the assumption be as in Theorem 2. Then we have* $\lambda(L_{\boldsymbol{\rho}})/L^{mod} \in \mathbb{I}^{\times}$.

The corollary tells us that $L_{mod} \in \mathbb{I}$ glues (up to units) well to $L_{\boldsymbol{\rho}}$ so that the image $\lambda(L_{\boldsymbol{\rho}})$ of $L_{\boldsymbol{\rho}}$ in $\mathbb{I}$ is equal to L^{mod} of $\mathbb{I}$ up to units as long as $\mathbb{I}$ contains Λ as a subalgebra.

As seen in Corollary 2.2, $C_1 = C_1(\widetilde{\lambda}) = \mathfrak{B}/\mathfrak{B}^2$ and $C_0 = C_0(\widetilde{\lambda}) = S/\mathfrak{B}$. If $r \leq 1$, C_1 is cyclic, and by Nakayama's lemma, $\mathfrak{B}$ is generated by an element θ of S. Since $C_1 \cong C_0$ by Tate's theorem and C_0 is $\mathbb{I}$-torsion, θ is a non-zero-divisor of S. Thus the multiplication by θ gives rise to $C_0 \cong C_1$.

References

Books

[BCM] N. Bourbaki, *Algèbre Commutative*, Hermann, Paris, 1961–83

[CGP] K. S. Brown, *Cohomology of Groups*, Graduate texts in Math. **87**, Springer, 1982

[CPI] K. Iwasawa, *Collected Papers*, Vol. 1-2, Springer, 2001

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

[HMI] H. Hida, *Hilbert modular forms and Iwasawa theory*, Oxford University Press, 2006.

[IAT] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press and Iwanami Shoten, 1971, Princeton-Tokyo

[ICF] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Text in Mathematics, **83**, Springer, 1980

[LFE] H. Hida, *Elementary Theory of L–functions and Eisenstein Series*, LMSST **26**, Cambridge University Press, Cambridge, 1993

[LGF] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901.

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

Articles

[Du] G. F. D. Duff, Differential forms in manifolds with boundary. Ann. of Math. **56**, (1952) 115–127

[MR70] B. Mazur and L. Robert, Local Euler characteristic, Invent. Math. **9** (1970), 201–234.

[M] B. Mazur, Courbes elliptiques et symbols modulaires, Sém. Bourbaki Exposé 414 (1972, juin)

[MS] B. Mazur and H. P. F. Swinnerton-Dyer, Arithmetic of Weil curves, Inventiones Math. **25** (1974), 1–61

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

[W2] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. **141** (1995), 443–551.

Department of Mathematics, UCLA, Los Angeles, CA 90095-1555, U.S.A.
E-mail address: hida@math.ucla.edu