ANNALES

DE

L'INSTITUT FOURIER

Tadashi OCHIAI

Euler system for Galois deformations

Tome 55, n° 1 (2005), p. 113-146.

<http://aif.cedram.org/item?id=AIF_2005__55_1_113_0>

Ann. Inst. Fourier, Grenoble
55, 1 (2005), 113–146

EULER SYSTEM FOR GALOIS DEFORMATIONS

by Tadashi OCHIAI (*)

For a motive M over a number field, the relation between the size of the Selmer groups for M and the special values of L-function for M is one of the main theme of arithmetic geometry. In Iwasawa theory, we are interested in the relation between the Selmer group and the p-adic L-function for a Galois deformation of the p-adic realization of M. After original works by Iwasawa for ideal class groups in the cyclotomic tower, many people followed and generalized his philosophy to study elliptic curves, modular forms or more general p-adic representations in the cyclotomic tower. In early 90's, Greenberg [Gr2] proposed a vast generalization and reformulation of Iwasawa theory through Mazur's theory of deformations of Galois representations.

In this paper, we study the theory of Euler system for Galois deformations to bound the size of the Selmer group of a Galois deformation by the characteristic ideal of an Euler system. Such theory was first obtained by Kolyvagin and it has been developed by Kato, Perrin-Riou and Rubin in the case of cyclotomic deformations. However, the method of their theory does not work well for Galois representations over general deformation rings R. The difficulty comes from impossibility of finding nice system of Frobenius elements which reflects the R-module structure of the Selmer group except the case where R is the group algebra of a $\mathbb{Z}_p^d$-extension. Thus, the aim of this paper is to overcome these difficulties in Euler system theory over a more general deformation ring R such as a nearly ordinary Hecke algebra of Hida by introducing a new approach to the Euler system theory. As a corollary, we show one of the inequalities predicted by the two-variable Iwasawa main conjecture for a nearly ordinary Hida deformation. This

(*) The author is supported by Japan Society for Promotion of Science.
Keywords: Euler system, Hida theory, Iwasawa main conjecture.
Math. classification: 11G40, 11R23, 11R34, 11F80, 11F33.

is the first example of such inequality of the generalized Iwasawa Main conjecture proposed by Greenberg over a deformation ring which is not the group algebra of $\mathbb{Z}_p^d$-extension of a number field.

1. Two-variable Iwasawa main conjecture for Hida deformation.

In this section, we shall introduce our main result in the case of Hida deformations. To introduce our result, let us recall briefly Hida's nearly ordinary modular deformations.

We fix a prime number $p \geq 3$ and a norm compatible system $\{\zeta_{p^n}\}_{n\geq 1}$ of primitive p^n-th roots of unity throughout the paper. Let Γ be the Galois group $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$ of the rational number field $\mathbb{Q}$. We denote by Γ' the group of diamond operators for the tower of modular curves $\{Y_1(p^t)\}_{t\geq 1}$. We have the canonical isomorphisms

$$\Gamma \xrightarrow[\chi]{\sim} 1+p\mathbb{Z}_p \subset \mathbb{Z}_p^\times, \quad \Gamma' \xrightarrow[\chi']{\sim} 1+p\mathbb{Z}_p \subset \mathbb{Z}_p^\times.$$

Fix a topological generator γ (resp. γ') of Γ (resp. Γ'). From now on, we fix an embedding of an algebraic closure $\overline{\mathbb{Q}}$ into the field $\mathbb{C}$ of complex numbers and an embedding of $\overline{\mathbb{Q}}$ into a fixed algebraic closure $\overline{\mathbb{Q}}_p$ of the field $\mathbb{Q}_p$ of p-adic numbers simultaneously.

Let $\mathbb{H}_{\mathcal{F}}^{\mathrm{ord}}$ be the quotient of the universal ordinary Hecke algebra with certain fixed tame conductor, which corresponds to a certain Λ-adic eigen newform $\mathcal{F}$. The algebra $\mathbb{H}_{\mathcal{F}}^{\mathrm{ord}}$ is a local domain finite flat over $\mathbb{Z}_p[[\Gamma']]$. Hida's nearly ordinary Hecke algebra $\mathbb{H}_{\mathcal{F}}^{\mathrm{n.o}}$ is defined to be the formal tensor product of $\mathbb{H}_{\mathcal{F}}^{\mathrm{ord}}$ and the cyclotomic Iwasawa algebra $\mathbb{Z}_p[[\Gamma]]$ over $\mathbb{Z}_p$. By this, $\mathbb{H}_{\mathcal{F}}^{\mathrm{n.o}}$ is isomorphic to $\mathbb{H}_{\mathcal{F}}^{\mathrm{ord}}[[\Gamma]]$ and is a local domain finite flat over $\mathbb{Z}_p[[\Gamma\times\Gamma']]$.

In his celebrated paper [Hi1], Hida constructs a big Galois representation $\rho\colon G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\widetilde{T})$, where $\widetilde{T}$ is a finitely generated torsion-free module of generic rank two over $\mathbb{H}_{\mathcal{F}}^{\mathrm{n.o}}$. The representation $\widetilde{T}$ is presented as $\widetilde{T}^{\mathrm{ord}}\widehat{\otimes}\mathbb{Z}_p[[\Gamma]](\widetilde{\chi})$, where $\widetilde{\chi}$ is the universal cyclotomic character $G_{\mathbb{Q}} \twoheadrightarrow \Gamma \hookrightarrow \mathbb{Z}_p[[\Gamma]]^\times$ and $\mathbb{Z}_p[[\Gamma]](\widetilde{\chi})$ is a rank 1 free $\mathbb{Z}_p[[\Gamma]]$-module on which $G_{\mathbb{Q}}$ acts via the character $\widetilde{\chi}$. We always assume the following condition:

$$(\mathbf{F}) \qquad \begin{cases} \widetilde{T} \text{ is free of rank 2 over } \mathbb{H}_{\mathcal{F}}^{\mathrm{n.o}} \text{ and the residual representation} \\ \widetilde{T}/\mathfrak{M}\widetilde{T} \text{ of } \widetilde{T} \text{ is an irreducible } G_{\mathbb{Q}}\text{-module, where } \mathfrak{M} \text{ is the} \\ \text{maximal ideal of } \mathbb{H}_{\mathcal{F}}^{\mathrm{n.o}}. \end{cases}$$

We expect an equality between the ideal generated by the p-adic L-function and the characteristic ideal of the Selmer group for Hida deformation (Iwasawa Main Conjecture which will be proposed later). In this paper, we shall show one of the inequalities between these two objects under certain assumptions. In this section, we summarize briefly our main result in this paper (Theorem C) and apply it to the Iwasawa Main Conjecture by combining with our previous works (Theorem B).

Let us recall the following definition:

DEFINITION 1.1. — Let w be an integer. A point $\kappa \in \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{H}_{\mathcal{F}}^{\mathrm{ord}}, \overline{\mathbb{Q}}_p)$ is called *an arithmetic point of weight* w if there exists an open subgroup U of Γ' such that the restriction $\kappa_{|\mathbb{Z}_p[[\Gamma']]}\colon \mathbb{Z}_p[[\Gamma']] \longrightarrow \overline{\mathbb{Q}}_p$ sends u to ${\chi'}^w(u)$ for any $u \in U$. For an arithmetic point κ of $\mathbb{H}_{\mathcal{F}}^{\mathrm{ord}}$, we will denote by $w(\kappa)$ the weight of κ.

We briefly recall the properties of this Hida deformation $\widetilde{T}$ (cf. [Hi1], [Wi]):

Basic Property of Hida deformation. — Assume the condition (**F**). Hida's nearly ordinary deformation $\widetilde{T}$ has the following properties:

1) $\widetilde{T}$ is unramified outside a finite set of primes S of $\mathbb{Q}$ containing p and the archimedean prime.

2) Let $\widetilde{\chi}' : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_p[[\Gamma']]^{\times}$ be the universal character defined to be the composite

$$G_{\mathbb{Q}} \xrightarrow{\tilde{\chi}} \mathbb{Z}_p[[\Gamma]]^{\times} \xrightarrow{\sim} \mathbb{Z}_p[[\Gamma']]^{\times}$$

obtained by the canonical isomorphism $\Gamma \xrightarrow{\sim} \Gamma'$. Then the determinant representation $G_{\mathbb{Q}} \to \mathrm{Aut}(\overset{2}{\wedge} \widetilde{T}) \cong (\mathbb{H}_{\mathcal{F}}^{\mathrm{n.o}})^{\times}$ coincides with the character

$$G_{\mathbb{Q}} \xrightarrow{\chi^{-1}(\tilde{\chi}^2 \times \tilde{\chi}'^{-1})} \mathcal{O}[[\Gamma \times \Gamma']] \hookrightarrow (\mathbb{H}_{\mathcal{F}}^{\mathrm{n.o}})^{\times}$$

modulo a character of finite order.

3) For each pair (j, κ) of integer j and an arithmetic point $\kappa \in \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{H}_{\mathcal{F}}^{\mathrm{ord}}, \overline{\mathbb{Q}}_p)$ satisfying $1 \leq j \leq w(\kappa) + 1$, we denote by $T^{(j,\kappa)}$ the specialization of $\widetilde{T}$ by the homomorphism

$$\chi^{j-1} \circ \kappa\colon \mathbb{H}_{\mathcal{F}}^{\mathrm{n.o}} = \mathbb{H}_{\mathcal{F}}^{\mathrm{ord}}[[\Gamma]] \longrightarrow \kappa(\mathbb{H}_{\mathcal{F}}^{\mathrm{ord}})[[\Gamma]] \longrightarrow \overline{\mathbb{Q}}_p.$$

Then there exists a normalized eigen cusp form f_κ of weight $w(\kappa) + 2$ and $T^{(j,\kappa)}$ is the twist $T_{f_\kappa} \otimes \chi^j$ of Deligne's Galois representation T_{f_κ} associated to f_κ.

4) If we restrict the action of $G_{\mathbb{Q}}$ on $\widetilde{T}$ to the decomposition group $G_{\mathbb{Q}_p}$ at p, $\widetilde{T}$ has a filtration $0 \to \mathrm{F}^+\widetilde{T} \to \widetilde{T} \to \mathrm{F}^-\widetilde{T} \to 0$ such that the graded pieces $\mathrm{F}^+\widetilde{T}$ and $\mathrm{F}^-\widetilde{T}$ are free of rank 1 over $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$.

5) Further, the representation $\mathrm{F}^+\widetilde{T}$ is isomorphic to

$$\mathbb{Z}_p[[\Gamma]](\widetilde{\chi}) \mathbin{\widehat{\otimes}_{\mathbb{Z}_p}} \mathbb{H}^{\mathrm{ord}}_{\mathcal{F}}(\widetilde{\alpha})$$

as a $G_{\mathbb{Q}_p}$-module, where $\widetilde{\alpha}$ is an unramified character $G_{\mathbb{Q}_p} \to (\mathbb{H}^{\mathrm{ord}}_{\mathcal{F}})^\times$ such that $A_p = \widetilde{\alpha}(\mathrm{Frob}_p) \in \mathbb{H}^{\mathrm{ord}}_{\mathcal{F}}$ satisfies an interpolation property $\kappa(A_p) = a_p(f_\kappa)$ for each arithmetic point κ of $w(\kappa) \geq 0$ and $\mathbb{H}^{\mathrm{ord}}_{\mathcal{F}}(\widetilde{\alpha})$ is a rank one free $\mathbb{H}^{\mathrm{ord}}_{\mathcal{F}}$-module on which $G_{\mathbb{Q}_p}$ acts via the character $\widetilde{\alpha}$.

In order to consider p-tame twist of the representation $\widetilde{T}$ by a power of the Teichmuller character ω, we will consider the nearly ordinary deformation $\mathcal{T} = \widetilde{T} \otimes \omega^i$ for $0 \leq i \leq p-2$. Let $\mathcal{A}$ be the discrete Galois representation $\mathcal{T} \otimes_{\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}} \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}, \mathbb{Q}_p/\mathbb{Z}_p)$. We denote by $\mathbb{Q}_S$ the maximal Galois extension of $\mathbb{Q}$ which is unramified outside S. The Selmer group is defined as a subgroup of $H^1(\mathbb{Q}_S/\mathbb{Q}, \mathcal{A})$. Once we fix a local condition $H^1_?(\mathbb{Q}_p, \mathcal{A}) \subset H^1(\mathbb{Q}_p, \mathcal{A})$ at p, we define a Selmer group $\mathrm{Sel}^?_{\mathcal{T}}$ as follows:

$$\mathrm{Sel}^?_{\mathcal{T}} = \mathrm{Ker}\Big[H^1(\mathbb{Q}_S/\mathbb{Q}, \mathcal{A}) \to \prod_{\ell \in S, \ell \neq p} \frac{H^1(\mathbb{Q}_\ell, \mathcal{A})}{H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, \mathcal{A})} \times \frac{H^1(\mathbb{Q}_p, \mathcal{A})}{H^1_?(\mathbb{Q}_p, \mathcal{A})}\Big].$$

Let us consider two important types of local conditions ? = Gr or BK.

1) Greenberg's local condition $H^1_{\mathrm{Gr}}(\mathbb{Q}_p, \mathcal{A}) \subset H^1(\mathbb{Q}_p, \mathcal{A})$ is defined to be

$$H^1_{\mathrm{Gr}}(\mathbb{Q}_p, \mathcal{A}) = \mathrm{Ker}\big[H^1(\mathbb{Q}_p, \mathcal{A}) \to H^1(\mathbb{Q}_p^{\mathrm{ur}}, \mathrm{F}^-\mathcal{A})\big],$$

where $\mathbb{Q}_p^{\mathrm{ur}}$ is the maximal unramified extension of $\mathbb{Q}_p$.

2) Let (j,k) be a pair of integers satisfying $1 \leq j \leq k-1$ and let $\Phi^{(j,k)}_{s,t} \subset \mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$ be a height 2 ideal $(\gamma^{p^s} - \chi^{j-1}(\gamma^{p^s}), \gamma'^{p^t} - \chi'^{k-2}(\gamma'^{p^t}))$. We denote by $\mathcal{A}[\Phi^{(j,k)}_{s,t}]$ the $\Phi^{(j,k)}_{s,t}$-torsion part of $\mathcal{A}$, which is cofree of finite rank over $\mathbb{Z}_p$. We define a Bloch-Kato type local condition $H^1_{\mathrm{BK}}(\mathbb{Q}_p, \mathcal{A}) \subset H^1(\mathbb{Q}_p, \mathcal{A})$ to be

$$H^1_{\mathrm{BK}}(\mathbb{Q}_p, \mathcal{A}) = \varinjlim_{s,t} H^1_f\big(\mathbb{Q}_p, \mathcal{A}[\Phi^{(j,k)}_{s,t}]\big),$$

where $H^1_f(\mathbb{Q}_p, \mathcal{A}[\Phi^{(j,k)}_{s,t}]) \subset H^1(\mathbb{Q}_p, \mathcal{A}[\Phi^{(j,k)}_{s,t}])$ is the "finite part" defined by Bloch-Kato in their paper [BK] using Fontaine's ring of p-adic periods.

