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 $\text{GL}_n(A)$ 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 $\hat{G} := \text{Hom}(G, S^1)$ ($S^1 := \{z \in \mathbb{C}^\times : |z| = 1\}$) 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 $\text{Gal}(k^{ab}/k)$ (Class field theory).
If $G$ is non-abelian, there is no-character group; though from the category $\text{Tan}_G$ 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 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$)? Though the motivic Galois group (far bigger than $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) 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 $F/F_p$ and a local $p$-profinite noetherian ring $B$ flat over $\mathbb{Z}_p$ with residue field $F$. Let $C = C_B$ be either the category of artinian local $B$-algebra with residue field $F$ or just $p$-profinite local $B$-algebra with residue field $F$ (this category is denoted by $CL_B$). Morphisms of $C$ 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 $\rho : G \to GL_n(A)$, we write $F(\rho) := K^{\text{Ker}(\rho)}$ (splitting field).
§0.1. Deformation of a character. The smallest (unique) choice of the base ring \( B \) is the discrete valuation ring \( W = W(F) \) unramified over \( \mathbb{Z}_p \) with residue field \( F \) (Witt vector ring with coefficients in \( F \)), or you can choose a bigger one \( W(F)[\mu_{p^r}] \) adding \( p^r \)-th roots of unity or the Iwasawa algebra \( \Lambda = W[[T]] \).

We fix the origin; i.e., the starting continuous character \( \bar{\rho} : G \to \text{GL}_1(F) \). A deformation into \( \text{GL}_2(A) \) \((A \in \mathcal{O})\) over \( G \) is a continuous character \( \rho_A : G \to \text{GL}_1(A) \) such that \( \rho_A \mod m_A = \bar{\rho} \).

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

\[
D(A) = \{ \rho_A : G \to \text{GL}_1(A) | \rho_A \mod m_A = \bar{\rho} \}.
\]

If \( \phi \in \text{Hom}_\mathcal{O}(A, A') \), \( \rho_A \mapsto \phi \circ \rho_A \) induces covariant functoriality. We fix a set \( \mathcal{P} \) of properties of Galois characters. A deformation \( \rho_A \) is called \( \mathcal{P} \)-deformation if \( \rho_A \) satisfies \( \mathcal{P} \).
§0.2. Examples of \( \mathcal{P} \):

- **Unramfied everywhere** (full deformation for the maximal \( K/k \) unramfied everywhere);
- **Unramfied outside \( p \)** (full deformation if we take \( K \) to be the maximal \( p \)-profinite extension of \( F(\overline{\rho}) \) unramfied outside \( p \));
- **Unramfied 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 \( F(\overline{\rho}) \) unramfied outside \( S \));
- Suppose that \( \overline{\rho} \) is ramified at \( S \) outside \( p \) with ramification index prime to \( p \). A deformation \( \rho_A \) 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 \( F(\overline{\rho}) \) unramfied outside \( p \). Since ramification of a minimal deformation \( \rho_A \) is concentrated to \( F(\overline{\rho})/k \), \( \rho_A \) factors through \( G = \text{Gal}(G/k) \); so, our choice is this \( K \).
§0.3. **Universal-deformation of a character.**

A couple \((R, \rho)\) (universal couple) made of an object \(R\) of \(\mathcal{C}\) (or pro-category \(CL_B\) of \(\mathcal{C}\)) and a character \(\rho : G \rightarrow R^\times\) satisfying \(P\) is called a universal couple for \(\overline{\rho}\) if for any \(P\)-deformation \(\rho : G \rightarrow A^\times\) of \(\overline{\rho}\), we have a unique morphism \(\phi_\rho : R \rightarrow A\) in \(CL_W\) (so it is a local \(W\)-algebra homomorphism) such that \(\phi_\rho \circ \rho = \rho\).

