Introductory lecture slide No.0 for Math 207c

Haruzo Hida

An expectation: For a given group G,
Knowing all irreducible representations is equivalent to knowing the group G?
as representations are easier to understand. If G is finite, a representation embeds G into $\mathrm{GL}_n(A)$ for a suitable ring A; so, the question is "a sort of" valid (but hard to describe the image). But if G is huge?

When G is abelian, the unitary character group $\widehat{G} := \mathrm{Hom}(G, S^1)$ ($S^1 := \{z \in \mathbb{C}^\times : |z| = 1\}$) determines G (as long as G is locally compact; Pontryagin duality). Taking G to be the Galois group of the maximal abelian extension k^{ab} of a number field k, we get exact description of $\mathrm{Gal}(k^{ab}/k)$ (Class field theory).

If G is non-abelian, there is no-character group; though from the category Tan_G of all representation of G, we can recover an algebraic group G as its automorphism group basically fixing one point and preserving tensor product (Tannakian theory). This is not very useful as the category is too big if G is big (like Galois group Gal($\overline{\mathbb{Q}}/\mathbb{Q}$))? Though the motivic Galois group (far bigger than Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)) is made this way (largely conjectural; Theory of motives).

Therefore we somehow want to fix dimension of representations, and somehow we want to know the collection of all representation reducing to a fixed small one (deformation theory), and from that information, try to see the group?

§**0.0. Set-up in abelian case.** We describe the universal deformation ring for representations (characters) into GL_1 and introduce invariants to compute it.

We fix an odd prime p (and later move p). Fix a finite extension $\mathbb{F}/\mathbb{F}_p$ and a local p-profinite noetherian ring B flat over $\mathbb{Z}_p$ with residue field $\mathbb{F}$. Let $\boxed{\mathcal{C} = \mathcal{C}_B}$ be either the category of artinian local B-algebra with residue field $\mathbb{F}$ or just p-profinite local B-algebra with residue field $\mathbb{F}$ (this category is denoted by CL_B). Morphisms of $\mathcal{C}$ is a local B-algebra homomorphism.

Let k be a base field (a finite extension of $\mathbb{Q}$) with integer ring O. We take a Galois extension K/k over its Galois group G we consider deformation. For a representation $\rho : G \to \mathrm{GL}_n(A)$, we write $F(\rho) := K^{\mathrm{Ker}(\rho)}$ (splitting field).

$\S$**0.1. Deformation of a character.** The smallest (unique) choice of the base ring B is the discrete valuation ring $W = W(\mathbb{F})$ unramified over $\mathbb{Z}_p$ with residue field $\mathbb{F}$ (Witt vector ring with coefficients in $\mathbb{F}$), or you can choose a bigger one $W(\mathbb{F})[\mu_{p^r}]$ adding p^r-th roots of unity or the Iwasawa algebra $\Lambda = W[[T]]$.

We fix the origin; i.e., the starting continuous character $\overline{\rho} : G \to \mathrm{GL}_1(\mathbb{F})$. A deformation into $\mathrm{GL}_2(A)$ ($A \in \mathcal{C}$) over G is a **continuous** character $\rho_A : G \to \mathrm{GL}_1(A)$ such that $\rho_A \bmod \mathfrak{m}_A = \overline{\rho}$.

The (full) deformation (covariant) functor $\mathcal{D} : G \to \mathrm{GL}_1(A)$

$$\mathcal{D}(A) = \{\rho_A : G \to \mathrm{GL}_1(A) | \rho_A \bmod \mathfrak{m}_A = \overline{\rho}\}.$$

If $\phi \in \mathrm{Hom}_{\mathcal{C}}(A, A')$, $\rho_A \mapsto \phi \circ \rho_A$ induces covariant functoriality. We fix a set $\mathcal{P}$ of properties of Galois characters. A deformation ρ_A is called *$\mathcal{P}$-deformation* if ρ_A satisfies $\mathcal{P}$.

§**0.2. Examples of $\mathcal{P}$:**

• Unramfied everywhere (full deformation for the maximal K/k unramified everywhere);

• Unramified outside p (full deformation if we take K to be the maximal p-profinite extension of $F(\overline{\rho})$ unramified outside p);

• Unramified outside S for a fixed finite set S of places of k (full deformation if we take K to be the maximal p-profinite extension of $F(\overline{\rho})$ unramified outside S);

• Suppose that $\overline{\rho}$ is ramified at S outside p with ramification index prime to p. A deformation ρ_A is *minimal* if $\rho_A(I_l) \cong \overline{\rho}(I_l)$ by restriction for all $l \neq p$, where $I_l \subset G$ is the inertia subgroup.