First, we recall the following result concerning these Selmer groups:

PROPOSITION A. — *Assume the condition* (**F**) *above. We have the following statements*:

1) *Two Selmer groups* $\mathrm{Sel}_{\mathcal{T}}^{\mathrm{BK}}$ *and* $\mathrm{Sel}_{\mathcal{T}}^{\mathrm{Gr}}$ *are equal as subgroups of* $H^1(\mathbb{Q}_S/\mathbb{Q},\mathcal{A})$. *Especially, the definition of* $\mathrm{Sel}_{\mathcal{T}}^{\mathrm{BK}}$ *does not depend on the choice of* (j,k) *as above.*

2) *The Pontryagin duals* $(\mathrm{Sel}_{\mathcal{T}}^{\mathrm{BK}})^{\vee}$ *and* $(\mathrm{Sel}_{\mathcal{T}}^{\mathrm{Gr}})^{\vee}$ *of our Selmer groups are torsion modules over* $\mathbb{H}_{\mathcal{F}}^{n.o}$.

The first statement of the above proposition is proved in [Oc2], §4. The second one is proved by a specialization of two variable Selmer group to a certain weight k and by the use of results of Kato and Rubin (cf. [Ka3] and [Ru1]) for cotorsion-ness of one-variable Selmer groups over the cyclotomic tower. For such specialization argument of Selmer group, see [Oc1]. By the above proposition, we will denote the Selmer group for $\mathcal{T}$ simply by $\mathrm{Sel}_{\mathcal{T}}$ no matter how it is Greenberg type or Bloch-Kato type.

Now we will relate the characteristic ideal of the above Selmer group to a two-variable p-adic L-function for Hida deformation by using an Euler system of Beilinson-Kato.

In order to introduce Beilinson-Kato elements, we need to prepare notations. For each arithmetic point κ of weight $w(\kappa) \geq 0$, we denote by

$$\overline{f}_{\kappa} = \sum_{n>0} a_n(f_{\kappa})^{\sigma} q^n$$

be the dual modular form of $f_{\kappa} = \sum_{n>0} a_n(f_{\kappa}) q^n$ where σ is a complex conjugation. The dual modular form $\overline{f}_{\kappa}$ is known to be a Hecke eigen cusp form of weight $k = w(\kappa)+2$ with Neben character dual of that of f_{κ}. We denote by $\mathbb{Q}_{\overline{f}_{\kappa}}$ a finite extension of $\mathbb{Q}$ obtained by adjoining all Fourier coefficients of $\overline{f}_{\kappa}$ to $\mathbb{Q}$. We associate the de Rham realization $V_{\mathrm{dR}}(\overline{f}_{\kappa})$ to $\overline{f}_{\kappa}$. The de Rham realization $V_{\mathrm{dR}}(\overline{f}_{\kappa})$ has the following properties:

1) $V_{\mathrm{dR}}(\overline{f}_{\kappa})$ is a 2 dimensional vector space over $\mathbb{Q}_{\overline{f}_{\kappa}}$ and is equipped with a de Rham filtration $\mathrm{Fil}^i V_{\mathrm{dR}}(\overline{f}_{\kappa}) \subset V_{\mathrm{dR}}(\overline{f}_{\kappa})$, which is a decreasing filtration of $\mathbb{Q}_{\overline{f}_{\kappa}}$-vector spaces.

2) We have $\mathrm{Fil}^0 V_{\mathrm{dR}}(\overline{f}_{\kappa}) = V_{\mathrm{dR}}(\overline{f}_{\kappa})$ and $\mathrm{Fil}^{w(\kappa)+2} V_{\mathrm{dR}}(\overline{f}_{\kappa}) = \{0\}$. For each j such that $1 \leq j \leq w(\kappa)+1$, $\mathrm{Fil}^j V_{\mathrm{dR}}(\overline{f}_{\kappa})$ is naturally identified with one-dimensional $\mathbb{Q}_{\overline{f}_{\kappa}}$-vector space $\mathbb{Q}_{\overline{f}_{\kappa}} \cdot \overline{f}_{\kappa}$.

3) For each j such that $1 \leq j \leq w(\kappa)+1$, $\mathrm{Fil}^{w(\kappa)+2-j} V_{\mathrm{dR}}(\overline{f}_{\kappa}) \otimes_{\mathbb{Q}_{\overline{f}_{\kappa}}} \widehat{\mathbb{Q}}_{\overline{f}_{\kappa}}$ is naturally identified with $\mathrm{Fil}^0 \mathrm{D}_{\mathrm{dR}}((V^{(j,\kappa)})^*(1))$, where $\widehat{\mathbb{Q}}_{\overline{f}_{\kappa}}$ is the p-adic

completion of $\mathbb{Q}_{\overline{f}_\kappa}$ in the fixed embedding $\mathbb{Q}_{\overline{f}_\kappa} \hookrightarrow \overline{\mathbb{Q}}_p$, $V^{(j,\kappa)}$ is $T^{(j,\kappa)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $(\ )^*$ means the $\mathbb{Q}_p$-linear dual here.

For each $1 \leq j \leq w(\kappa)+1$, we denote by $\overline{\delta}_\kappa^{\mathrm{dR}}$ the $\mathbb{Q}_{\overline{f}_\kappa}$-basis of $\mathrm{Fil}^{w(\kappa)+2-j} V_{\mathrm{dR}}(\overline{f}_\kappa)$ sent to $\overline{f}_\kappa$ under the natural identification

$$\mathrm{Fil}^{w(\kappa)+2-j} V_{\mathrm{dR}}(\overline{f}_\kappa) = \mathbb{Q}_{\overline{f}_\kappa} \cdot \overline{f}_\kappa.$$

Kato [Ka3] constructs elements in the K_2 of modular curves. By using his elements, we have the following system of elements in Galois cohomology.

Proposition 1.2 (see [Ka3]). — *Assume the condition* (**F**). *Let* $\mathcal{R}$ *be the set of all square-free natural numbers which are prime to* S. *Then we have a collection of elements* $\{\mathcal{Z}(r) \in H^1(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_r),\mathcal{T}^*(1))\}_{r\in\mathcal{R}}$ *satisfying the following properties*:

1) *The element* $\mathcal{Z}(r)$ *is unramified outside primes of* $\mathbb{Q}(\zeta_r)$ *over* S *for each* $r \in \mathcal{R}$. *Let* r *be a square-free number and let* q *be a prime number such that* $(r,q) = 1$. *Then the norm* $\mathrm{Norm}_{\mathbb{Q}(\zeta_{rq})/\mathbb{Q}(\zeta_r)}\mathcal{Z}(rq)$ *is equal to* $P_q(\mathrm{Frob}_q)\mathcal{Z}(r)$, *where* $P_q(X) \in \mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}[X]$ *is the polynomial* $\det(1-\mathrm{Frob}_q X;\mathcal{T})$ *and* Frob_q *is* (*the conjugacy class of*) *a geometric Frobenius element at* q *in the Galois group* $\mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$.

2) *For each pair* (j,κ) *of an integer* j *and an arithmetic point* κ *such that* $1 \leq j \leq w(\kappa)+1$, *let* $z^{(j,\kappa)}(1) \in H^1(\mathbb{Q}_S/\mathbb{Q},(T^{(j,\kappa)})^*(1))$ *be the specialization of* $\mathcal{Z}(1) \in H^1(\mathbb{Q}_S/\mathbb{Q},\mathcal{T}^*(1))$ *via* $\chi^{j-1}\circ\kappa$. *If we denote by* $\mathrm{loc}_{/f}(z^{(j,\kappa)}(1))$ *the image of* $z^{(j,\kappa)}(1)$ *under the localization map*

$$H^1\big(\mathbb{Q}_S/\mathbb{Q},(T^{(j,\kappa)})^*(1)\big) \longrightarrow H^1_{/f}\big(\mathbb{Q}_p,(T^{(j,\kappa)})^*(1)\big) := \frac{H^1(\mathbb{Q}_p,(T^{(j,\kappa)})^*(1))}{H^1_f(\mathbb{Q}_p,(T^{(j,\kappa)})^*(1))},$$

then $\exp^*(\mathrm{loc}_{/f}(z^{(j,\kappa)}(1)))$ *is contained in*

$$\mathrm{Fil}^{w(\kappa)+2-j} V_{\mathrm{dR}}(\overline{f}_\kappa) \subset \mathrm{Fil}^0 \mathrm{D}_{\mathrm{dR}}\big((V^{(j,\kappa)})^*(1)\big),$$

for the dual exponential map

$$H^1_{/f}\big(\mathbb{Q}_p,(T^{(j,\kappa)})^*(1)\big) \xrightarrow{\exp^*} \mathrm{Fil}^0 \mathrm{D}_{\mathrm{dR}}\big((V^{(j,\kappa)})^*(1)\big)$$

defined by Kato (*cf.* [Ka1]).

3) *Further*, $\exp^*(\mathrm{loc}_{/f}(z^{(j,\kappa)}(1)))$ *is equal to*

$$\frac{L_{(p)}(f_\kappa,\omega^{i-j},j)}{(2\sqrt{-1}\pi)^{j-1}C^{(-1)^i}_{\infty,\kappa}} \cdot \overline{\delta}_\kappa^{\mathrm{dR}}$$

where $C^{\pm}_{\infty,\kappa} \in \mathbb{C}$ *is a complex period* (*see* [Oc2], §3 *and* [Oc3] *for* $C^{\pm}_{\infty,\kappa}$).

Let $H^1_{/f}(\mathbb{Q}_p,\mathcal{T}^*(1))$ be $\varprojlim_{s,t} H^1_{/f}(\mathbb{Q}_p,\mathcal{T}^*(1)/\Phi^{(1,2)}_{s,t}\mathcal{T}^*(1))$. We also denote by $\mathrm{loc}_{/f}(\mathcal{Z}(1))$ the image of $\mathcal{Z}(1)$ under the localization map:

$$H^1\big(\mathbb{Q},\mathcal{T}^*(1)\big)\longrightarrow H^1\big(\mathbb{Q}_p,\mathcal{T}^*(1)\big)\longrightarrow\!\!\!\!\rightarrow H^1_{/f}\big(\mathbb{Q}_p,\mathcal{T}^*(1)\big).$$

The main theorem in our previous paper [Oc2] is the construction of the two-variable p-adic L-function $L_p(\mathcal{T})$ as follows:

THEOREM B (see [Oc2], Theorem 3.14). — *We assume condition* (**F**). *Assume further that* $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$ *is integrally closed in its field of fraction. Then we have a map*

$$\Xi\colon\ H^1_{/f}\big(\mathbb{Q}_p,\mathcal{T}^*(1)\big)\longrightarrow\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$$

such that $L_p(\mathcal{T}):=\Xi(\mathrm{loc}_{/f}(\mathcal{Z}(1)))$ *has the following properties*:

1) *For each height* 1 *prime* $\mathfrak{p}$ *of* $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$, *then we have the equality*

$$\mathrm{length}_{(\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}})_{\mathfrak{p}}}\big(H^1_{/f}(\mathbb{Q}_p,\mathcal{T}^*(1))/\mathrm{loc}_{/f}\big(\mathcal{Z}(1)\big)\big)_{\mathfrak{p}}=\mathrm{ord}_{\mathfrak{p}}\big(L_p(\mathcal{T})\big).$$

2) *We have the interpolation property* :

$$(\chi^{j-1}\circ\kappa)\big(L_p(\mathcal{T})\big)/C_{p,\kappa}=(-1)^{j-1}(j-1)!\Big(1-\frac{\omega^{i-j}(p)p^{j-1}}{a_p(f_\kappa)}\Big)\Big(\frac{p^{j-1}}{a_p(f_\kappa)}\Big)^{q(i,j)}\times G(\omega^{j-i})\frac{L(f_\kappa,\omega^{i-j},j)}{(2\pi\sqrt{-1})^{j-1}C^{(-1)^i}_{\infty,\kappa}}$$

for each (j,κ) *with* $0\le j-1\le w(\kappa)$, *where* $C_{p,\kappa}\in\overline{\mathbb{Q}}_p^{\times}$ *is a p-adic period* (*see* [Oc2] *and* [Oc3] *for* $C_{p,\kappa}$) *at each arithmetic point* $\kappa\in\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{H}^{\mathrm{ord}}_{\mathcal{F}},\overline{\mathbb{Q}}_p)$, $G(\omega^{j-i})$ *is the Gauss sum and* $q(i,j)$ *is equal to the p-order of the conductor of* ω^{i-j}.

Remark 1.3. — The condition that $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$ is normal in the above theorem is necessary only to assure that the image of Ξ is contained in the integral part $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$. Without this condition, we only know that the localization of the image of Ξ is in the fraction field $\mathrm{Frac}(\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}})$ of $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$ is contained in $(\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}})_{\mathfrak{p}}$ for each height 1 prime $\mathfrak{p}$ of $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$. Then, interpolation properties as above hold without the condition that $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$ is integrally closed (see the arguments in [Oc2], §5).

By the above Proposition A and Theorem B, we propose the following conjecture which was first proposed by Greenberg [Gr2]:

Iwasawa Main Conjecture. — *We assume the condition* (**F**). *For each height* 1 *prime* $\mathfrak{p}$ *of* $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$, *we have the equality*

$$\mathrm{length}_{(\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}})_{\mathfrak{p}}}(\mathrm{Sel}^{\vee}_{\mathcal{T}})_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}}\big(L_p(\mathcal{T})\big).$$

To relate our Euler system $\mathcal{Z}(1)$ to the Selmer group, we need to develop the Euler system theory for Galois deformations which generalize the Euler system theory for the cyclotomic tower proved by Kato [Ka4], Perrin-Riou [Pe] and Rubin [Ru2]. The following theorem is the main result of this paper (see Theorem 2.4 and Theorem 2.6):

Theorem C. — *We assume that* $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$ *is isomorphic to a two-variable power series algebra* $\mathcal{O}[[X_1, X_2]]$ *over the ring of the integers* $\mathcal{O}$ *of a certain finite extension of* $\mathbb{Q}_p$. *Let us assume the condition* (**F**) *and the existence of the elements* $\tau \in G_{\mathbb{Q}(\mu_{p^\infty})}$ *and* $\tau' \in G_{\mathbb{Q}}$ *which satisfy the following properties*:

1) *The image of* τ *under the representation*

$$G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(\mathcal{T}) \cong \mathrm{GL}_2(\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}})$$

has a presentation $\left(\begin{smallmatrix} 1 & P_\tau \\ 0 & 1 \end{smallmatrix}\right)$ *under certain choice of basis* $\mathrm{Aut}(\mathcal{T}) \cong \mathrm{GL}_2(\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}})$, *where* P_τ *is a non-zero element of* $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$.