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

All deformation functor listed in §0.2 is represented by \((B[[G_{ab}^p]], \rho)\) defined in the following section. *Does the ring \(B[[G_{ab}^p]]\) determine explicitly the group \(G_{ab}^p\)? and if yes, how?*
§0.4. **Group algebra is universal.** Let $G^a_b$ be the maximal $p$-profinite abelian quotient $G_p = \lim\limits_{\leftarrow} n (G^{ab}/p^n G^{ab})$ for $G^{ab} = G/[G,G]$. Consider the group algebra $B[[G^a_b]] = \lim\limits_{\leftarrow} n B[G_n]$ writing $G^a_b = \lim\limits_{\leftarrow} n G_n$ with finite $G_n$.

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

If $A = \lim\limits_{\leftarrow} n A_n$ for finite $A_n$ with $A_n = A/m_n$, $\rho_n := \rho_A \rho_0^{-1}$ mod $m_n : G \to A_n^\times$ has to factor through $G_{m(n)}$ for some $m(n)$ by continuity, and we get $\varphi_n \in \text{Hom}(B[G_{m(n)}], A_n)$ given by $\sum g a g g \mapsto \sum g a g \rho_n \chi_0^{-1}(g) \in A$. Then $\varphi_n \circ \rho = \rho_n$. Passing to the limit, we have $\varphi \circ \rho = \rho_A$ for $\varphi = \lim\limits_{\leftarrow} n \varphi_n : B[[G^a_b]] \to A$. 
§0.5. Example of group algebras.

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

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

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

Note that $f_1 := t^{p^{r_1}} - 1, \ldots, f_r := t^{p^{r_n}} - 1$ in $m_{B[[T_1, \ldots, T_n]]}$ is a regular sequence, and $B[G_{ab}^{p}]$ 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 $m_{B[[T_1, \ldots, T_n]]}$ 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.
Ray class groups of finite level.

Fix an $O$-ideal $c$. Recall

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

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

$$\text{Cl}_k^+(cp \infty) = \lim_{\leftarrow n} \text{Cl}_k^+(cp^n).$$

Write $H_{cp^n}/k$ for the ray class field modulo $cp^n$; i.e., a unique abelian extension $H_{cp^n}/k$ only ramified at $cp \infty$ such that we can identify $\text{Gal}(H_{cp^n}/k)$ with the strict ray class group $\text{Cl}_k^+(cp^n)$ by sending a class of prime $l$ in $\text{Cl}_k^+(cp^n)$ to the Frobenius element $\text{Frob}_l \in \text{Gal}(H_{cp^n}/k)$. This isomorphism is called the Artin symbol.
§0.7. Ray class group of infinite level.
The group $Cl_k^+(cp^n)$ is finite as we have an exact sequence:

$$(O/cp^n) \times \frac{\alpha \mapsto \alpha}{i} \to Cl_k^+(cp^n) \to Cl_k \to 1.$$ 

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

$$O_p^\times \times (O/c) \times \frac{\alpha \mapsto \alpha}{i} \to Cl_k^+(cp^\infty) = \lim_{n} Cl_k^+(cp^n) \to Cl_k \to 1$$

Then for $H_{cp^\infty} = \bigcup_n H_{cp^n}$, $Cl_k^+(cp^\infty) \cong \text{Gal}(H_{cp^\infty}/k)$ by $[l] \mapsto \text{Frob}_l$ for primes $l \nmid cp$.

- Image of $l$-component of $i$ is the $l$-inertia subgroup of $\text{Gal}(H_{cp^n}/k)$.

If $k = \mathbb{Q}$ and $c = (N)$ for $0 < N \in \mathbb{Z}$, we have $H_{cp^n}$ is the cyclotomic field $\mathbb{Q}[\mu_{Np^n}]$ for the group $\mu_{Np^n}$ of $Np^n$-th roots of unity; so, $Cl_{\mathbb{Q}}(cp^n) \cong (\mathbb{Z}/Np^n\mathbb{Z})^\times$ and $Cl_{\mathbb{Q}}(cp^\infty) \cong (\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p^\times$. 
\[0.8. \text{ Universal deformation ring for a Galois character } \overline{\rho}.\]

Let \(C_k(p^\infty)\) (resp. \(C_k\)) for the maximal \(p\)-profinite quotient of \(Cl_k^+(p^\infty)\) (resp. \(Cl_k^+\)). Suppose \(\rho\) is minimal, and let \(G = \text{Gal}(K/k)\) for \(K = F(p)(\overline{\rho})\). we consider minimal deformations \(\rho_A\). Since ramification outside \(l\) has index prime to \(p\), we conclude \(G^{ab}_p = C_k(p^\infty)\). Let \(H_\infty \subset H_{p^\infty}\) with \(\text{Gal}(H_\infty/k) = C_k(p^\infty)\).