The minimal deformation problem is a full deformation problem if we choose K as follows: Take $K = F^{(p)}(\overline{\rho})$ to be the maximal p-profinite extension of $F(\overline{\rho})$ unramified outside p. Since ramification of a minimal deformation ρ_A is concentrated to $F(\overline{\rho})/k$, ρ_A factors through $G = \mathrm{Gal}(G/k)$; so, our choice is this K.

§0.3. Universal-deformation of a character.

A couple $(R, \boldsymbol{\rho})$ (universal couple) made of an object R of $\mathcal{C}$ (or pro-category CL_B of $\mathcal{C}$) and a character $\boldsymbol{\rho} : G \to R^\times$ satisfying $\mathcal{P}$ is called a *universal couple* for $\overline{\rho}$

if for any $\mathcal{P}$-deformation $\rho : G \to A^\times$ 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 $\phi_\rho \circ \boldsymbol{\rho} = \rho$.

Thus $\mathcal{D}(A) \cong \mathrm{Hom}_{\mathcal{C}}(R, A)$ by $\rho_A = \phi \circ \boldsymbol{\rho} \leftrightarrow \phi \in \mathrm{Hom}_{\mathcal{C}}(R, A)$, and R (pro-)represents the functor $\mathcal{D}$. By the universality, if exists, the couple $(R, \boldsymbol{\rho})$ is determined uniquely up to isomorphisms.

All deformation functor listed in §0.2 is represented by $(B[[G_p^{ab}]], \boldsymbol{\rho})$ defined in the following section. Does the ring $B[[G_p^{ab}]]$ determine explicitly the group G_p^{ab}? and if yes, how?

§0.4. Group algebra is universal. Let G_p^{ab} be the maximal p-profinite abelian quotient $G_p = \varprojlim_n (G^{ab}/p^n G^{ab})$ for $G^{ab} = G/\overline{[G,G]}$. Consider the group algebra $B[[G_p^{ab}]] = \varprojlim_n B[\mathcal{G}_n]$ writing $G_p^{ab} = \varprojlim_n \mathcal{G}_n$ with finite $\mathcal{G}_n$.

Since $\mathbb{F}^\times \hookrightarrow B^\times$, we may regard $\overline{\rho}$ as a character $\rho_0 : \mathcal{G} \to B^\times$ (Teichmüller lift of $\overline{\rho}$). Define $\boldsymbol{\rho} : G \to B[[G_p^{ab}]]^\times$ by $\boldsymbol{\rho}(g) = \rho_0(g) g_p$ for the image g_p of g in G_p^{ab}. Note that $B[G_n^{ab}]$ is a local ring with residue field $\mathbb{F}$; so, is $B[[G_p^{ab}]]$.

If $A = \varprojlim_n A_n$ for finite A_n with $A_n = A/\mathfrak{m}_n$, $\rho_n := \rho_A \rho_0^{-1} \bmod \mathfrak{m}_n : G \to A_n^\times$ has to factor through $\mathcal{G}_{m(n)}$ for some $m(n)$ by continuity, and we get $\varphi_n \in \mathrm{Hom}(B[\mathcal{G}_{m(n)}], A_n)$ given by $\sum_g a_g g \mapsto \sum_g a_g \rho_n \chi_0^{-1}(g) \in A$. Then $\varphi_n \circ \boldsymbol{\rho} = \rho_n$. Passing to the limit, we have $\varphi \circ \boldsymbol{\rho} = \rho_A$ for $\varphi = \varprojlim_n \varphi_n : B[[G_p^{ab}]] \to A$.

§0.5. Example of group algebras.

• If G_p^{ab} is a cyclic group C of order p^r, $B[G_p^{ab}] = B[T]/(t^{p^r} - 1)$ for $t = 1 + T$ by sending a generator $g \in C$ to t.