2) *The element* $\tau' \in G_{\mathbb{Q}}$ *acts on* $\mathcal{T}$ *via the multiplication by* -1.

Then there exists an integer $k \geq 0$ *such that we have the following inequality for each height* 1 *prime* $\mathfrak{p}$ *of* $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$:

$$\mathrm{length}_{(\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}})_{\mathfrak{p}}}(\mathrm{Sel}^{\vee}_{\mathcal{T}})_{\mathfrak{p}} \leq \mathrm{length}_{(\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}})_{\mathfrak{p}}}\big((H_{/f}(\mathbb{Q}_p, \mathcal{T}^*(1))/\mathrm{loc}_{/f}\big(\mathcal{Z}(1))\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}\big)_{\mathfrak{p}} + \mathrm{ord}_{\mathfrak{p}}(P^k_\tau).$$

Finally, our results combining Proposition A, Theorem B and Theorem C are summarized as follows.

Theorem. — *Let us assume the condition* (**F**) *and the existence of elements* $\tau \in G_{\mathbb{Q}(\mu_{p^\infty})}$ *and* $\tau' \in G_{\mathbb{Q}}$ *satisfying the conditions* 1) *and* 2) *stated in Theorem C. Assume further that the local ring* $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$ *is isomorphic to a two-variable power series algebra* $\mathcal{O}[[X_1, X_2]]$. *Then*:

1) *The Pontryagin dual* $\mathrm{Sel}_{\mathcal{T}}^{\vee}$ *of* $\mathrm{Sel}_{\mathcal{T}}$ *is a finitely generated torsion* $\mathbb{H}_{\mathcal{F}}^{n,o}$*-module.*

2) *If we assume the two conditions given in Theorem B, there exists an integer* k *such that we have the following inequality for each height* 1 *prime* $\mathfrak{p}$ *of* $\mathbb{H}_{\mathcal{F}}^{n,o}$:

$$\mathrm{length}_{(\mathbb{H}_{\mathcal{F}}^{n,o})_{\mathfrak{p}}}(\mathrm{Sel}_{\mathcal{T}}^{\vee})_{\mathfrak{p}} \leq \mathrm{ord}_{(\mathbb{H}_{\mathcal{F}}^{n,o})_{\mathfrak{p}}}(L_p(\mathcal{T})) + \mathrm{ord}_{\mathfrak{p}}(P_{\tau}^{k}).$$

The key of the proof of the inequality in Theorem C consists of:

1) The specialization lemma (see Proposition 3.6 and Proposition 3.11), which recovers the characteristic ideal of a given torsion Iwasawa module M over an n-variable Iwasawa algebra $\Lambda^{(n)}$ from the variation of the sizes of the specializations M_{α} of M via a certain (well-chosen) family of homomorphisms $\{\alpha\colon \Lambda^{(n)} \to \overline{\mathbb{Q}}_p\}_{\alpha\in A}$.

2) Induction argument (§4) using the above specialization lemma, which reduces the problem of the Euler system theory over an n-variable Iwasawa algebra to the Euler system theory over a discrete valuation ring already studied by several people.

We remark that our approach via the specialization lemma makes the proof of the Euler system theory easier even in the classical case of the Euler system theory in a $\mathbb{Z}_p^d$-extension (compare to [Ka4], [Pe] and [Ru2]). One feature of our proof is the use of non-arithmetic specializations $\alpha\colon\Lambda^{(n)} \to \overline{\mathbb{Q}}_p$ such that the specialized Galois representations $\mathcal{T}_{\alpha}$ are not necessarily associated to motives. Over a one-variable Iwasawa algebra, a similar idea of the simplification of the Euler system argument is given also in a recent article [MR] by Mazur and Rubin. The specializations of our result on the two variable main conjecture to other non-critical or non-ordinary representations might give us some interesting consequences. Thus, we expect that further inquiry of such systematic use of the induction argument combined with the specializations will bring about fruitful applications and new perspectives in the research of Iwasawa theory for Galois deformations.

Notations. — For an integer r, we denote by μ_r the group of r-th roots of unity and denote by $\mathbb{Q}(\mu_r)$ the field obtained by adjoining μ_r to the rational number field $\mathbb{Q}$. We often denote by $\mathbb{Q}(\mu_{p^{\infty}})$ the field obtained by adjoining all p-power roots of unity to the rational number field $\mathbb{Q}$. For any Galois extension $L/\mathbb{Q}$ and a prime number q which is unramified in $L/\mathbb{Q}$, we denote by $\mathrm{Frob}_q \in \mathrm{Gal}(L/\mathbb{Q})$ (resp. $\varphi_q \in \mathrm{Gal}(L/\mathbb{Q})$) (a conjugate class of) a geometric (resp. arithmetic) Frobenius element at q.

Aknowledgments. — The author expresses his sincere gratitude to professor Kazuya Kato for advice on the use of non-arithmetic specializations. He thanks Yoshitaka Hachimori, Kazuo Matsuno and Takeshi Saito for useful discussion. He also thanks Ralph Greenberg and Haruzo Hida for stimulating conversation on the subject and encouragement.

2. The main theorem for Euler system and its applications.

Throughout the paper we denote by $\mathcal{O}$ the ring of the integers of a finite extension K of $\mathbb{Q}_p$. For a natural number n, let $\Lambda_{\mathcal{O}}^{(n)}$ be an n-variable Iwasawa algebra over $\mathcal{O}$. That is, $\Lambda_{\mathcal{O}}^{(n)}$ is an n-variable power series ring $\mathcal{O}[[X_1,\dots,X_n]]$ over $\mathcal{O}$. Let $\mathcal{T}$ be a free $\Lambda_{\mathcal{O}}^{(n)}$-module of rank 2 with continuous $G_{\mathbb{Q}}$-action. We denote the Kummer dual representation $\mathrm{Hom}_{\Lambda_{\mathcal{O}}^{(n)}}(\mathcal{T},\Lambda_{\mathcal{O}}^{(n)})\otimes_{\mathbb{Z}_p}\mathbb{Z}_p(1)$ by $\overline{\mathcal{T}}$, where $\otimes_{\mathbb{Z}_p}\mathbb{Z}_p(1)$ means the Tate twist.

The definition of the Euler system for Galois deformation is as follows:

Definition 2.1. — Let $\overline{\mathcal{T}}$ be a free $\Lambda_{\mathcal{O}}^{(n)}$-module of rank 2 with continuous $G_{\mathbb{Q}}$-action which is unramified outside a finite set of primes S which contains $\{p,\infty\}$. We denote by $\mathcal{R}$ the set of all square-free natural numbers which are prime to S. An Euler system for $\overline{\mathcal{T}}$ is a collection of cohomology classes $\{\mathcal{Z}(r)\in H^1(\mathbb{Q}(\mu_r),\overline{\mathcal{T}})\}_{r\in\mathcal{R}}$ with the following properties:

1) The element $\mathcal{Z}(r)$ is unramified outside $S\cup\{r\}$ for each $r\in\mathcal{R}$.

2) The norm $\mathrm{Norm}_{\mathbb{Q}(\mu_{rq})/\mathbb{Q}(\mu_r)}\mathcal{Z}(rq)$ is equal to $P_q(\mathrm{Frob}_q)\mathcal{Z}(r)$, where $P_q(X)\in\Lambda_{\mathcal{O}}^{(n)}[X]$ is a polynomial $\det(1-\mathrm{Frob}_q X;\mathcal{T})$ and Frob_q is a (conjugacy class of) geometric Frobenius element at q in the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_r)/\mathbb{Q})$.

Definition 2.2. — Let M be a finitely generated torsion $\Lambda_{\mathcal{O}}^{(n)}$-module. For each height 1 prime $\mathfrak{p}$ of $\Lambda_{\mathcal{O}}^{(n)}$, we denote by $\ell(M;\mathfrak{p})$ the length of $\Lambda_{\mathcal{O},\mathfrak{p}}^{(n)}$-module $M_{\mathfrak{p}}$, where $\Lambda_{\mathcal{O},\mathfrak{p}}^{(n)}$ (resp. $M_{\mathfrak{p}}$) means the localization at $\mathfrak{p}$. Note that $\ell(M;\mathfrak{p})$ is an integer which is zero for almost all height 1 primes $\mathfrak{p}$ of $\Lambda_{\mathcal{O}}^{(n)}$. Then the characteristic ideal $\mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}}(M)$ of M is defined to be the ideal $\prod_{\mathfrak{p}}\mathfrak{p}^{\ell(M;\mathfrak{p})}$, where $\mathfrak{p}$ runs all height 1 primes in $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$. A torsion $\Lambda_{\mathcal{O}}^{(n)}$-module M is called pseudo-null if $\ell(M;\mathfrak{p})$ is zero for all height 1 primes $\mathfrak{p}$ of $\Lambda_{\mathcal{O}}^{(n)}$.

DEFINITION 2.3. — We say that the representation $\mathcal{T}$ satisfies (**Im**) if there exist $\tau \in G_{\mathbb{Q}(\mu_{p^\infty})}$ and $\tau' \in G_{\mathbb{Q}}$ such that the following two conditions hold for the Galois image of τ and τ':

1) The image of τ under the representation $G_{\mathbb{Q}} \to \mathrm{Aut}(\mathcal{T}) \cong \mathrm{GL}_2(\Lambda_{\mathcal{O}}^{(n)})$ has a presentation $\left(\begin{smallmatrix} 1 & P_\tau \\ 0 & 1 \end{smallmatrix}\right)$ under certain choice of basis $\mathrm{Aut}(\mathcal{T}) \cong \mathrm{GL}_2(\Lambda_{\mathcal{O}}^{(n)})$, where P_τ is a non-zero element of $\Lambda_{\mathcal{O}}^{(n)}$.

2) The element $\tau' \in G_{\mathbb{Q}}$ acts on $\mathcal{T}$ via the multiplication by -1.

Let $Ш_S^2(\overline{\mathcal{T}})$ be the kernel of the restriction map

$$H^2(\mathbb{Q}_S/\mathbb{Q}, \overline{\mathcal{T}}) \longrightarrow \bigoplus_{v \in S} H^2(\mathbb{Q}_v, \overline{\mathcal{T}}).$$

Our main theorem is as follows:

THEOREM 2.4. — *Let* $\left\{\mathcal{Z}(r) \in H^1(\mathbb{Q}(\mu_r), \overline{\mathcal{T}})\right\}_{r \in \mathcal{R}}$ *be an Euler system for* $\overline{\mathcal{T}}$*. Assume the following conditions*:

(i) *The element* $\mathcal{Z}(1)$ *is not contained in the* $\Lambda_{\mathcal{O}}^{(n)}$*-torsion part of* $H^1(G_S, \overline{\mathcal{T}})$.

(ii) *For each finite place* $v \in S$, $H^2(\mathbb{Q}_v, \overline{\mathcal{T}})$ *is a torsion* $\Lambda_{\mathcal{O}}^{(n)}$*-module.*

(iii) *The images of the determinant representations* $G_{\mathbb{Q}} \to \mathrm{Aut}(\overset{2}{\wedge}\, \mathcal{T}) \cong (\Lambda_{\mathcal{O}}^{(n)})^\times$ *and* $G_{\mathbb{Q}} \to \mathrm{Aut}(\overset{2}{\wedge}\, \overline{\mathcal{T}}) \cong (\Lambda_{\mathcal{O}}^{(n)})^\times$ *contain elements of infinite order.*

(iv) *The residual representation* $\mathcal{T}/(\pi_{\mathcal{O}}, X_1, \ldots, X_n)\mathcal{T} \cong \mathbb{F}^{\oplus 2}$ *is an irreducible representation of* $G_{\mathbb{Q}}$.

(v) *The* $\pm$*-eigen spaces* $\mathcal{T}^{\pm}$ *of a complex conjugate element are both rank* 1 *modules over* $\Lambda_{\mathcal{O}}^{(n)}$.

Assume further the condition (**Im**) *and fix* $\tau \in G_{\mathbb{Q}(\mu_{p^\infty})}$ *satisfying this condition. Then we have the following statements*:

1) *The group* $Ш_S^2(\overline{\mathcal{T}})$ *is a finitely generated torsion* $\Lambda_{\mathcal{O}}^{(n)}$*-module.*

2) *Assume that the finitely generated* $\Lambda_{\mathcal{O}}^{(n)}$*-module* $Ш_S^2(\overline{\mathcal{T}})$ *admits a set of generators consisting of* k *elements. Then the following inclusion of the characteristic ideals holds*:

$$(P_\tau^k)\mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}}\left(H^1(\mathbb{Q}_S/\mathbb{Q}, \overline{\mathcal{T}})/\mathcal{Z}(1)\Lambda_{\mathcal{O}}^{(n)}\right) \subset \mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}}\left(Ш_S^2(\overline{\mathcal{T}})\right).$$

Remark 2.5. — Though we assume that $\mathrm{rank}_{\Lambda_{\mathcal{O}}^{(n)}}(\mathcal{T}) = 2$ throughout the paper, it is not essential assumption for the proof of the above result.

A few minor modification of the conditions in Theorem 2.4 and (**Im**) allows us a similar result in the case $\mathrm{rank}_{\Lambda_{\mathcal{O}}^{(n)}}(\mathcal{T}) > 2$. Since the application to Hida deformation requires only the rank 2 case, we restrict ourselves to this case in order to avoid complicated notations. We would like to discuss the general case together with other generalization in a subsequent paper.

The proof of Theorem 2.4 is completed in §4 after preparation in §3. Let us apply Theorem 2.4 to Hida's nearly ordinary deformation $\mathcal{T} = \widetilde{T} \otimes \omega^i$ explained in §1.