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 \(\rho_0\) of \(\overline{\rho}\) and the inclusion \(\kappa : G^{ab}_p = C_k(p^\infty) \hookrightarrow W[[C_k(p^\infty)]]\), we define \(\rho(\sigma) := \rho_0(\sigma)\kappa(\sigma)\). Then the universality of the group algebra tells us

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

- As long as $\rho$ satisfies minimality, the universal deformation ring $W[[C'_k(p^\infty)]]$ is essentially independent of $\rho$ (its dependence is the coefficient ring $W$).
- If $k$ is totally real, $\operatorname{rank}_{\mathbb{Z}_p} C_p(p^\infty)$ is expected to be 1 (Leopoldt conjecture).
- More generally, if $k$ has $r_1$ real places and $r_2$ complex places, then $\operatorname{rank}_{\mathbb{Z}_p} C_k(p^\infty) = r_2 + 1$? (Leopoldt conjecture).
- If $k = \mathbb{Q}$, $C_{\mathbb{Q}}(p^\infty) = \Gamma$, so

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

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

$$\text{Der}_B(R, M) := \{ \delta \in \text{Hom}_B(R, M) \mid \delta(ab) = a\delta(b) + b\delta(a) \ (a, b \in R) \}.$$ 

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

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

By this, if $R$ is generated over $B$ by $r_1, \ldots, r_n$, $\Omega_{R/B}$ is an $R$-module generated by $dr_1, \ldots, dr_n$. So $\Omega_{B[[T]]/B} = B[[T]]dT$ and

$$\Omega_{(B[[T]])/(f))/B = (B[[T]])/(f,f')dT = B[\theta]/(f'(\theta)) \text{ for } f'(T) = \frac{df}{dT} \text{ and } B[[T]] \ni T \mapsto \theta \in B[[T]]/(f).$$
§0.11. Congruence modules $C_0$ and $C_1$. Let $\phi : R \to A \in \text{Hom}_C(R, A)$. We define $C_1(\phi; A) := \Omega_{R/B} \otimes_{R, \phi} A$. To define $C_0$, we assume (i) $A = B$, (ii) $B$ is a domain and (iii) $R \cong B'$ as $B$-modules. The total quotient ring $\text{Frac}(R)$ can be decomposed

$$\text{Frac}(R) = \text{Frac}(\text{Im}(\phi)) \oplus X$$

(unique algebra direct sum).

Write $1_\phi$ for the idempotent of $\text{Frac}(\text{Im}(\phi))$ in $\text{Frac}(R)$. Let $b = \text{Ker}(R \to X) = (1_\phi R \cap R)$, $S = \text{Im}(R \to X)$ and $b = \text{Ker}(\phi)$. Here the intersection $1_\phi R \cap R$ is taken in $\text{Frac}(R) = \text{Frac}(\text{Im}(\phi)) \times X$. First note that $b = R \cap (B \times 0)$ and $t = (0 \times X) \cap R$. Put

$$C_0 = C_0(\phi; B) := (R/b) \otimes_{R, \phi} \text{Im}(\phi)$$

and $C_1 := \Omega_{R/B} \otimes_{R} B$.

The module $C_j$ is called the congruence module (of degree $j$) of $\phi$. Note: $C_0 = \text{Im}(\phi)/(\phi(a)) \cong A/a \cong R/(a \oplus b) \cong S/b$ via projection to $B$ and $S$ (an exercise).
§0.12. 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:

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

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

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

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 $\text{gr}(S) \cong C_0[x]$ 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?
§0.13. Explicit form of $C_1(\pi; F)$ as cotangent space.
Write $\pi : R \to R/m_R = F$ for the projection. Let $F[\varepsilon] = F[x]/(x^2)$ with $x \leftrightarrow \varepsilon$. Then $\varepsilon^2 = 0$.