• If $G_p^{ab} = C_1 \times \cdots \times C_n$ for p-cyclic groups C_j with order p^{r_j}, then

$$B[G_p^{ab}] = \frac{B[T_1, \ldots, T_n]}{(t_1^{p^{r_1}} - 1, \ldots, t_n^{p^{r_n}} - 1)} = \frac{B[[T_1, \ldots, T_n]]}{(t_1^{p^{r_1}} - 1, \ldots, t_n^{p^{r_n}} - 1)} \; (t_i = 1+T_i).$$

Note that $f_1 := t^{p^{r_1}} - 1, \ldots, f_r := t^{p^{r_n}} - 1$ in $\mathfrak{m}_{B[[T_1,\ldots,T_n]]}$ is a regular sequence, and $B[G_p^{ab}]$ is free of finite rank over B. A ring of the form $B[[T_1, \ldots, T_n]]/(f_1, \ldots, f_n)$ with regular sequence (f_j) in $\mathfrak{m}_{B[[T_1,\ldots,T_n]]}$ is called a *local complete intersection* over B if it is free of finite rank over B.

• The Iwasawa algebra $\Lambda = W[[\Gamma]]$ ($\Gamma = 1 + p\mathbb{Z}_p = (1 + p)^{\mathbb{Z}_p}$) is isomorphic to $W[[T]]$ by $1 + p \leftrightarrow t = 1 + T$.

We now explore an arithmetic expression of the universal ring.

§0.6. Ray class groups of finite level.

Fix an O-ideal $\mathfrak{c}$. Recall

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

Here $\alpha \equiv 1 \bmod^\times \mathfrak{c}\infty$ means that $\alpha = a/b$ for $a, b \in O$ with $(b)+\mathfrak{c} = O$ is totally positive and $a \equiv b \mod \mathfrak{c}$. Removing the condition "∞", we define Cl_k. Passing to the limit, write

$$Cl_k^+(\mathfrak{c}p^\infty) = \varprojlim_n Cl_k^+(\mathfrak{c}p^n).$$

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

§0.7. Ray class group of infinite level.

The group $Cl_k^+(\mathfrak{c}p^n)$ is finite as we have an exact sequence:

$$(O/\mathfrak{c}p^n)^\times \xrightarrow[i]{\alpha\mapsto(\alpha)} Cl_k^+(\mathfrak{c}p^n) \to Cl_k \to 1.$$

Note $|Cl_k^+|/|Cl_k| \Big| 2^e$ $(e = |\mathrm{Isom}_{\mathrm{field}}(k,\mathbb{R})|$. Passing to the limit,

$$O_p^\times \times (O/\mathfrak{c})^\times \xrightarrow[i]{\alpha\mapsto(\alpha)} Cl_k^+(\mathfrak{c}p^\infty) = \varprojlim_n Cl_k^+(\mathfrak{c}p^n) \to Cl_k \to 1$$

Then for $H_{\mathfrak{c}p^\infty} = \bigcup_n H_{\mathfrak{c}p^n}$, $Cl_k^+(\mathfrak{c}p^\infty) \cong \mathrm{Gal}(H_{\mathfrak{c}p^\infty}/k)$ by $[\mathfrak{l}] \mapsto \mathrm{Frob}_{\mathfrak{l}}$ for primes $\mathfrak{l} \nmid \mathfrak{c}p$.

- Image of $\mathfrak{l}$-component of i is the $\mathfrak{l}$-inertia subgroup of $\mathrm{Gal}(H_{\mathfrak{c}p^n}/k)$.

If $k = \mathbb{Q}$ 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 $Cl_{\mathbb{Q}}(\mathfrak{c}p^\infty) \cong (\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p^\times$.

§0.8. Universal deformation ring for a Galois character $\overline{\rho}$. Let $C_k(p^\infty)$ (resp. C_k) for the maximal p-profinite quotient of $Cl_k^+(p^\infty)$ (resp. Cl_k^+). Suppose $\overline{\rho}$ is minimal, and let $G = \mathrm{Gal}(K/k)$ for $K = F^{(p)}(\overline{\rho})$. we consider minimal deformations ρ_A. Since ramification outside l has index prime to p, we conclude $G_p^{ab} = C_k(p^\infty)$. Let $H_\infty \subset H_{p^\infty}$ with $\mathrm{Gal}(H_\infty/k) = C_k(p^\infty)$. If $k = \mathbb{Q}$, $C_k(p^\infty) = 1 + p\mathbb{Z}_p =: \Gamma$ and $H_\infty = \mathbb{Q}_\infty \subset \mathbb{Q}[\mu_{p^\infty}]$ for the unique $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$ as $Cl_{\mathbb{Q}}^+(p^\infty) = \mathbb{Z}_p^\times$.