From now on throughout the section, we assume that $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$ is isomorphic to a two-variable power series algebra $\mathcal{O}[[X_1, X_2]]$ over a complete discrete valuation ring $\mathcal{O}$ which is finite flat over $\mathbb{Z}_p$.

THEOREM 2.6. — *Assume the condition* (**F**). *We also assume that* $\mathcal{T} = \widetilde{T} \otimes \omega^i$ *satisfies the condition* (**Im**) *and fix* $\tau \in G_{\mathbb{Q}(\mu_{p^\infty})}$ *satisfying this condition. Let* $\mathcal{Z}(1) \in H^1(\mathbb{Q}_S/\mathbb{Q}, \mathcal{T}^*(1))$ *be the Beilinson-Kato element* (*see Proposition* 1.2). *Then, under the assumption that* $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$ *is isomorphic to* $\mathcal{O}[[X_1, X_2]]$, *we have the following statements*:

1) *The group* $Ш^2_S(\mathcal{T}^*(1))$ *is a finitely generated torsion* $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$*-module.*

2) *Assume that the finitely generated* $\Lambda_{\mathcal{O}}^{(n)}$*-module* $Ш^2_S(\overline{\mathcal{T}})$ *admits a set of generators consisting of* k *elements. Then the following inclusion of the characteristic ideals holds*:

$$(P_\tau^k)\mathrm{char}_{\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}}\big(H^1(\mathbb{Q}_S/\mathbb{Q}, \mathcal{T}^*(1))/\mathcal{Z}(1)\big) \subset \mathrm{char}_{\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}}\big(Ш^2_S\big(\mathcal{T}^*(1)\big)\big).$$

Let us deduce Theorem 2.6 from Theorem 2.4.

Proof of Theorem 2.6. — It is sufficient to check that our Galois module $\mathcal{T}$ and the Euler system $\mathcal{Z}(1)$ satisfies the conditions in Theorem 2.4. Condition (iv) is already assumed by the condition (**F**). Condition (v) is due to the fact that the determinant of the representation associated to an elliptic modular form is odd. For the condition (iii), we recall the basic properties of Hida deformation introduced after Definition 1.1. The most non-trivial condition is (i). We need the result in Theorem B that the composite homomorphism

$$H^1\big(\mathbb{Q}_S/\mathbb{Q}, \mathcal{T}^*(1)\big) \longrightarrow H^1_{/f}\big(\mathbb{Q}_p, \mathcal{T}^*(1)\big) \xrightarrow{\Xi_d} \mathcal{O}[[X_1, X_2]]$$

sends $\mathcal{Z}(1)$ to $L_p(\mathcal{T})$. Since $L_p(\mathcal{T}) \in \mathcal{O}[[X_1, X_2]]$ is not zero, condition (i) follows. This completes the proof. □

Let us deduce Theorem C stated in §1 from Theorem 2.6.

Proof of Theorem C. — By the global duality theorem, we have a four term exact sequence:

$$0 \to H^1\big(\mathbb{Q}_S/\mathbb{Q}, \mathcal{T}^*(1)\big)/\mathcal{Z}(1) \longrightarrow H^1_{/f}\big(\mathbb{Q}_p, \mathcal{T}^*(1)\big)/\big(\mathrm{loc}_{/f}(\mathcal{Z}(1))\big) \longrightarrow \mathrm{Sel}^\vee_{\mathcal{T}} \longrightarrow Ш^2_S\big(\mathcal{T}^*(1)\big) \to 0.$$

Since $H^1_{/f}(\mathbb{Q}_p, \mathcal{T}^*(1))$ is a torsion-free $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$-module of generic rank 1 by [Oc2], §4, $H^1_{/f}(\mathbb{Q}_p, \mathcal{T}^*(1))/\mathrm{loc}_{/f}(\mathcal{Z}(1))$ is a torsion $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$-module. Hence by Theorem 2.6, $\mathrm{Sel}^\vee_{\mathcal{T}}$ is a torsion $\mathbb{H}^{\mathrm{n.o}}_{\mathcal{F}}$-module. We see that the inequality Theorem 2.6, 2) and the inequality in Theorem C are equivalent by the exactness of the above sequence. □

3. Iwasawa module and its specialization.

In this section, we discuss about a characterization of the characteristic ideal of a given torsion Iwasawa module by the behavior of the orders of its specializations. The results obtained in this section are used for the proof of our main result in §4.

Before going into the main subject of this section, we give the following lemma, which will be used in this section and the next:

LEMMA 3.1. — *Let $n \geq 2$ and let N be a pseudo-null $\Lambda^{(n)}_{\mathcal{O}}$-module. Let I be a height 1 prime of $\Lambda^{(n)}_{\mathcal{O}}$ such that $\Lambda^{(n)}_{\mathcal{O}}/I$ is a regular local ring of Krull dimension n. Then, we have the following equality between ideals of $\Lambda^{(n)}_{\mathcal{O}}/I$:*

$$\mathrm{char}_{\Lambda^{(n)}_{\mathcal{O}}/I}\big(N[I]\big) = \mathrm{char}_{\Lambda^{(n)}_{\mathcal{O}}/I}(N/IN).$$

Especially, $N[I]$ is a pseudo-null $\Lambda^{(n)}_{\mathcal{O}}/I$-module if and only if N/IN is a pseudo-null $\Lambda^{(n)}_{\mathcal{O}}/I$-module.

Since we have no reference for this lemma, we briefly give a proof here.

Proof. — Let us take arbitrary height 1 prime $\mathfrak{p}$ of $\Lambda^{(n)}_{\mathcal{O}}/I$ and let $\widetilde{\mathfrak{p}} \subset \Lambda^{(n)}_{\mathcal{O}}$ be the inverse image of $\mathfrak{p}$ via $\Lambda^{(n)}_{\mathcal{O}} \to \Lambda^{(n)}_{\mathcal{O}}/I$. Then $\widetilde{\mathfrak{p}}$ is a height 2 prime of $\Lambda^{(n)}_{\mathcal{O}}$. We apply the functor $\otimes_{\Lambda^{(n)}_{\mathcal{O}}}(\Lambda^{(n)}_{\mathcal{O}})_{\widetilde{\mathfrak{p}}}$ to the following exact sequence:

$$0 \to N[I] \longrightarrow N \longrightarrow N \longrightarrow N/IN \to 0.$$

Since a localization functor preserves an exact sequence, we have the following:

$$0 \to (N[I])_{\tilde{\mathfrak{p}}} \longrightarrow (N)_{\tilde{\mathfrak{p}}} \longrightarrow (N)_{\tilde{\mathfrak{p}}} \longrightarrow (N/IN)_{\tilde{\mathfrak{p}}} \to 0. \tag{1}$$

Note that we have $(N[I])_{\tilde{\mathfrak{p}}} = (N[I])_{\mathfrak{p}}$ (resp. $(N/IN)_{\tilde{\mathfrak{p}}} = (N/IN)_{\mathfrak{p}}$). We have to prove the equality $\mathrm{length}_{(\Lambda_{\mathcal{O}}^{(n)}/I)_{\mathfrak{p}}}(N[I])_{\mathfrak{p}} = \mathrm{length}_{(\Lambda_{\mathcal{O}}^{(n)}/I)_{\mathfrak{p}}}(N/IN)_{\mathfrak{p}}$ or equivalently the equality

$$\mathrm{length}_{(\Lambda_{\mathcal{O}}^{(n)})_{\tilde{\mathfrak{p}}}}\big(N[I]\big)_{\tilde{\mathfrak{p}}} = \mathrm{length}_{(\Lambda_{\mathcal{O}}^{(n)})_{\tilde{\mathfrak{p}}}}(N/IN)_{\tilde{\mathfrak{p}}}.$$

Note that $(N)_{\tilde{\mathfrak{p}}}$ is also a pseudo-null $(\Lambda_{\mathcal{O}}^{(n)})_{\tilde{\mathfrak{p}}}$-module. Since $(\Lambda_{\mathcal{O}}^{(n)})_{\tilde{\mathfrak{p}}}$ is of Krull dimension 2, any pseudo-null $(\Lambda_{\mathcal{O}}^{(n)})_{\tilde{\mathfrak{p}}}$-module has finite length. Hence by the above four term exact sequence (1), we have $\mathrm{length}_{(\Lambda_{\mathcal{O}}^{(n)})_{\tilde{\mathfrak{p}}}}(N[I])_{\tilde{\mathfrak{p}}} = \mathrm{length}_{(\Lambda_{\mathcal{O}}^{(n)})_{\tilde{\mathfrak{p}}}}(N/IN)_{\tilde{\mathfrak{p}}}$. This completes the proof of the lemma. □

We introduce the following notations:

Definition 3.2. — Let $n \geq 1$ be an integer.

1) *A linear element* ℓ in an n-variable Iwasawa algebra $\Lambda_{\mathcal{O}}^{(n)} \cong \mathcal{O}[[X_1, \ldots, X_n]]$ is a polynomial $\ell = a_0 + a_1X_1 + \cdots + a_nX_n \in \Lambda_{\mathcal{O}}^{(n)}$ with $a_i \in \mathcal{O}$ of degree at most 1 such that ℓ is not divisible by $\pi_{\mathcal{O}}$ and is not invertible in $\Lambda_{\mathcal{O}}^{(n)}$. That is, ℓ is a polynomial of degree at most 1 such that a_0 is divisible by $\pi_{\mathcal{O}}$, but not all a_i are divisible by $\pi_{\mathcal{O}}$.

2) We denote by $\mathcal{L}_{\mathcal{O}}^{(n)}$ the set of all linear ideals of $\Lambda_{\mathcal{O}}^{(n)}$. That is:

$$\mathcal{L}_{\mathcal{O}}^{(n)} = \big\{(\ell) \subset \Lambda_{\mathcal{O}}^{(n)} \mid \ell \text{ is a linear element in } \Lambda_{\mathcal{O}}^{(n)}\big\}.$$

3) Let $n \geq 2$. For a torsion $\Lambda_{\mathcal{O}}^{(n)}$-module M, we denote by $\mathcal{L}_{\mathcal{O}}^{(n)}(M)$ a subset of $\mathcal{L}_{\mathcal{O}}^{(n)}$ which consists of $(\ell) \subset \mathcal{L}_{\mathcal{O}}^{(n)}$ satisfying the following conditions:

(a) the quotient $M/(\ell)M$ is a torsion $\Lambda_{\mathcal{O}}^{(n)}/(\ell)$-module;

(b) the image of the characteristic ideal $\mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}}(M) \subset \Lambda_{\mathcal{O}}^{(n)}$ in $\Lambda_{\mathcal{O}}^{(n)}/(\ell)$ is equal to the characteristic ideal $\mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}/(\ell)}(M/(\ell)M) \subset \Lambda_{\mathcal{O}}^{(n)}/(\ell)$.

Definition 3.3. — *A linear transform* σ of an n-variable Iwasawa algebra $\mathcal{O}[[X_1, \ldots, X_n]]$ is an automorphism of $\mathcal{O}[[X_1, \ldots, X_n]]$ given by $\sigma(X_j) = \sum_{1 \leq i \leq n} t_{i,j}X_i$ such that $(t_{i,j})_{1 \leq i,j \leq n}$ is in $\mathrm{GL}_n(\mathcal{O})$.

Note that a linear element defined in Definition 3.2 is stable under the action of a linear transform. Let $x \in \Lambda_{\mathcal{O}}^{(n)}$. Take arbitrary linear transform σ of $\Lambda_{\mathcal{O}}^{(n)}$, $\sigma(x)$ is a linear element in $\Lambda_{\mathcal{O}}^{(n)}$ if and only if x is a linear element in $\Lambda_{\mathcal{O}}^{(n)}$.

For a natural number m, we denote by $\mathbb{P}^m(\mathcal{O})$ the projective space of dimension m. That is, $\mathbb{P}^m(\mathcal{O})$ is the set of ratios $(x_0 : \cdots : x_m)$ with $x_i \in \mathcal{O}$. We have the following lemma:

LEMMA 3.4. — *Let $n \geq 1$ be an integer.*

1) *Let ℓ and ℓ' be linear elements in $\Lambda_{\mathcal{O}}^{(n)}$. If $\ell = u\ell'$ holds for a certain unit $u \in (\Lambda_{\mathcal{O}}^{(n)})^\times$, u is necessarily a constant element contained in $\mathcal{O}^\times$.*

2) *The set $\mathcal{L}_{\mathcal{O}}^{(n)}$ is (non-canonically) identified with $\mathcal{M}_{\mathcal{O}} \times \mathbb{P}^{n-1}(\mathcal{O})$.*

3) *Let $n \geq 2$. For a torsion $\Lambda_{\mathcal{O}}^{(n)}$-module M, $\mathcal{L}_{\mathcal{O}}^{(n)}(M)$ is equal to*

$$\left\{(\ell) \in \mathcal{L}_{\mathcal{O}}^{(n)} \mid M/(\ell)M \text{ is a torsion } \Lambda_{\mathcal{O}}^{(n)}/(\ell)\text{-module}\right\} \cap \mathcal{L}_{\mathcal{O}}^{(n)}(M_{\mathrm{null}}),$$

where M_{null} is the largest pseudo-null sub-module of M.

Proof. — Let us prove the first statement. We take linear elements $\ell = a_0 + \sum_{1 \leq i \leq n} a_i X_i$, $\ell' = a_0' + \sum_{1 \leq i \leq n} a_i' X_i$ and $u \in (\Lambda_{\mathcal{O}}^{(n)})^\times$, where a_i (resp. a_i') is an element in $\mathcal{O}$ for each i. By the definition of linear elements, one of the coefficients a_i' of ℓ' is a unit of $\mathcal{O}$. In order to show that u is contained in $\mathcal{O}^\times$, we may assume that a_n' is a unit without loss of generality. By multiplying an element of $\mathcal{O}^\times$, we assume that $a_n' = 1$. We denote $\ell' - X_n \in \mathcal{O}[[X_1, \ldots, X_{n-1}]]$ by α. By definition α is contained in the maximal ideal $\mathcal{M}$ of $\mathcal{O}[[X_1, \ldots, X_{n-1}]]$. Since $u \in \Lambda_{\mathcal{O}}^{(n)} = \mathcal{O}[[X_1, \ldots, X_{n-1}]][[X_n]]$ has an expansion $u = \sum_{0 \leq j < \infty} b_j X_n^j$, where b_j is an element in $\mathcal{O}[[X_1, \ldots, X_{n-1}]]$, we have the following expansion of $u\ell'$ in $\mathcal{O}[[X_1, \ldots, X_{n-1}]][[X_n]]$:

$$u\ell' = (\alpha + X_n)\Big(\sum_{0 \leq j < \infty} b_j X_n^j\Big) = \alpha b_0 + \sum_{1 \leq j < \infty} (\alpha b_j + b_{j-1}) X_n^j.$$

By the assumption that $\ell = u\ell'$, $\alpha b_j + b_{j-1}$ must be zero for each $j \geq 2$. Thus we have an expression $b_j = (-\alpha)^r b_{j+r}$ for arbitrary integers $j, r \geq 1$. Since b_j is divisible by arbitrary large power of $\mathcal{M}$, b_j must be zero for each $j \geq 1$ (Note that $\bigcap_{r \geq 1} \mathcal{M}^r = 0$). Hence we have $\ell = \alpha b_0 + b_0 X_n$ in $\mathcal{O}[[X_1, \ldots, X_{n-1}]][[X_n]]$. Since the coefficient of X_n must be contained in $\mathcal{O}$, we have $b_0 \in \mathcal{O}$. This completes the proof of the statement 1).