For $\phi \in \text{Hom}_{B\text{-alg}}(R, F[\varepsilon])$, 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 $\text{Hom}_{B\text{-alg}}(R, F[\varepsilon]) = \text{Der}_B(R, F)$ by $\phi \leftrightarrow \delta$.

$\phi$ is determined by $\phi|m_R$ which kills $m_R^2 + m_B$ as $\varepsilon^2 = 0$. Thus

$$\text{Hom}_F(\Omega_{R/B} \otimes_R F, F) \cong \text{Hom}_R(\Omega_{R/B}, F) \cong \text{Der}_B(R, F) = \text{Hom}_R(t^*_{R/B}, F),$$

for $t^*_{R/B} := m_R/(m_R^2 + m_B)$. Taking $F$-dual, if $t^*_{R/B}$ is finite dimensional, we get $\Omega_{R/B} \otimes_R F \cong t^*_{R/B}$; in particular, $\Omega_{R/B}$ is an $R$-module of finite type (by Nakayama’s lemma).
§0.14. Congruence modules for group algebras.
Let $H$ be a finite $p$-abelian group. If $m$ is a maximal ideal of $B[H]$, then for the inclusion $\kappa : H \hookrightarrow B[H]^\times$ with $\kappa(\sigma) = \sigma$, $\kappa \mod m$ is trivial as the finite field $B[H]/m$ has no non-trivial $p$-power roots of unity; so, $m$ is generated by $\{\sigma - 1\}_{h \in H}$ and $m_B$. Thus $m$ 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 \textit{augmentation} homomorphism of the group algebra. Write this map $\pi : B[H] \to B$. Then $b = \ker(\pi)$ is generated by $\sigma - 1$ for $\sigma \in H$. Thus

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

We compute the congruence module and the differential module $C_j(\pi, B)$ ($j = 0, 1$).
§0.15. **Theorem.** Suppose $B$ is an integral domain with characteristic 0 $\text{Frac}(B)$. 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 $K := \text{Frac}(B)$. Then $\pi$ 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 $a = K\varepsilon \cap B[H] = (\sum_{\sigma \in H} \sigma)$ and $\pi(B(H))/a = (\varepsilon)/a \cong B/|H|B.$
§0.16. **Proof of** $C_1(\pi; B) = H \otimes_{\mathbb{Z}} B$, **1st step.**

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

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

Thus $R := B[H]$ and the character $\rho : H \to B[H]$ (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 $\Phi(X) = \{\rho \in \mathcal{F}(R[X]) | \rho \mod X = \rho\}$. Write

$$\rho(\sigma) = \rho(\sigma) \oplus u^\prime_{\rho}(\sigma)$$

for $u^\prime_{\rho} : H \to X$. 
§0.17. Proof, Second step.

Since

$$\rho(\sigma \tau) \oplus u'_\rho(\sigma \tau) = \rho(\sigma \tau)$$

$$= (\rho(\sigma) \oplus u'_\rho(\sigma))(\rho(\tau) \oplus u'_\rho(\tau))$$

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

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

This shows

$$\text{Hom}(H, X) = \Phi(X).$$
§0.18. Proof, Third step.

Any $B$-algebra homomorphism $\xi : R \to R[X]$ with $\xi \mod X = \text{id}_R$ can be written as $\xi = \text{id}_R \oplus d_\xi$ 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, $d_\xi \in \text{Der}_B(R, X)$. By universality of $(R, \rho)$, we have

$$\Phi(X) \cong \{\xi \in \text{Hom}_{B\text{-alg}}(R, R[X]) | \xi \mod X = \text{id}\} = \text{Der}_B(R, X) = \text{Hom}_R(\Omega_{R/B}, X).$$
§0.19. Proof, Fourth step, Yoneda’s lemma.