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

Theorem 1. *The couple $(W[[C_k(p^\infty)]], \boldsymbol{\rho})$ is universal among all minimal deformations. If $\overline{\rho}$ is unramified everywhere, $(W[C_k], \boldsymbol{\rho})$ is universal among everywhere unramified deformations.*

§0.9. Some remarks.

• As long as $\overline{\rho}$ satisfies minimality, the universal deformation ring $W[[C_k(p^\infty)]]$ is essentially independent of $\overline{\rho}$ (its dependence is the coefficient ring W.

• If k is totally real, $\mathrm{rank}_{\mathbb{Z}_p} C_p(p^\infty)$ is expected to be 1 (Leopoldt conjecture).

• More generally, if k has r_1 real places and r_2 complex places, then $\mathrm{rank}_{\mathbb{Z}_p} C_k(p^\infty) = r_2 + 1$? (Leopoldt conjecture).

• If $k = \mathbb{Q}$, $C_{\mathbb{Q}}(p^\infty) = \Gamma$, so

$$W[[C_{\mathbb{Q}}(p^\infty)]] = \varprojlim_n W[\Gamma/\Gamma^{p^n}] = \varprojlim_n W[[T]]/(t^{p^n} - 1) = W[[T]].$$

Iwasawa algebra again shows up. In general, if $C_k = \{1\}$ and $C_k(p^\infty) \cong \mathbb{Z}_p^{r_2+1}$, then $W[[C_k(p^\infty)]] \cong W[[T_1, \ldots, T_{r_2+1}]]$.

We now introduce some ring invariants C_0 and C_1 to recover the group G_p^{ab} out of the ring $B[[G_p^{ab}]]$.

§**0.10. Differentials.** Fix $R \in \mathcal{C}$. For a continuous R-module M, define continuous B-derivations by

$$Der_B(R,M) := \Big\{\delta \in \mathrm{Hom}_B(R,M) \Big| \delta(ab) = a\delta(b) + b\delta(a)\ (a,b \in R)\Big\}.$$

Here B-linearity of $\delta \Leftrightarrow \delta(B) = 0$. The association $M \mapsto Der_B(R,M)$ is a covariant functor from the category $MOD_{/R}$ of continuous profinite R-modules to modules MOD, which is represented by an R-module $\Omega_{R/B}$ with universal differential $d : R \to \Omega_{R/B}$, e.g.,

$$\Omega_{R/B} = \frac{\text{free module over } R \text{ with basis } dr\ (r \in R)}{\langle\langle d(ab) - bda - adb, d(\beta a + b) - \beta da - db\rangle\rangle_{a,b\in R,\beta\in B}}.$$

Here "$\langle\langle ? \rangle\rangle$" means the $\mathfrak{m}_R$-adic closure of the R-submodule generated by "?".

§0.11. When R is a B-module of finite type.

Suppose that B is noetherian and that R is a B-module of finite type. Choose $r_1, \ldots, r_n$ so that $R = Br_1 + \cdots + Br_n$. Then by B-linearity, $\Omega' := \bigoplus_{r \in R} R \cdot dr / \langle d(\beta a + b) - \beta da - db \rangle_{a,b \in R}$ is generated by $dr_1, \ldots, dr_n$; so, $\langle\langle d(ab) - bda - adb \rangle\rangle_{a,b \in R, \beta \in B} \subset \Omega'$ is equal to $\langle d(ab) - bda - adb \rangle_{a,b \in R, \beta \in B}$ inside Ω'. Therefore we can replace $\langle\langle ? \rangle\rangle$ by $\langle ? \rangle$ in the definition of $\Omega_{R/B}$ for B noetherian and R of finite type as B-modules. In this case, by B-linearity, any B-derivation $\delta : R \to M$ is actually continuous.

By this, $\Omega_{B[[T]]/B} = B[[T]]dT$ and for $f = f(T) \in B[[T]]$,

$$\Omega_{(B[[T]]/(f))/B} = (B[[T]]/(f, f'))dT = B[\theta]/(f'(\theta))$$

with $f'(T) = \frac{df}{dT}(T)$ and $B[[T]] \ni T \mapsto \theta := (T \bmod (f)) \in B[[T]]/(f)$.