By definition, the set of linear elements $\ell \in \Lambda_{\mathcal{O}}^{(n)}$ is isomorphic to $\mathcal{M}_{\mathcal{O}} \times (\mathcal{O}^{\oplus n} \setminus \mathcal{M}_{\mathcal{O}}^{\oplus n})$. Let $\ell, \ell' \in \Lambda_{\mathcal{O}}^{(n)}$ be linear elements. As is shown above, $(\ell) = (\ell')$ holds if and only if there exists a unit $u \in \mathcal{O}^{\times}$ such that $\ell = u\ell'$. Thus the set of linear ideals $\mathcal{L}_{\mathcal{O}}^{(n)}$ is isomorphic to $(\mathcal{M}_{\mathcal{O}} \times (\mathcal{O}^{\oplus n} \setminus \mathcal{M}_{\mathcal{O}}^{\oplus n}))/\sim$, where $\sim$ is the equivalence relation under the diagonal action by the multiplication of the elements of $\mathcal{O}^{\times}$. Note that $(\mathcal{O}^{\oplus n} \setminus \mathcal{M}_{\mathcal{O}}^{\oplus n}))/\sim$ is isomorphic to $\mathbb{P}^{n-1}(\mathcal{O})$. We consider a map $\mathcal{M}_{\mathcal{O}} \times (\mathcal{O}^{\oplus n} \setminus \mathcal{M}_{\mathcal{O}}^{\oplus n})$ to $\mathcal{M}_{\mathcal{O}} \times (\mathcal{O}^{\oplus n} \setminus \mathcal{M}_{\mathcal{O}}^{\oplus n})$ which sends $(m, x_0, \ldots, x_{n-1})$ to $(mx_i^{-1}, x_0 x_i^{-1}, \ldots, x_{n-1}x_i^{-1})$, where i is the minimal integer such that x_i is a unit of $\mathcal{O}$. This induces a map $\big(\mathcal{M}_{\mathcal{O}} \times (\mathcal{O}^{\oplus n} \setminus \mathcal{M}_{\mathcal{O}}^{\oplus n})\big)/\sim$ to $\mathcal{M}_{\mathcal{O}} \times (\mathcal{O}^{\oplus n} \setminus \mathcal{M}_{\mathcal{O}}^{\oplus n})/\sim$. It is checked that the map $\mathcal{L}_{\mathcal{O}}^{(n)} \longrightarrow \mathcal{M}_{\mathcal{O}} \times \mathbb{P}^{n-1}(\mathcal{O})$ defined above is bijective. This completes the proof of 2).

Let us consider the fundamental exact sequence:

$$0 \to M/M_{\mathrm{null}} \longrightarrow \bigoplus_{\mathfrak{p}} \bigoplus_{1 \le i \le k(\mathfrak{p})} \Lambda_{\mathcal{O}}^{(n)}/\mathfrak{p}^{e_i} \longrightarrow \mathcal{N} \to 0,$$

where $\mathcal{N}$ is a pseudo-null $\Lambda_{\mathcal{O}}^{(n)}$-quotient. Let $(\ell) \in \mathcal{L}_{\mathcal{O}}^{(n)}$ be a linear ideal such that $M/(\ell)M$ is a torsion $\Lambda_{\mathcal{O}}^{(n)}/(\ell)$-module. Note that the multiplication by ℓ is injective on $\bigoplus_{\mathfrak{p}} \bigoplus_{1 \le i \le k(\mathfrak{p})} \Lambda_{\mathcal{O}}^{(n)}/\mathfrak{p}^{e_i}$ and that the characteristic ideal of the $\Lambda_{\mathcal{O}}^{(n)}/(\ell)$-module of $\bigoplus_{\mathfrak{p}} \bigoplus_{1 \le i \le k(\mathfrak{p})} \Lambda_{\mathcal{O}}^{(n)}/((\ell), \mathfrak{p}^{e_i})$ is equal to the image of $\mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}}(M)$ in $\Lambda_{\mathcal{O}}^{(n)}/(\ell)$ in this case. By the snake lemma, we have the following exact sequence:

$$\begin{aligned} 0 \to \mathcal{N}[\ell] \longrightarrow (M/M_{\mathrm{null}})/(\ell)(M/M_{\mathrm{null}}) \\ \longrightarrow \bigoplus_{\mathfrak{p}} \bigoplus_{1 \le i \le k(\mathfrak{p})} \Lambda_{\mathcal{O}}^{(n)}/((\ell), \mathfrak{p}^{e_i}) \longrightarrow \mathcal{N}/(\ell)\mathcal{N} \to 0. \end{aligned}$$

By Lemma 3.1, we have:

$$\begin{aligned} &\mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}/(\ell)}\big((M/M_{\mathrm{null}})/(\ell)(M/M_{\mathrm{null}})\big) \\ &\qquad = \mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}/(\ell)}\Big(\bigoplus_{\mathfrak{p}} \bigoplus_{1 \le i \le k(\mathfrak{p})} \Lambda_{\mathcal{O}}^{(n)}/((\ell), \mathfrak{p}^{e_i})\Big). \end{aligned}$$

On the other hand, since multiplication map by ℓ is injective on M/M_{null}, we have the following exact sequence:

$$0 \to M_{\mathrm{null}}/(\ell)M_{\mathrm{null}} \longrightarrow M/(\ell)M \longrightarrow (M/M_{\mathrm{null}})/(\ell)(M/M_{\mathrm{null}}) \to 0.$$

Hence (ℓ) is contained in $\mathcal{L}_{\mathcal{O}}^{(n)}(M)$ if and only if $(\ell) \in \mathcal{L}_{\mathcal{O}}^{(n)}(M_{\mathrm{null}})$. This completes the proof of 3). □

Let us investigate the set $\mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N})$ for a pseudo-null $\Lambda_{\mathcal{O}}^{(n)}$-module $\mathcal{N}$. For this purpose, we introduce the specialization map of $\mathcal{L}_{\mathcal{O}}^{(n)}$. Let $\mathbb{F}_{\mathcal{O}}$ be the residue field of $\mathcal{O}$. We denote by $\mathrm{Sp}_{\mathcal{O}}$ the following specialization map

$$\mathcal{L}_{\mathcal{O}}^{(n)} \cong \mathcal{M}_{\mathcal{O}} \times \mathbb{P}^{n-1}(\mathcal{O}) \longrightarrow \mathbb{P}^{n-1}(\mathbb{F}_{\mathcal{O}}),$$
$$\big(a, (x_0 : \cdots : x_{n-1})\big) \longmapsto (\overline{x}_0 : \cdots : \overline{x}_{n-1}),$$

where $\overline{x}_i \in \mathbb{F}_{\mathcal{O}}$ is the reduction modulo $\mathcal{M}_{\mathcal{O}}$ of $x_i \in \mathcal{O}$ for each $0 \leq i \leq n-1$.

LEMMA 3.5. — *Let $n \geq 2$. We have the following statements*:

1) *Let $\mathcal{N}$ be a finitely generated pseudo-null $\Lambda_{\mathcal{O}}^{(n)}$-module and let $\{P_j\}_{1\leq j\leq k}$ the set of the associated primes of height two for $\mathcal{N}$. Then we have*:

$$\mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}) = \bigcap_{1\leq j\leq k} \mathcal{L}_{\mathcal{O}}^{(n)}(\Lambda_{\mathcal{O}}^{(n)}/P_i).$$

2) *Let P be a height 2 prime of $\Lambda_{\mathcal{O}}^{(n)}$. The set $\mathcal{L}_{\mathcal{O}}^{(n)}(\Lambda_{\mathcal{O}}^{(n)}/P)$ contains $(\ell) \in \mathcal{L}_{\mathcal{O}}^{(n)}$ if and only if (ℓ) is not a sub-ideal of P. The complement $\mathcal{L}_{\mathcal{O}}^{(n)} \setminus \mathcal{L}_{\mathcal{O}}^{(n)}(\Lambda_{\mathcal{O}}^{(n)}/P)$ is infinite if and only if P contains at least two different ideals $(\ell_1),(\ell_2) \in \mathcal{L}_{\mathcal{O}}^{(n)}$. Further, if $\mathcal{L}_{\mathcal{O}}^{(n)} \setminus \mathcal{L}_{\mathcal{O}}^{(n)}(\Lambda_{\mathcal{O}}^{(n)}/P)$ is infinite, there exist two linear elements $\ell,\ell' \in \Lambda_{\mathcal{O}}^{(n)}$ such that P is equal to (ℓ,ℓ').*

3) *Let $P = (\ell,\ell')$ be a height 2 prime of $\Lambda_{\mathcal{O}}^{(n)}$ generated by two linear elements. If P contains the ideal $(\pi_{\mathcal{O}})$, there exists an element $\overline{x} \in \mathbb{P}^{n-1}(\mathbb{F}_{\mathcal{O}})$ such that the complement $\mathcal{L}_{\mathcal{O}}^{(n)} \setminus \mathcal{L}_{\mathcal{O}}^{(n)}(\Lambda_{\mathcal{O}}^{(n)}/P)$ is equal to the inverse image $(\mathrm{Sp}_{\mathcal{O}})^{-1}(\overline{x})$ of $\overline{x}$. If P does not contain the ideal $(\pi_{\mathcal{O}})$, the complement $\mathcal{L}_{\mathcal{O}}^{(n)} \setminus \mathcal{L}_{\mathcal{O}}^{(n)}(\Lambda_{\mathcal{O}}^{(n)}/P)$ is isomorphic to $\mathbb{P}^1(\mathcal{O})$.*

Proof. — First, we show the assertion 1). If all prime ideals in the set $\mathrm{Ass}_{\Lambda_{\mathcal{O}}^{(n)}}(\mathcal{N})$ of the associated primes of a pseudo-null $\Lambda_{\mathcal{O}}^{(n)}$-module $\mathcal{N}$ have height greater than 2, the set $\mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N})$ is equal to $\mathcal{L}_{\mathcal{O}}^{(n)}$. Hence we have nothing to prove in this case. If $\mathcal{N}$ is the extension $0 \to \mathcal{N}' \to \mathcal{N} \to \mathcal{N}'' \to 0$ of two pseudo-null $\Lambda_{\mathcal{O}}^{(n)}$-modules $\mathcal{N}'$ and $\mathcal{N}''$, we have $\mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}) \supset \mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}') \cap \mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}'')$ by definition. For a linear element $\ell \in \Lambda_{\mathcal{O}}$, consider the exact sequence:

$$\mathcal{N}''[\ell] \longrightarrow \mathcal{N}'/(\ell)\mathcal{N}' \longrightarrow \mathcal{N}/(\ell)\mathcal{N} \longrightarrow \mathcal{N}''/(\ell)\mathcal{N}'' \to 0.$$

By the surjectivity of the last map, we have $\mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}) \subset \mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}'')$. If ℓ is contained in $\mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}) \setminus (\mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}') \cap \mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}'')) = \mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}) \setminus \mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}')$, $\mathcal{N}''/(\ell)\mathcal{N}''$ and $\mathcal{N}''[\ell]$ must be a pseudo-null $\Lambda_{\mathcal{O}}^{(n)}/(\ell)$-module by Lemma 3.1. Thus we have $\mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}) = \mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}') \cap \mathcal{L}_{\mathcal{O}}^{(n)}(\mathcal{N}'')$. If $\mathrm{Ass}_{\Lambda_{\mathcal{O}}^{(n)}}(\mathcal{N})$ contains a

prime $\mathfrak{p} \subset \Lambda_{\mathcal{O}}^{(n)}$ such that $\mathrm{ht}(\mathfrak{p}) \geq 3$, $\mathcal{N}$ has a submodule which is isomorphic to $\Lambda_{\mathcal{O}}^{(n)}/\mathfrak{p}$ (see [Ma], Theorem 6.4). Since $\mathcal{L}_{\mathcal{O}}^{(n)}(\Lambda_{\mathcal{O}}^{(n)}/\mathfrak{p}) = \mathcal{L}_{\mathcal{O}}^{(n)}$, we may replace $\mathcal{N}$ by a quotient of $\mathcal{N}$ by $\Lambda_{\mathcal{O}}^{(n)}/\mathfrak{p}$ in order to investigate the set $\mathcal{N}$. Since $\mathcal{N}$ is finitely generated, we may suppose that $\mathrm{Ass}_{\Lambda_{\mathcal{O}}^{(n)}}(\mathcal{N})$ consists only of prime ideals $\{P_j\}_{1 \leq j \leq k}$ of height 2 by repeating the above process. Thus $\mathcal{N}$ is a successive extension of a $\Lambda_{\mathcal{O}}^{(n)}$-module of type $\Lambda_{\mathcal{O}}^{(n)}/P_i$ (see [Ma], Theorem 6.4). This completes the proof of 1).

