Start with an $n$-dimensional compatible system $\rho = \{\rho_l\}$ of $\mathcal{G}_K$. For simplicity, we assume that its coefficient field $T$ is $\mathbb{Q}$. Pick a prime $p$ and its member $\rho_p$ (since $\mathcal{G}_K$ is compact, $\rho_p$ has values in the maximal compact subgroup $GL_n(\mathbb{Z}_p)$ up to conjugation). Let $\bar{\rho} = \rho_p \mod p;\mathcal{G}_K \to GL_n(\mathbb{F}_p)$. A deformation $\varphi: \mathcal{G}_K \to GL_n(A)$ for a local $\mathbb{Z}_p$-algebra $A$ is such that $\varphi \mod m_A \cong \bar{\rho}$. The universal deformation ring with some specific property $P$ parameterizes all deformations with $P$. In other words, there exists a universal deformation $\rho: \mathcal{G}_K \to GL_n(R)$ with property $P$ such that for any deformation $\varphi$ as above, there exists a $\mathbb{Z}_p$-algebra homomorphism $\phi: R \to A$ such that $\phi \circ \rho \cong \varphi$. We study the relation between the module of differential $\Omega_{R/\mathbb{Z}_p}$ and a certain Selmer group $\text{Sel}_P(Ad(\rho))$. We start studying differentials for general rings.
§1.1. 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

\[
\text{Der}_A(R, M) = \left\{ \delta : R \to M \in \text{Hom}_A(R, M) \left| \begin{array}{c}
\delta: \text{continuous, } \delta(ab) = a\delta(b) + b\delta(a) \ (a, b \in R)
\end{array} \right. \right\}.
\]

Here the \( A \)-linearity of a derivation \( \delta \) is equivalent to \( \delta(A) = 0 \). The association \( M \mapsto \text{Der}_A(R, M) \) is a covariant functor from the category \( MOD/R \) of continuous \( R \)-modules to modules \( MOD \).
§1.2. Differentials.

The differential $R$-module $\Omega_{R/A}$ is defined as follows: The multiplication $a \otimes b \mapsto ab$ induces a $A$–algebra homomorphism $m : R \hat{\otimes}_A R \to R$ taking $a \otimes b$ to $ab$. We put $I = \text{Ker}(m)$, which is an ideal of $R \hat{\otimes}_A R$. 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

$$a \cdot d(b) + b \cdot d(a) - d(ab)$$

$$= ab \otimes 1 - a \otimes b - b \otimes a + ba \otimes 1 - ab \otimes 1 + 1 \otimes ab$$

$$= ab \otimes 1 - a \otimes b - b \otimes a + 1 \otimes ab = (a \otimes 1 - 1 \otimes a)(b \otimes 1 - 1 \otimes b) \equiv 0 \mod I^2.$$

• We have a morphism of functors:

$$\text{Hom}_R(\Omega_{R/A}, ?) \to \text{Der}_A(R, ?) : \phi \mapsto \phi \circ d.$$
§1.3. Universality.

Proposition 1. The above morphism of two functors

\[ M \mapsto \text{Hom}_R(\Omega_{R/A}, M) \]

and \( M \mapsto \text{Der}_A(R, M) \) 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 \( \delta = \phi \circ d \).

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

\[ \sum_{a,b} m(a, b)a \otimes b = \sum_{a,b} m(a, b)a \otimes b - \sum_{a,b} m(a, b)ab \otimes 1 \]

\[ = \sum_{a,b} m(a, b)a(1 \otimes b) - b \otimes 1) = -\sum_{a,b} m(a, b)d(b). \]
§1.4. Proof.
Define $\phi : R \times R \to M$ by $(x, y) \mapsto x\delta(y)$ for $\delta \in \text{Der}_A(R, M)$. 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 $\phi$ 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 $\phi : \hat{R} \otimes_A R \to M$. 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 $\phi$ is unique as $d(R)$ generates $\Omega_{R/A}$. $\square$
Corollary 1 (Second fundamental exact sequence).

Let $\pi : R \to C$ be a surjective morphism in $\mathcal{C}L_{W}$, and write $J = \text{Ker}(\pi)$. Then we have the following natural exact sequence:

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

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

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

Note that $C - MOD : M \to \text{Hom}_C(\Omega_{R/A} \hat{\otimes}_R C, M)$ represents $M \mapsto \text{Der}_A(R, M)$. 
§1.6. **Proof, First step.** By assumption, we have algebra morphism $A \to R \to C = R/J$. By the Yoneda’s lemma, we only need to prove that

$$\begin{align*}
    \text{Der}_A(C, M) & \xrightarrow{\alpha} \text{Der}_A(R, M) \xrightarrow{\beta} \text{Hom}_C(J/J^2, M) \\
    \text{Hom}_A(\Omega_{C/A}, M) & \to \text{Hom}_A(\Omega_{R/A} \hat{\otimes}_R C, M) \to \text{Hom}_C(J/J^2, M)
\end{align*}$$

is exact for all continuous $C$–modules $M$. The first $\alpha$ is the pull back map. Thus the injectivity of $\alpha$ is obvious.
§1.7. Proof, Second step.

The map $\beta$ 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 $\alpha$. 
§1.8. The case $A = C$.

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

Let $\pi : R \rightarrow C$ 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 $\delta : R \rightarrow J/J^2$ given by $\delta(a) = a - P(a) \mod J^2$ for $P = \iota \circ \pi$. Then

$$a\delta(b) + b\delta(a) - \delta(ab)$$

$$= a(b - P(b)) + b(a - P(a)) - ab + P(ab)$$

$$P(ab) = P(a)P(b) \Rightarrow ab - aP(b) + ba - bP(a) - ab + P(a)P(b)$$

$$= (a - P(a))(b - P(b)) \equiv 0 \mod J^2.$$
§1.9. Proof continues in the case $A = C$.
Thus $\delta$ 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 $\phi$ is surjective.

Since $J$ kills $J/J^2$, the surjection $\phi$ factors through $\Omega_{R/A} \otimes_R C$ and induces $\gamma$. Note that $\beta(d \otimes 1_C) = d \otimes 1_C|_J$ for the identity $1_C$ of $C$; so, $\gamma \circ \beta^* = \text{id}$ as desired. \qed
§1.10. 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 $R[M] \in \text{CNL}_W$, if $M$ is of finite type, and $R[M] \in \text{CL}_W$ if $M$ is a $p$-profinite $R$-module. By definition,

$$\text{Der}_A(R, M) \cong \left\{ \phi \in \text{Hom}_{A-\text{alg}}(R, R[M]) \mid \phi \mod M = \text{id} \right\},$$

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

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

as an algebra direct product. Write $1_\phi$ for the idempotent of $\text{Frac}(\text{Im}(\phi))$ in $\text{Frac}(R)$. Let $a = \text{Ker}(R \to X) = (1_\phi R \cap R)$, $S = \text{Im}(R \to X)$ 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 $a = R \cap (A \times 0)$ and $b = (0 \times X) \cap R$. Put

$$C_0(\phi; A) = (R/a) \otimes_{R, \phi} \text{Im}(\phi)$$

$$\cong \text{Im}(\phi)/(\phi(a)) \cong A/a \cong R/(a \oplus b) \cong S/b,$$

which is called the congruence module of $\phi$ but is actually a ring.
§1.12. Congruence proposition.

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

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

we conclude that

**Proposition 2.** 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 $R/a$ such that $\phi(a) \equiv \phi'(a) \mod \mathfrak{p}$ for all $a \in R$.

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