§**0.12. Congruence modules C_0 and C_1.** Let $\phi : R \twoheadrightarrow A \in \mathrm{Hom}_{\mathcal{C}}(R, A)$. We define $\boxed{C_1(\phi; A) := \Omega_{R/B} \otimes_{R,\phi} A}$. To define C_0, we assume (i) $A = B$, (ii) B is a domain and (iii) $R \cong B^r$ as B-modules. The total quotient ring Frac(R) can be decomposed

$$\mathrm{Frac}(R) = \mathrm{Frac}(\mathrm{Im}(\phi)) \oplus X \quad \text{(unique algebra direct sum).}$$

Write 1_ϕ for the idempotent of Frac(Im(ϕ)) in Frac(R). Let $\mathfrak{b} = \mathrm{Ker}(R \to X) = (1_\phi R \cap R)$, $S = \mathrm{Im}(R \to X)$ 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 $\mathfrak{b} = R \cap (B \times 0)$ and $\mathfrak{x} = (0 \times X) \cap R$. Put

$$C_0 = C_0(\phi; B) := (R/\mathfrak{b}) \otimes_{R,\phi} \mathrm{Im}(\phi) \text{ and } C_1 := \Omega_{R/B} \otimes_R B.$$

The module C_j is called the *congruence* module (of degree j) of ϕ. Note: $C_0 = \mathrm{Im}(\phi)/(\phi(\mathfrak{a})) \cong A/\mathfrak{a} \cong R/(\mathfrak{a} \oplus \mathfrak{b}) \cong S/\mathfrak{b}$ via projection to B and S (an exercise).

§0.13. Higher congruence modules.

Suppose $\phi : R \to A$ is onto. We know $C_0 = S/\mathfrak{b}$ and we can prove $C_1 = \mathfrak{b}/\mathfrak{b}^2$ under (i)–(iii) by the second fundamental exact sequence:

$$\mathfrak{b}/\mathfrak{b}^2 \xrightarrow{b \mapsto db} \Omega_{R/B} \otimes_R A \to \Omega_{A/B} \to 0.$$

So why not we define $C_n := \mathfrak{b}^n/\mathfrak{b}^{n+1}$. Then $\mathrm{gr}(S) = \bigoplus_j C_j$ is the graded algebra. Knowledgeof $gr(S)$ is almost equivalent to the knowledge of S. Once we know S, we recover

$$R = B \times_{C_0} S = \{(b,s) \in B \times S | b \mod \mathfrak{a} = s \mod \mathfrak{b}\}.$$

If $C_1 = \mathfrak{b}/\mathfrak{b}^2$ is generated by one element over B, then by Nakayama's lemma, $\mathfrak{b} = (\theta)$ for a non-zero-divisor $\theta \in S$. Then $\mathrm{gr}(S) \cong C_0[x]$ by sending $\theta \mod \mathfrak{b}^2$ to the variable x.

What is S if $B = W$ and $C_0 = \mathbb{F}$?

Is there any good way to compute C_n when R is the universal deformation ring?

§0.14. Explicit form of $C_1(\pi;\mathbb{F})$ as cotangent space. Write $\pi : R \to R/\mathfrak{m}_R = \mathbb{F}$ for the projection. Let $\mathbb{F}[\varepsilon] = \mathbb{F}[x]/(x^2)$ with $x \leftrightarrow \varepsilon$. Then $\varepsilon^2 = 0$.

For $\phi \in \mathrm{Hom}_{B\text{-alg}}(R, \mathbb{F}[\varepsilon])$, write $\phi(a) = \pi(a) + \delta(a)\varepsilon$. From

$$\phi(ab) = \pi(a)\pi(b) + \pi(a)\delta(b)\varepsilon + \pi(b)\delta(a)\varepsilon,$$

we find $\mathrm{Hom}_{B\text{-alg}}(R, \mathbb{F}[\varepsilon]) = Der_B(R, \mathbb{F})$ by $\phi \leftrightarrow \delta$.

ϕ is determined by $\phi|_{\mathfrak{m}_R}$ which kills $\mathfrak{m}_R^2 + \mathfrak{m}_B$ as $\varepsilon^2 = 0$. Thus

$$\mathrm{Hom}_{\mathbb{F}}(\Omega_{R/B} \otimes_R \mathbb{F}, \mathbb{F}) \cong \mathrm{Hom}_R(\Omega_{R/B}, \mathbb{F}) \cong Der_B(R, \mathbb{F}) = \mathrm{Hom}_R(t^*_{R/B}, \mathbb{F}),$$

for $t^*_{R/B} := \mathfrak{m}_R/(\mathfrak{m}_R^2 + \mathfrak{m}_B)$. Taking $\mathbb{F}$-dual, if $t^*_{R/B}$ is finite dimensional, we get $\boxed{\Omega_{R/B} \otimes_R \mathbb{F} \cong t^*_{R/B}}$; in particular, $\Omega_{R/B}$ is an R-module of finite type (by Nakayama's lemma).