Let P be a height 2 prime of $\Lambda_{\mathcal{O}}^{(n)}$. The first two statements in 2) are rather clear. Let us assume that P contains an ideal (f, g) such that (f) and (g) are different linear ideals. If (f, g) is a prime, we must have $P = (f, g)$ since both ideals are of height 2. Suppose that (f, g) is not a prime. By replacing (f, g) with a suitable linear transform (f^σ, g^σ) if necessary, we may assume that $f = X_n + a$ with $a \in \mathcal{O}$. Let $\overline{g} \in \Lambda_{\mathcal{O}}^{(n)}/(f) = \mathcal{O}[[X_1, \ldots, X_{n-1}]]$ be the image of g by the specialization modulo (f). Since the degree of $\overline{g} \in \mathcal{O}[[X_1, \ldots, X_{n-1}]]$ is at most 1, $\overline{g}$ must be divisible by $\pi_{\mathcal{O}}$ if (f, g) is not a prime of $\Lambda_{\mathcal{O}}^{(n)}$. Let us write as $\overline{g} = \pi_{\mathcal{O}}^e \cdot \overline{g}'$ where $\overline{g}'$ is not divisible by $\pi_{\mathcal{O}}$. A height 1 primes of $\mathcal{O}[[X_1, \ldots, X_{n-1}]]$ which contains a principal ideal $(\overline{g})$ are only $(\pi_{\mathcal{O}})$ or $(\overline{g}')$ (if $\overline{g}'$ is not a unit). Hence P is either the inverse image of $(\pi_{\mathcal{O}})$ or $(\overline{g}')$ via $\Lambda_{\mathcal{O}}^{(n)} \to \Lambda_{\mathcal{O}}^{(n)}/(f)$. In the former case, P is equal to $(f, \pi_{\mathcal{O}}) = (f, f + \pi_{\mathcal{O}})$. In the latter case, let us regard $\overline{g}'$ as an element of $\Lambda_{\mathcal{O}}^{(n)}$ via the natural injection $\mathcal{O}[[X_1, \ldots, X_{n-1}]] \hookrightarrow \Lambda_{\mathcal{O}}^{(n)}$ and denote it by g'. Then (f, g') is the inverse image of $(\overline{g}')$ via $\Lambda_{\mathcal{O}}^{(n)} \longrightarrow \Lambda_{\mathcal{O}}^{(n)}/(f)$. This completes the proof of 2).

Let $P = (\ell, \ell')$ be a height 2 prime such that ℓ, ℓ' are linear elements. First, we suppose that P contains the ideal $(\pi_{\mathcal{O}})$. By this assumption, $P = (\ell, \pi_{\mathcal{O}})$ for a suitable linear element ℓ. If another linear element f is contained in P, we have $f = u\ell + u'\pi_{\mathcal{O}}$ with $u, u' \in \Lambda_{\mathcal{O}}^{(n)}$. Hence f is congruent to ℓ modulo $\pi_{\mathcal{O}}$. If $\overline{x} \in \mathbb{P}^{n-1}(\mathbb{F}_{\mathcal{O}})$ is the point corresponding to the reduction modulo $\pi_{\mathcal{O}}$ of ℓ, (f) corresponds to a point in $(\mathrm{Sp}_{\mathcal{O}})^{-1}(\overline{x}) \subset \mathcal{M}_{\mathcal{O}} \times \mathbb{P}^{n-1}(\mathcal{O})$. Suppose P does not contain the ideal $(\pi_{\mathcal{O}})$. By replacing (ℓ, ℓ') with a suitable linear transform $(\ell^\sigma, \ell'^\sigma)$ if necessary, we may assume that $\ell = X_n + a$ with $a \in \mathcal{O}$ and that $\ell' = X_{n-1} + b$ with $b \in \mathcal{O}$. If ℓ'' is an element of P, $\ell'' = u\ell + u'\ell'$ with $u, u' \in \Lambda_{\mathcal{O}}^{(n)}$. By similar argument of comparison of coefficients as the proof of Lemma 3.4, 1), we prove that u, u' are contained in $\mathcal{O}$. Hence (ℓ'') corresponds to a point of $\mathcal{O}\ell \oplus \mathcal{O}\ell'/\sim \cong \mathbb{P}^1(\mathcal{O})$. This completes the proof of 3). □

We have the following proposition which characterizes the characteristic ideal of a given torsion $\Lambda_{\mathcal{O}}^{(n)}$-module for $n \geq 2$:

PROPOSITION 3.6. — *Let $n \geq 2$ be an integer and let M and N be a finitely generated torsion $\Lambda_{\mathcal{O}}^{(n)}$-modules. Then the following three statements are equivalent*:

1) *We have* $\mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}}(M) \supset \mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}}(N)$.

2) *Let $\mathcal{O}'$ be arbitrary complete discrete valuation ring which is finite flat over $\mathcal{O}$. Then, for all but finitely many $(\ell) \in \mathcal{L}_{\mathcal{O}'}^{(n)}(M_{\mathcal{O}'}) \cap \mathcal{L}_{\mathcal{O}'}^{(n)}(N_{\mathcal{O}'})$, we have the inclusion*

$$\mathrm{char}_{\Lambda_{\mathcal{O}'}^{(n)}/(\ell)}(M_{\mathcal{O}'}/(\ell)M_{\mathcal{O}'}) \supset \mathrm{char}_{\Lambda_{\mathcal{O}'}^{(n)}/(\ell)}(N_{\mathcal{O}'}/(\ell)N_{\mathcal{O}'}).$$

3) *There exists a complete discrete valuation ring $\mathcal{O}'$ which is finite flat over $\mathcal{O}$ such that we have the inclusion*

$$\mathrm{char}_{\Lambda_{\mathcal{O}'}^{(n)}/(\ell)}(M_{\mathcal{O}'}/(\ell)M_{\mathcal{O}'}) \supset \mathrm{char}_{\Lambda_{\mathcal{O}'}^{(n)}/(\ell)}(N_{\mathcal{O}'}/(\ell)N_{\mathcal{O}'})$$

for all but finitely many $(\ell) \in \mathcal{L}_{\mathcal{O}'}^{(n)}(M_{\mathcal{O}'}) \cap \mathcal{L}_{\mathcal{O}'}^{(n)}(N_{\mathcal{O}'})$.

We recall the following well-known lemma (see [Bo], Chapter 7, §3.8, Proposition 6, or [NSW], Theorem 5.3.4):

LEMMA 3.7. — *Let R be a complete Noetherian local ring with its maximal ideal $\mathcal{M}_R$. Assume that $R/\mathcal{M}_R$ is a finite field. Then we have the following statements*:

1) *$f(X) = \sum_{i \geq 0} a_i X^i \in R[[X]]$ is a unit in $R[[X]]$ if and only if the constant term a_0 is a unit of R.*

2) *Assume that there exist integers i such that a_i are units of R. Take $r \geq 0$ to be the minimal one among such i's. Then there exists a unique decomposition*

$$f(X)u(X) = X^r + b_{r-1}X^{r-1} + \cdots + b_1 X + b_0,$$

where $u(X)$ is a unit in $R[[X]]$ and b_i is contained in $\mathcal{M}_R$ for each $1 \leq i \leq r-1$.

We will prove the following lemma:

LEMMA 3.8 (weak preparation). — *For $n \geq 2$, let*

$$f(X_1, \ldots, X_n) = \sum_{\boldsymbol{r} \geq 0} a_{\boldsymbol{r}} \mathbb{X}^{\boldsymbol{r}} \in \mathcal{O}[[X_1, \ldots, X_n]]$$

($a_{\boldsymbol{r}} \in \mathcal{O}$ is the coefficient of $\mathbb{X}^{\boldsymbol{r}} = X_1^{r_1} \cdots X_n^{r_n}$) be a power series which is not a unit of $\mathcal{O}[[X_1, \ldots, X_n]]$. Assume that $f(\mathbb{X})$ is not divisible by $\pi_{\mathcal{O}}$. Then there exist a finite extension $\mathcal{O}'$ of $\mathcal{O}$ and a linear transform σ of $\mathcal{O}'[[X_1, \ldots, X_n]]$ such that

$$\sigma(f)(\mathbb{X}) = u(\mathbb{X}) \left(X_n^r + b_{r-1} X_n^{r-1} + \cdots + b_1 X_n + b_0 \right),$$

with a unit $u(\mathbb{X})$ in $\mathcal{O}'[[X_1, \ldots, X_n]]$ and an integer r, where b_i belongs to the maximal ideal of $\mathcal{O}'[[X_1, \ldots, X_{n-1}]]$ for $0 \leq i \leq r-1$.

Before the proof of this lemma, we give the following lemma:

LEMMA 3.9. — *Let $n \geq 1$ be an integer and let $V_{r,\overline{\mathbb{F}}_p}$ be a $\overline{\mathbb{F}}_p$-vector space $\bigoplus_{\deg(\boldsymbol{r})=r} \overline{\mathbb{F}}_p \cdot X_1^{r_1} \cdots X_n^{r_n}$ spanned by n-variable monomials of degree r over $\overline{\mathbb{F}}_p$. Let us denote by p_n the projection map $V_{r,\overline{\mathbb{F}}_p} \to \overline{\mathbb{F}}_p \cdot X_n^r$. Then, for any non-zero element $v \in V_{r,\overline{\mathbb{F}}_p}$, there exists an element $\overline{\sigma} \in \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ such that $p_n(\overline{\sigma}(v))$ is not zero.*

Proof. — For an element $w \in V_{r,\overline{\mathbb{F}}_p}$, the following statements are equivalent:

1) The projection $p_n(w) \in \overline{\mathbb{F}}_p \cdot X_n^r$ is not zero.

2) The value $w(0, \ldots 0, 1) \in \overline{\mathbb{F}}_p$ of w at $(X_1, \ldots, X_{n-1}, X_n) = (0, \ldots, 0, 1)$ is not zero.

Let $(\alpha_1, \cdots, \alpha_n) \in \overline{\mathbb{F}}_p^n$ be a point such that $x(\alpha_1, \ldots, \alpha_n) \in \overline{\mathbb{F}}_p$ is not zero. We take $\overline{\sigma} = (\overline{t}_{i,j})_{1 \leq i,j \leq n} \in \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ such that $\overline{t}_{n,j} \alpha_n = \alpha_j$ for each $1 \leq j \leq n$. Let us denote by $\overline{\sigma}(v) \in V_{r,\overline{\mathbb{F}}_p}$ the action given by $g \cdot X_j = \sum_{1 \leq i \leq n} \overline{t}_{i,j} X_i$ for $g = (a_{i,j})_{1 \leq i,j \leq n} \in \mathrm{GL}_n(\overline{\mathbb{F}}_p)$. Then $\overline{\sigma}(v)(0, \cdots, 0, 1) = v(\alpha_1, \ldots, \alpha_n) \neq 0$. This completes the proof. □

Let us return to the proof of Lemma 3.8.

Proof of Lemma 3.8. — Since $f(\mathbb{X})$ is not divisible by $\pi_{\mathcal{O}}$, there exists an n-tuple $\boldsymbol{r} = (r_1, \ldots, r_n)$ such that $a_{\boldsymbol{r}} \in \mathcal{O}^\times$. Let $V_{r,\mathbb{F}}$ be a $\mathbb{F}$-vector space $\bigoplus_{\deg(\boldsymbol{r})=r} \mathbb{F} \cdot X_1^{r_1} \cdots X_n^{r_n}$ spanned by n-variable monomials of degree r. Let $v = \sum_{\deg(\boldsymbol{r})=r} \overline{a}_{\boldsymbol{r}} X_1^{r_1} \cdots X_n^{r_n} \in V_{r,\mathbb{F}}$ an element obtained by the modulo $\pi_{\mathcal{O}}$-reduction of degree r-part of $f(\mathbb{X})$. By the assumption, v is not zero. Hence, by using the Lemma 3.9, after taking a finite extension $\mathbb{F}'$ of $\mathbb{F}$ if necessary, there exists $\overline{\sigma} \in \mathrm{GL}_n(\mathbb{F}')$ such that the coefficient of $\overline{\sigma}(v)$ at X_n^r is not zero. Let $\sigma = (t_{i,j})_{1 \leq i,j \leq n} \in \mathrm{GL}_n(W(\mathbb{F}'))$ be a lift of $\overline{\sigma} = (\overline{t}_{i,j})_{1 \leq i,j \leq n} \in \mathrm{GL}_n(\mathbb{F}')$

where $t_{i,j} \in W(\mathbb{F}')$ is the Teichmuller representative of $t_{i,j}$. Let $\mathcal{O}'$ be a finite extension of $\mathcal{O}$ which contains $W(\mathbb{F}')$. As a power series of X_n, $\sigma(f)(\mathbb{X}) \in \mathcal{O}'[[X_1, \dots, X_{n-1}]][[X_n]]$ is presented as

$$b'_0 + b'_1 X_n + \cdots + b'_{r-1} X_n^{r-1} + b'_r X_n^r + (\text{higher order terms})$$

where b'_i is contained in the maximal ideal of $\mathcal{O}'[[X_1, \dots, X_{n-1}]]$ for each $0 \leq i \leq r-1$ and b'_r is a unit of $\mathcal{O}'$. By applying Lemma 3.7 for this $\sigma(f)(\mathbb{X})$ and for $R = \mathcal{O}[[X_1, \cdots, X_{n-1}]]$, we complete the proof of Lemma 3.8. □

Let us return to the proof of Proposition 3.6.