Thus we have

\[ \text{Hom}_B(H \otimes_{\mathbb{Z}_p} \mathbb{Z}_p, X) = \text{Hom}(H, X) \]

\[ = \text{Hom}_R(\Omega_{R/B}, X) \]

\[ = \text{Hom}_B(\Omega_{R/B} \otimes_R \pi B, X). \]

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

\[ H \cong \Omega_{R/B} \otimes_R \pi B = C_1(\pi; B). \]
§0.20. **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 $\text{Ind}_k^{\mathbb{Q}} \text{id} = \text{id} \oplus \chi$ and $H = C_k$. Then for $\Omega_k$ given basically by the regulator and some power of $(2\pi i)$,

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

We can identify $C_k^\vee = \text{Hom}(C_k, \mathbb{Q}_p/\mathbb{Z}_p)$ with the Selmer group of $\chi$ given by $\text{Sel}_k(1) := \text{Ker}(H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \to \prod_p H^1(I_p, \mathbb{Q}_p/\mathbb{Z}_p))$

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

for the $p$-inertia group $I_p \subset G$ and the $p$-inertia group $I_p \subset \text{Gal}(K/\mathbb{Q})$. 
§0.21. Class number formula.

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

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

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)
§0.22. What we study in the next few weeks.
Hereafter $k = \mathbb{Q}$ and $B = W$, and fix a 2-dimensional continuous odd representation $\bar{\rho} = \rho_F : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{F})$ ramified at finitely many primes. Take the maximal $p$-profinite extension $F^{(p)}(\bar{\rho})$ unramified outside $p$, and let $G = \text{Gal}(F^{(p)}(\rho)/\mathbb{Q})$. We consider the functor roughly defined

$$D(A) := \{ \rho_A : G \to \text{GL}_2(A) | \rho_A \mod m_A = \bar{\rho}, \ (\text{ord}), \ (\text{min}) \}/\Gamma(m_A).$$

$$D_\chi(A) := \{ \rho_A \in D(A) | (\text{det}) \}/\Gamma(m_A).$$

Here $\Gamma(m_A) = \text{Ker}(\text{GL}_2(A) \to \text{GL}_2(\mathbb{F}))$ acts by conjugation,

- (min) $\rho_A$ is a minimal deformation.
- (ord) $\rho_A|_{D_p} \cong \begin{pmatrix} e_A^* & 0 \\ 0 & \delta_A \end{pmatrix}$ with $\delta_A \mod m_A = \delta_F$ and $\delta$ unramified.
- (det) $\det(\rho_A) = \chi$, where $\chi$ is often of the form $\nu_p^{k-1} \psi$ for the $p$-adic cyclotomic character $\nu_p$ and a finite order character $\psi$. 
§0.23. Cases of the Bloch-Kato conjecture (BKC). Usually $D_{\chi} (\chi = \nu_p^{k-1}\psi, B = W)$ is represented by the (unique) local ring $T_{\chi}$ of the Hecke algebra $h_k(\psi)$ associated to $\rho$ acting on $S_k(\psi) := S_k(\Gamma_0(N), \psi; W)$ for the conductor $N$ of $\psi$. Given odd $\overline{\rho}$, $T_{\chi}$ always exists by Khare–Wintenberger. Here

$$h_k(\psi) := W[T(n)|n = 1, 2, \ldots] \subset \text{End}_W(S_k(\psi))$$

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

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

for an explicit constant $\ast$ independent of $p$ if $f$ has weight $k \geq 2$. 
§0.24. 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 $D$ is represented by a local ring of the big “ordinary” Hecke algebra $\mathcal{T}$ free of finite rank over $\Lambda = W[[\Gamma]] = W[[T]]$ such that $\mathcal{T}/(t - \chi(\gamma)) \cong \mathcal{T}_\chi$ 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 $\mathcal{T}$ moving $p$ for a fixed $f_0$, and try to prove that $\mathcal{T} = \Lambda$ if and only if $p \nmid L(1, Ad(f_0))/\ast$. An obvious question is to ask
- **What happens if $k_0 = 1$?**

When $k_0 = 1$, $\rho_{f_0}$ 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 $L(1, Ad(f))/\ast$ for $f$ with different weight $k$; so, it depends on $p$. 