§0.15. Congruence modules for group algebras.

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

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

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

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

§**0.16. Theorem.** Suppose B is an integral domain with characteristic 0 Frac(B). We have

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

Proof for the congruence module.

Let $K :=$ Frac(B). 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 $\mathfrak{a} = K\varepsilon \cap B[H] = (\sum_{\sigma \in H} \sigma)$ and $\pi(B(H))/\mathfrak{a} = (\varepsilon)/\mathfrak{a} \cong B/|H|B$.

§0.17. Proof of $C_1(\pi; B) = H \otimes_{\mathbb{Z}} B$, 1st step.

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

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

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

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 $x, y \in X$.

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 $u'_\rho : H \to X$.

§0.18. Proof, Second step.

Since

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

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

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

§0.19. Proof, Third step.

Any B-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, $d_\xi \in Der_B(R, X)$. By universality of $(R, \boldsymbol{\rho})$, we have

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

§0.20. Proof, Fourth step, Yoneda's lemma.

Thus we have

$$\begin{aligned}\mathrm{Hom}_B(H \otimes_{\mathbb{Z}_p} \mathbb{Z}_p, X) &= \mathrm{Hom}(H, X) \\ &= \mathrm{Hom}_R(\Omega_{R/B}, X) \\ &= \mathrm{Hom}_B(\Omega_{R/B} \otimes_{R,\pi} B, X).\end{aligned}$$

This is true for all X, we have (essentially by Yoneda's lemma)

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

§0.21. Class group and Selmer group.

For simplicity, assume $p \nmid [k : \mathbb{Q}]$ and that $k/\mathbb{Q}$ is a Galois extension. Note that $K/\mathbb{Q}$ is a Galois extension as K is the maximal p-profinite extension of k unramified outside p. Let $\mathrm{Ind}_k^{\mathbb{Q}}\,\mathrm{id} = \mathrm{id} \oplus \chi$ and $H = C_k$. Then for Ω_k given basically by the regulator and some power of $(2\pi i)$,

$$|L(1,\chi)/\Omega_k|_p = \Big||C_k|\Big|_p.$$

We can identify $C_k^\vee = \mathrm{Hom}(C_k, \mathbb{Q}_p/\mathbb{Z}_p)$ with the Selmer group of χ given by $\mathrm{Sel}_k(1) := \mathrm{Ker}(H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \to \prod_{\mathfrak{p}|p} H^1(I_{\mathfrak{p}}, \mathbb{Q}_p/\mathbb{Z}_p))$

$$\mathrm{Sel}_k(1) \overset{\text{Shapiro}+\alpha}{=} \mathrm{Sel}_{\mathbb{Q}}(\chi) := \mathrm{Ker}(H^1(K/\mathbb{Q}, V(\chi)^*) \to H^1(I_p, V(\chi)^*))$$

for the $\mathfrak{p}$-inertia group $I_{\mathfrak{p}} \subset G$ and the p-inertia group $I_p \subset \mathrm{Gal}(K/\mathbb{Q})$.

§0.22. Class number formula.

Theorem 2 (Class number formula)**.** *For the augmentation homomorphism* $\pi : \mathbb{Z}_p[C_k] \to \mathbb{Z}_p$*,*

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

and $C_1(\pi;\mathbb{Z}_p) = \Omega_{\mathbb{Z}_p[C_k]/\mathbb{Z}_p} \otimes_{\mathbb{Z}_p[C_k]} \mathbb{Z}_p = C_k$ *and* $C_0(\pi;\mathbb{Z}_p) = \mathbb{Z}_p/|C_k|\mathbb{Z}_p$*.*

Is there any way of proving the above class number formula without using the classical ideal theory of integer ring of k but the Galois deformation theory?

There are three incarnations of C_k as the p-primary part of the class group (field arithmetic), as the Galois group of the maximal abelian unramified extension (Galois theory), and as a Selmer group (Cohomology theory)

§0.23. What we study in the next few weeks.