Proof of Proposition 3.6. — The implications 1) ⇒ 2) ⇒ 3) are clear. Let us show the implication 3) ⇒ 1). Let us fix fundamental isomorphisms for M and N:

$$M \xrightarrow{f_M} \bigoplus_i \Lambda_{\mathcal{O}}^{(n)}/(\pi_{\mathcal{O}}^{\mu_i}) \oplus \bigoplus_j \Lambda_{\mathcal{O}}^{(n)}/(f_j(\mathbb{X}))^{\lambda_j},$$

$$N \xrightarrow{f_N} \bigoplus_{i'} \Lambda_{\mathcal{O}}^{(n)}/(\pi_{\mathcal{O}}^{\mu'_{i'}}) \oplus \bigoplus_{j'} \Lambda_{\mathcal{O}}^{(n)}/(g_{j'}(\mathbb{X}))^{\lambda'_{j'}},$$

where $\mathrm{Ker}(f_M)$ (resp. $\mathrm{Ker}(f_N)$) and $\mathrm{Coker}(f_M)$ (resp. $\mathrm{Coker}(f_N)$) are pseudo-null $\Lambda_{\mathcal{O}}^{(n)}$-modules and f_j's and $g_{j'}$'s are monic polynomials. Let $f(\mathbb{X}) = \prod_j f_j(\mathbb{X})^{n_j}$ (resp. $g(\mathbb{X}) = \prod_{j'} g_{j'}(\mathbb{X})^{n'_{j'}}$) and let $\mu = \sum_i \mu_i$ (resp. $\mu' = \sum_{i'} \mu'_{i'}$). In order to show that $\mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}}(M) \supset \mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}}(N)$, it suffices to show that the image of the ideal $(g(\mathbb{X}))$ (resp. $\pi_{\mathcal{O}}^{\mu'}$) is zero in the ring $\Lambda_{\mathcal{O}}^{(n)}/(f(\mathbb{X}))$ (resp. $\Lambda_{\mathcal{O}}^{(n)}/(\pi_{\mathcal{O}}^{\mu'})$). If $f(\mathbb{X})$ is a unit in $\Lambda_{\mathcal{O}}^{(n)}$, there is nothing to prove. We assume that $f(\mathbb{X})$ is not a unit in $\Lambda_{\mathcal{O}}^{(n)}$ from now on. By Lemma 3.8, after a finite base change $\mathcal{O}'$ of $\mathcal{O}$ and change of the coordinate by a linear transform, we may assume that $f(\mathbb{X})$ is of the form $f(\mathbb{X}) = (X_n^r + b_{r-1}X_n^{r-1} + \cdots + b_1 X_n + b_0)u(\mathbb{X})$ where b_i belongs to the maximal ideal of $\mathcal{O}'[[X_1, \dots, X_{n-1}]]$ for each $0 \leq i \leq r-1$ and $u(\mathbb{X})$ is a unit of $\Lambda_{\mathcal{O}'}^{(n)}$. The algebra $\Lambda_{\mathcal{O}'}^{(n)}/(f(\mathbb{X}))$ is finite flat over $\mathcal{O}'[[X_1, \dots, X_{n-1}]]$ ($\subset \Lambda_{\mathcal{O}'}^{(n)} = \mathcal{O}'[[X_1, \dots, X_n]]$). We have the following claim:

Claim 3.10. — *There exist a complete discrete valuation ring $\mathcal{O}''$ which is finite flat over $\mathcal{O}'$ and a set $\{(\ell_i) \in \mathcal{L}_{\mathcal{O}''}^{(n)}\}_{1 \leq i < \infty}$ satisfying the following properties*:

(i) *the ideals (ℓ_i) are all different*;

(ii) *for each $i \geq 1$, ℓ_i is contained in $\mathcal{O}''[[X_1, \dots, X_{n-1}]]$*;

(iii) *for each i, (ℓ_i) is contained in $\mathcal{L}_{\mathcal{O}''}^{(n)}(M_{\mathcal{O}''}) \cap \mathcal{L}_{\mathcal{O}''}^{(n)}(N_{\mathcal{O}''})$.*

By this claim, if we replace $\mathcal{O}'$ by a sufficiently large extension of $\mathcal{O}'$ if necessary, we may suppose that we have a set $\{(\ell_i) \in \mathcal{L}^{(n)}_{\mathcal{O}'}\}_{1\leq i<\infty}$ satisfying the above three properties. By the third condition of the claim, the image of $g(\mathbb{X})$ in $\Lambda^{(n)}_{\mathcal{O}'}/(f(\mathbb{X}),\ell_i)$ is zero for each i. By the first two conditions, for each $j \geq 1$ we have an injection

$$\mathcal{O}'[[X_1,\dots,X_{n-1}]]/(\ell_1\cdots\ell_j) \hookrightarrow \prod_{1\leq i\leq j} \mathcal{O}'[[X_1,\dots,X_{n-1}]]/(\ell_i).$$

Since the extension $\Lambda^{(n)}_{\mathcal{O}'}/(f(\mathbb{X}))$ is finite flat over $\mathcal{O}'[[X_1,\dots,X_{n-1}]]$, for each $j \geq 1$ we have an injection

$$\Lambda^{(n)}_{\mathcal{O}'}/(f(\mathbb{X}),\ell_1\cdots\ell_j) \hookrightarrow \prod_{1\leq i\leq j} \Lambda^{(n)}_{\mathcal{O}'}/(f(\mathbb{X}),\ell_i).$$

Thus the image of $g(\mathbb{X})$ in $\Lambda^{(n)}_{\mathcal{O}'}/(f(\mathbb{X}),\ell_1\cdots\ell_j)$ is zero for each $j \geq 1$. By the completeness of $\Lambda^{(n)}_{\mathcal{O}'}/(f(\mathbb{X}))$, we have

$$\varprojlim_j \Lambda^{(n)}_{\mathcal{O}'}/(f(\mathbb{X}),\ell_1\cdots\ell_j) \cong \Lambda^{(n)}_{\mathcal{O}'}/(f(\mathbb{X}))$$

and $g(\mathbb{X})$ must be zero in $\Lambda^{(n)}_{\mathcal{O}'}/(f(\mathbb{X}))$. As for the inclusion $(\pi^{\mu}_{\mathcal{O}'}) \supset (\pi^{\mu}_{\mathcal{O}'})$ in $\Lambda^{(n)}_{\mathcal{O}'}$, it suffices to find only one linear element $\ell \in \mathcal{L}^{(n)}_{\mathcal{O}'}(M_{\mathcal{O}'}) \cap \mathcal{L}^{(n)}_{\mathcal{O}'}(N_{\mathcal{O}'})$. Then the element $\pi^{\mu}_{\mathcal{O}'}$ (resp.$\pi^{\mu}_{\mathcal{O}'}$) is equal to the highest power of $\pi_{\mathcal{O}}$ dividing the characteristic power series of $M_{\mathcal{O}'}/(\ell)M_{\mathcal{O}'}$ (resp. $N_{\mathcal{O}'}/(\ell)N_{\mathcal{O}'}$). This completes the proof assuming the above claim.

Finally, we give the proof of Claim 3.10. By Lemma 3.4, 3), $\mathcal{L}^{(n)}_{\mathcal{O}'}(M_{\mathcal{O}'}) \cap \mathcal{L}^{(n)}_{\mathcal{O}'}(N_{\mathcal{O}'})$ is equal to $\mathcal{L}^{(n)}_{\mathcal{O}'}((M_{\mathrm{null}} \oplus M_{\mathrm{null}})_{\mathcal{O}'})$, where M_{null} (resp. N_{null}) is the largest pseudo-null submodule of M (resp. N). The set of linear ideals of $\Lambda^{(n-1)}_{\mathcal{O}'} = \mathcal{O}'[[X_1,\dots,X_{n-1}]]$ is $\mathcal{L}^{(n)}_{\mathcal{O}'} = \mathcal{M}_{\mathcal{O}'} \times \mathbb{P}^{n-2}(\mathcal{O}')$. By Lemma 3.5, $\mathcal{L}^{(n)}_{\mathcal{O}'} \setminus \mathcal{L}^{(n)}_{\mathcal{O}'}((M_{\mathrm{null}} \oplus M_{\mathrm{null}})_{\mathcal{O}'})$ is of the following form:

$$\Big(\bigcup_{1\leq i\leq j} x_i\Big) \cup \Big(\bigcup_{1\leq i'\leq j'} \mathrm{Sp}^{-1}_{\mathcal{O}'}(\overline{y}_{i'})\Big) \cup \Big(\bigcup_{1\leq i''\leq j''} \mathbb{P}^1(\mathcal{O}')\Big),$$

where x_i is an element of $\mathbb{P}^{n-1}(\mathcal{O}')$ for each i, $\overline{y}_{i'}$ is an element of $\mathbb{P}^{n-1}(\mathbb{F}_{\mathcal{O}'})$ for each i'. Note that the inverse image $\mathrm{Sp}^{-1}_{\mathcal{O}'}(\mathbb{P}^{n-2}(\mathbb{F}_{\mathcal{O}'}))$ is contained in $\mathcal{L}^{(n)}_{\mathcal{O}'}$. Let $n \geq 3$. By replacing $\mathcal{O}'$ by a sufficiently large unramified extension if necessary, we choose $\overline{x} \in \mathbb{P}^{n-2}(\mathbb{F}_{\mathcal{O}'})$ which is equal to none of $\overline{y}_{i'}$. Then $\mathrm{Sp}^{-1}_{\mathcal{O}'}(\overline{x}) \cap (\bigcup_{1\leq i'\leq j'} \mathrm{Sp}^{-1}_{\mathcal{O}'}(\overline{y}_{i'}))$ is empty and

$\mathrm{Sp}_{\mathcal{O}'}^{-1}(\overline{x}) \cap (\bigcup_{1 \leq i'' \leq j''} \mathbb{P}^1(\mathcal{O}'))$ is finite. Thus, if we choose arbitrary sequence of different linear ideals $(\ell_i) \in \mathrm{Sp}_{\mathcal{O}'}^{-1}(\overline{x}) \setminus (\bigcup_{1 \leq i \leq j} x_i \cup \bigcup_{1 \leq i'' \leq j''} \mathbb{P}^1(\mathcal{O}'))$, this satisfies the three conditions of the claim. Let $n = 2$. If one of $\overline{y}_{i'} \in \mathbb{P}^1(\mathbb{F}_{\mathcal{O}'})$ coincides with the point $\overline{y}_0$ corresponding to $\mathrm{Sp}_{\mathcal{O}'}(\mathcal{L}_{\mathcal{O}'}^{(1)})$, we can not choose $\overline{x}$ as in the case of $n \geq 3$. Hence, if $\overline{y}_0$ coincides with one of $\overline{y}_{i''}$, we need to replace $\mathcal{O}'$ by a sufficiently large unramified extension and replace a transform $\overline{\sigma}$ in Lemma 3.9 so that $\mathrm{Sp}_{\mathcal{O}'}(\mathcal{L}_{\mathcal{O}'}^{(1)})$ is different from all $\overline{y}_{i'}$. If we choose arbitrary sequence of different linear ideals $(\ell_i) \in \mathrm{Sp}_{\mathcal{O}'}^{-1}(\overline{y}_0) \setminus (\bigcup_{1 \leq i \leq j} x_i \cup \bigcup_{1 \leq i'' \leq j''} \mathbb{P}^1(\mathcal{O}'))$, this satisfies the three conditions of the claim. □

Next, we discuss how to recover the characteristic ideal of a torsion $\Lambda_{\mathcal{O}}^{(n)}$-module in the case of $n = 1$. For short, we denote $\Lambda_{\mathcal{O}}^{(1)}$ (resp. $\mathcal{L}_{\mathcal{O}}^{(1)}$) by $\Lambda_{\mathcal{O}}$ (resp. $\mathcal{L}_{\mathcal{O}}$), when $n = 1$.

Recall that a monic polynomial

$$E(X) = X^e + a_{e-1}X^{e-1} + \cdots + a_1 X + a_0 \in \mathcal{O}[X]$$

is called *an Eisenstein polynomial* if the i-th coefficient a_i is contained in the maximal ideal $\mathcal{M}_{\mathcal{O}}$ of $\mathcal{O}$ for each $0 \leq i \leq e-1$ and $\pi_{\mathcal{O}}$ divides a_0 exactly. It is known that $\mathcal{O}_E = \mathcal{O}[X]/(E(X))$ is a complete discrete valuation ring whose fraction field $\mathrm{Frac}(\mathcal{O}_E)$ is a totally ramified extension of $\mathrm{Frac}(\mathcal{O})$ and that the image of X in $\mathcal{O}_E$ is a uniformizer of $\mathcal{O}_E$. Note that an Eisenstein polynomial $E(X) \in \mathcal{O}[X]$ is not a unit in a power series algebra $\mathcal{O}[[X]]$ and $\mathcal{O}[X]/(E(X))$ is isomorphic to $\mathcal{O}[[X]]/(E(X))$.

A set of ideals $\mathcal{E}_{\mathcal{O}} = \{I_m \subset \Lambda_{\mathcal{O}} \mid m \in \mathbb{Z}_{\geq 1}\}$ is called Eisenstein type if $I_m = (E_m(X))$ where $E_m(X)$ is an Eisenstein polynomial of degree m in $\mathcal{O}[X]$ for each $m \geq 1$. The result is as follows:

PROPOSITION 3.11. — *Let M and N be finitely generated torsion $\mathcal{O}[[X]]$-modules. We have the following*:

1) *The following conditions are equivalent*:

   (a) *There exists an integer $h \geq 0$ such that* $\mathrm{char}_{\Lambda_{\mathcal{O}}}(M) \supset (\pi_{\mathcal{O}}^h)\mathrm{char}_{\Lambda_{\mathcal{O}}}(N)$.

   (b) *Let $\mathcal{O}'$ be arbitrary complete discrete valuation ring which is finite flat over $\mathcal{O}$. Then there exists a constant c depending only on $M_{\mathcal{O}'}$ and $N_{\mathcal{O}'}$ such that $\sharp(M_{\mathcal{O}'}/IM_{\mathcal{O}'})$ divides $c \cdot \sharp(N_{\mathcal{O}'}/IN_{\mathcal{O}'})$ for all but finitely many $I \in \mathcal{L}_{\mathcal{O}'}$.*

2) *As for the difference by the constant ideal* $(\pi_{\mathcal{O}}^h)$, *we have the following equivalence*:

(a) *Let* $M_{(\pi_{\mathcal{O}})}$ (*resp.* $N_{(\pi_{\mathcal{O}})}$) *be the localization of* M (*resp.* N) *at the prime ideal* $(\pi_{\mathcal{O}})$. *Then we have*

$$\mathrm{length}_{(\Lambda_{\mathcal{O}})_{(\pi_{\mathcal{O}})}}\big(M_{(\pi_{\mathcal{O}})}\big) \leq \mathrm{length}_{(\Lambda_{\mathcal{O}})_{(\pi_{\mathcal{O}})}}\big(N_{(\pi_{\mathcal{O}})}\big).$$

(b) *There exist a set of ideals* $\mathcal{E}_{\mathcal{O}} = \{I_m \mid m \in \mathbb{Z}_{\geq 1}\}$ *of Eisenstein type and a constant* c *depending only on* M *and* N *such that* $\sharp(M/I_mM)$ *divides* $c \cdot \sharp(N/I_mN)$ *for all but finitely many* I_m.