Hereafter $k = \mathbb{Q}$ and $B = W, \Lambda$ Fix a 2-dimensional continuous *odd* representation $\overline{\rho} = \rho_{\mathbb{F}}$: Gal$(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ ramified at finitely many primes. Take the maximal p-profinite extension $F^{(p)}(\overline{\rho})$ unramified outside p, and let $G = \mathrm{Gal}(F^{(p)}(\boldsymbol{\rho})/\mathbb{Q})$. We consider the functor roughly defined

$$\mathcal{D}(A) := \{\rho_A : G \to \mathrm{GL}_2(A) | \rho_A \text{ mod } \mathfrak{m}_A = \overline{\rho}, \text{ (ord), (min)}\}/\Gamma(\mathfrak{m}_A).$$

$$\mathcal{D}_\chi(A) := \{\rho_A \in \mathcal{D}(A) | \text{(det)}\}/\Gamma(\mathfrak{m}_A).$$

Here $\Gamma(\mathfrak{m}_A) = \mathrm{Ker}(\mathrm{GL}_2(A) \to \mathrm{GL}_2(\mathbb{F}))$ acts by conjugation,

(min) ρ_A is a minimal deformation.

(ord) $\rho_A|_{D_p} \cong \begin{pmatrix} \epsilon_A & * \\ 0 & \delta_A \end{pmatrix}$ with δ_A mod $\mathfrak{m}_A = \delta_{\mathbb{F}}$ and δ unramified.

(det) $\det(\rho_A) = \chi$, where χ is often of the form $\nu_p^{k-1}\psi$ for the p-adic cyclotomic character ν_p and a finite order character ψ.

§**0.24. Cases of the Bloch-Kato conjecture (BKC).** Usually $\mathcal{D}_\chi$ ($\chi = \nu_p^{k-1}\psi, B = W$) is represented by the (unique) local ring $\mathbb{T}_\chi$ of the Hecke algebra $\mathbf{h}_k(\psi)$ associated to $\overline{\rho}$ acting on $S_k(\psi) := S_k(\Gamma_0(N), \psi; W)$ for the conductor N of ψ. Given odd $\overline{\rho}$, $\mathbb{T}_\chi$ always exists by Khare–Wintenberger. Here

$$\mathbf{h}_k(\psi) := W[T(n)|n = 1, 2, \dots] \subset \mathrm{End}_W(S_k(\psi))$$

for the Hecke operators $T(n)$. If $\phi : \mathbb{T}_\chi \to W$ is given by $f|T(n) = \phi(T(n))f$ for a cusp form f and its p-adic Galois representation ρ_f, we describe the identities $\boxed{C_1 \cong \mathrm{Sel}(Ad(\rho_f))}$ (the adjoint Selmer group) and Adjoint class number formula:

$$|\mathrm{Sel}(Ad(\rho_f))| = |C_1| = |C_0| = \left|\frac{L(1, Ad(f))}{*}\right|_p^{-1} \qquad \text{(BKC)}$$

for an explicit constant $*$ independent of p if f has weight $k \geq 2$.

§**0.25. Some general goals and questions.** Fix $f \in S_{k_0}(\psi_0)$ with $f|T(n) = \phi(T(n))f$, and put $\chi_0 = \nu_p^{k_0-1}\psi_0$. The bigger functor $\mathcal{D}$ is represented by a local ring of the big "ordinary" Hecke algebra $\mathbb{T}$ free of finite rank over $\Lambda = W[[\Gamma]] = W[[T]]$ such that $\mathbb{T}/(t-\chi(\gamma)) \cong \mathbb{T}_\chi$ for all $\chi = \nu_p^{k-1}\psi$ of the form $\chi \equiv \chi_0$ as long as $k \geq 2$. Our goals in the coming few weeks are:

- Supposing $k \geq 2$, study $\mathbb{T}$ moving p for a fixed f_0, and try to prove that $\mathbb{T} = \Lambda$ if and only if $p \nmid L(1, Ad(f_0))/*$.

An obvious question is to ask

- What happens if $k_0 = 1$?

When $k_0 = 1$, ρ_{f_0} has finite image independent of p (an Artin Galois representation) by Deligne–Serre; so, it looks easier. However we do not know (BKC) and we need to deal with the p-adic value $L_p(Ad(f_0))$ for the p-adic L $L_p(Ad(f))$ interpolating $L(1, Ad(f))/*$ for f with different weight k; so, it depends on p.