Proof. — Let us fix fundamental sequences for given torsion $\Lambda_{\mathcal{O}}$-modules:

$$M \xrightarrow{f_M} \bigoplus_i \Lambda_{\mathcal{O}}/(\pi_{\mathcal{O}}^{\mu_i}) \oplus \bigoplus_j \Lambda_{\mathcal{O}}/(f_j(X))^{\lambda_j}$$
$$N \xrightarrow{f_N} \bigoplus_{i'} \Lambda_{\mathcal{O}}/(\pi_{\mathcal{O}}^{\mu'_{i'}}) \oplus \bigoplus_{j'} \Lambda_{\mathcal{O}}/(g_{j'}(X))^{\lambda'_{j'}},$$

where $\mathrm{Ker}(f_M)$ (resp. $\mathrm{Ker}(f_N)$) and $\mathrm{Coker}(f_M)$ (resp. $\mathrm{Coker}(f_N)$) are finite groups and $f_j(X)$ (resp. $g_{j'}(X)$) is a monic polynomial for each j (resp. j'). Let $\mathcal{O}'$ be arbitrary complete discrete valuation ring which is finite flat over $\mathcal{O}$. Let us denote $\prod f_j(X) \in \mathcal{O}[[X]]$ (resp. $\prod g_j(X) \in \mathcal{O}[[X]]$) by $f(X)$ (resp. $g(X)$). Put $\mu = \sum_i \mu_i$ (resp. $\mu' = \sum_{i'} \mu'_{i'}$). By a simple diagram chasing argument using the snake lemma, we see that

$$\begin{aligned}\sharp(M_{\mathcal{O}'}/IM_{\mathcal{O}'}) = \sharp\Lambda_{\mathcal{O}'}/((\pi_{\mathcal{O}}^{\mu}), I) \cdot \sharp\Lambda_{\mathcal{O}'}/((f(X)), I) \\ \cdot \sharp\big(\mathrm{Ker}(f_M) \otimes_{\mathcal{O}} \mathcal{O}'/I\mathrm{Ker}(f_M) \otimes_{\mathcal{O}} \mathcal{O}'\big),\\ \sharp(N_{\mathcal{O}'}/IN_{\mathcal{O}'}) = \sharp\Lambda_{\mathcal{O}'}/((\pi_{\mathcal{O}}^{\mu'}), I) \cdot \sharp\Lambda_{\mathcal{O}'}/((g(X)), I) \\ \cdot \sharp\big(\mathrm{Ker}(f_N) \otimes_{\mathcal{O}} \mathcal{O}'/I\mathrm{Ker}(f_N) \otimes_{\mathcal{O}} \mathcal{O}'\big)\end{aligned}$$

for any $I \in \mathcal{L}_{\mathcal{O}'} \cup \mathcal{E}_{\mathcal{O}'}$ such that $M_{\mathcal{O}'}/IM_{\mathcal{O}'}$ and $N_{\mathcal{O}'}/IN_{\mathcal{O}'}$ are finite. Hence we may replace $M_{\mathcal{O}'}$ (resp. $N_{\mathcal{O}'}$) by a fundamental type module $\Lambda_{\mathcal{O}'}/(\pi_{\mathcal{O}}^{\mu}) \oplus \Lambda_{\mathcal{O}'}/(f(X))$ (resp. $\Lambda_{\mathcal{O}'}/(\pi_{\mathcal{O}}^{\mu'}) \oplus \Lambda_{\mathcal{O}'}/(g(X))$) in order to show the equivalence between (a) and (b). For the fundamental type modules above, the implication (a) $\Rightarrow$ (b) is easy to see in both cases (a) and (b). In the rest of the proof, we show the implication (b) $\Rightarrow$ (a) for such fundamental type modules.

Let us consider the first statement 1). Take fundamental modules $M = \Lambda_{\mathcal{O}}/(\pi_{\mathcal{O}}^{\mu}) \oplus \Lambda_{\mathcal{O}}/(f(X))$ and $N = \Lambda_{\mathcal{O}}/(\pi_{\mathcal{O}}^{\mu'}) \oplus \Lambda_{\mathcal{O}}/(g(X))$. Suppose

that $f(X)$ does not divide $g(X)$. We will deduce a contradiction to the statement (b) from this assumption. Let $\mathcal{O}' \subset \overline{\mathbb{Z}}_p$ be a complete discrete valuation ring which is finite flat over $\mathcal{O}$ which contains all roots of $f(X)$ and $g(X)$. Thus we have a decomposition $f(X) = \prod(X - \alpha_i)^{s_i}$ (resp. $g(X) = \prod(X - \beta_j)^{t_j}$) with $\alpha_i \in \mathcal{O}'$ (resp. $\beta_j \in \mathcal{O}'$) such that $\alpha_i \neq \alpha_{i'}$ (resp. $\beta_j \neq \beta_{j'}$) if $i \neq i'$ (resp. $j \neq j'$).

If $f(X)$ does not divide $g(X)$, there exists i_0 such that $(X - \alpha_{i_0})^{s_{i_0}}$ does not divide $g(X)$. For each $m \geq 1$, we define $(\ell_m) \in \mathcal{L}_{\mathcal{O}'}$ to be $(\ell_m) = (X - \alpha_{i_0} - p^m)$. The order of $\Lambda_{\mathcal{O}'}/(\pi_{\mathcal{O}}^{\mu}, \ell_m)$ is bounded independent of m. Thus the order of $M_{\mathcal{O}'}/(\ell_m)M_{\mathcal{O}'} = \Lambda_{\mathcal{O}'}/(\pi_{\mathcal{O}}^{\mu}, \ell_m) \oplus \Lambda_{\mathcal{O}'}/(f(X), \ell_m))$ is equal to $\sharp(\mathcal{O}'/p^m)^{a_{i_0}}$ modulo a finite error bounded independent of m. On the other hand, the order of $N_{\mathcal{O}'}/(\ell_m)N_{\mathcal{O}'} = \Lambda_{\mathcal{O}'}/(\pi_{\mathcal{O}}^{\mu'}, \ell_m) \oplus \Lambda_{\mathcal{O}'}/(g(X), \ell_m)$ is equal to $\sharp(\mathcal{O}'/p^m)^{t_{i_0}}$ modulo a finite error bounded independent of m, where the number $t_{i_0} \geq 0$ is the maximal integer such that $(X - \alpha_{i_0})^{t_{i_0}}$ divides $g(X)$. Since we assume $t_{i_0} < s_{i_0}$, $\sharp(N_{\mathcal{O}'}/(\ell_m)N_{\mathcal{O}'})/\sharp(M_{\mathcal{O}'}/(\ell_m)M_{\mathcal{O}'})$ converges to zero when m tends to ∞. This contradicts to the statement (b) of 1).

Next, we prove the statement 2). We assume that $\pi_{\mathcal{O}}^{\mu}$ does not divides $\pi_{\mathcal{O}}^{\mu'}$, namely $\mu > \mu'$. In this case, we consider a sequence $I_m \in \mathcal{E}_{\mathcal{O}}$ such that the extension degree e_m of $\Lambda_{\mathcal{O}}/I_m$ over $\mathcal{O}$ tends to ∞. The order of $\Lambda_{\mathcal{O}}/(\pi_{\mathcal{O}}^{\mu}, I_m)$ (resp. $\Lambda_{\mathcal{O}}/(\pi_{\mathcal{O}}^{\mu'}, I_m)$) is equal to $\sharp(\mathcal{O}/\pi_{\mathcal{O}})^{e_m\mu}$ (resp. $\sharp(\mathcal{O}/\pi_{\mathcal{O}})^{e_m\mu'}$). On the other hand, the order of $\Lambda_{\mathcal{O}}/(f(X), I_m)$ (resp. $\Lambda_{\mathcal{O}}/(g(X), I_m)$) is bounded by a finite constant independent of m. Hence $\sharp(N/I_mN)/\sharp(M/I_mM)$ converges to zero when m tends to ∞. This again contradicts to the statement (b) of 2). This completes the proof. □

4. Proof of the main theorem.

In this section, we give a proof of Theorem 2.4 for an Euler system over an n-variable Iwasawa algebra $\Lambda_{\mathcal{O}}^{(n)}$. We reduce Theorem 2.4 to the Euler system theory over discrete valuation rings (Theorem 4.7) by using a method of specializations of Iwasawa modules established in §3 (cf. Proposition 3.6 and Proposition 3.11).

First, we prepare the following lemmas:

LEMMA 4.1. — *Let $n \geq 1$ and let M be a finitely generated $\Lambda_{\mathcal{O}}^{(n)}$-module. We denote by M_{tor}* (resp. M_{null}) *the largest torsion* (*resp. pseudo-null*) *$\Lambda_{\mathcal{O}}^{(n)}$-submodule of M. Then, for each height 1 prime I of $\Lambda_{\mathcal{O}}^{(n)}$ such*

that I is prime to the characteristic ideal of M_{tor}, we have an isomorphism $M[I] \cong M_{\mathrm{null}}[I]$.

See [Oc1] for the proof of the above lemma in the case $n = 1$. We prove the above lemma by using a fundamental isomorphism of torsion $\Lambda_{\mathcal{O}}^{(n)}$-module (cf. [Bo], Chapter 7). Since the proof for general n is done exactly in the same way as the case $n = 1$, we omit the proof here.

Let N be a finite discrete module with continuous $G_{\mathbb{Q}}$-action unramified outside a finite set of primes S of $\mathbb{Q}$. We define the Tate-Shafarevich group $Ш_S^i(N)$ to be the kernel of the restriction map $H^i(\mathbb{Q}_S/\mathbb{Q}, N) \to \bigoplus_{v\in S} H^i(\mathbb{Q}_v, N)$. For an inductive system $\{M_j\}$ (resp. projective system $\{N_j\}$) of finite discrete $G_{\mathbb{Q}}$-modules, we define

$$Ш_S^i(\varinjlim_j M_j)$$

(resp. $Ш_S^i(\varprojlim_j N_j)$) to be the inductive limit $\varinjlim_j (Ш_S^i(M_j))$ (resp. projective limit $\varprojlim_j (Ш_S^i(N_j))$).

Since $\varinjlim_j H^i(\mathbb{Q}_S/\mathbb{Q}, M_j)$ (resp. $\varinjlim_j H^i(\mathbb{Q}_v, M_j)$) is isomorphic to $H^i(\mathbb{Q}_S/\mathbb{Q}, \varinjlim_j M_j)$ (resp. $H^i(\mathbb{Q}_v, \varinjlim_j M_j)$) (cf. [Se], Proposition 8), $Ш_S^i(\varinjlim_j M_j)$ is equal to the kernel of

$$H^i(\mathbb{Q}_S/\mathbb{Q}, \varinjlim_j M_j) \longrightarrow \bigoplus_{v\in S} H^i(\mathbb{Q}_v, \varinjlim_j M_j).$$

$Ш_S^i(\varprojlim_j N_j)$ is equal to the kernel of

$$H^i(\mathbb{Q}_S/\mathbb{Q}, \varprojlim_j N_j) \longrightarrow \bigoplus_{v\in S} H^i(\mathbb{Q}_v, \varprojlim_j N_j)$$

since $\varprojlim_j H^i(\mathbb{Q}_S/\mathbb{Q}, N_j)$ (resp. $\varprojlim_j H^i(\mathbb{Q}_v, N_j)$) is isomorphic to $H^i(\mathbb{Q}_S/\mathbb{Q}, \varprojlim_j N_j)$ (resp. $H^i(\mathbb{Q}_v, \varprojlim_j N_j)$) by [Ta], Corollary (2.2).

The following proposition is a part of the global duality theorem (cf. [NSW], Chapter VIII):

Lemma 4.2. — *For a finite discrete $G_{\mathbb{Q}}$-module M unramified outside a finite set of primes S, the Tate-Shafarevich groups $Ш_S^1(N)$ and $Ш_S^2(N^\vee(1))$ are finite and we have a canonical perfect pairing*:

$$Ш_S^1(N) \times Ш_S^2\big(N^\vee(1)\big) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

The following two lemmas will be a key to the reduction step of the proof of Theorem 2.4:

LEMMA 4.3. — *Let the assumptions and the notations be as in Theorem* 2.4. *We have the following statements*:

1) *Let I be a height* 1 *prime of $\Lambda_{\mathcal{O}}^{(n)}$. We denote by $\overline{\mathcal{T}}_I$ be the quotient module $\overline{\mathcal{T}}/I\overline{\mathcal{T}}$. Then the natural map $Ш_S^2(\overline{\mathcal{T}})/IШ_S^2(\overline{\mathcal{T}}) \xrightarrow{p_I} Ш_S^2(\overline{\mathcal{T}}_I)$ is surjective. Especially, if $(\Lambda_{\mathcal{O}}^{(n)})$-module $Ш_S^2(\overline{\mathcal{T}})$ admits a set of generators consisting k elements, $(\Lambda_{\mathcal{O}}^{(n)}/I)$-module $Ш_S^2(\overline{\mathcal{T}}_I)$ admits a set of generators consisting of k elements.*

2) *For all but finitely many height* 1 *prime ideals I of $\Lambda_{\mathcal{O}}^{(n)}$, $\mathrm{Ker}(p_I)$ is a torsion $\Lambda_{\mathcal{O}}^{(n)}/I$-module. Further, $\mathrm{Ker}(p_I)$ is a subquotient of $\mathcal{P}[I]$ for all but finitely many height* 1 *primes I. Here $\mathcal{P}$ is the largest pseudo-null $\Lambda_{\mathcal{O}}^{(n)}$-submodule of $\bigoplus_{v\in S}(\mathcal{T}^*)_{G_{\mathbb{Q}_v}}$, where $\mathcal{T}^* = \mathrm{Hom}_{\Lambda_{\mathcal{O}}^{(n)}}(\mathcal{T}, \Lambda_{\mathcal{O}}^{(n)})$. Especially, the order of the kernel of $Ш_S^2(\overline{\mathcal{T}})/IШ_S^2(\overline{\mathcal{T}}) \to Ш_S^2(\overline{\mathcal{T}}_I)$ is bounded by the order of a finite group $\mathcal{P}$ for all but finitely many height* 1 *primes I of $\Lambda_{\mathcal{O}}$ when $n = 1$.*

Proof. — By the global duality theorem (Proposition 4.2), $Ш_S^2(\overline{\mathcal{T}})$ is the Pontryagin dual of $Ш_S^1(\mathcal{A})$, where $\mathcal{A}$ is the discrete Galois representation $\mathcal{T} \otimes_{\Lambda_{\mathcal{O}}^{(n)}} \mathrm{Hom}_{\mathbb{Z}_p}(\Lambda_{\mathcal{O}}^{(n)}, \mathbb{Q}_p/\mathbb{Z}_p)$. By taking the Pontryagin dual of the map $Ш_S^2(\overline{\mathcal{T}})/IШ_S^2(\overline{\mathcal{T}}) \to Ш_S^2(\overline{\mathcal{T}}_I)$, it suffices to prove that the restriction map $Ш_S^1(\mathcal{A}[I]) \to Ш_S^1(\mathcal{A})[I]$ is injective to prove (1). By the irreducibility of the residual representation, we have

$$H^0(\mathbb{Q}_S/\mathbb{Q}, \mathcal{A}[\mathfrak{M}]) = H^0(\mathbb{Q}_S/\mathbb{Q}, \mathcal{A})[\mathfrak{M}] = 0,$$

where $\mathfrak{M}$ is the maximal ideal of $\Lambda_{\mathcal{O}}^{(n)}$. Hence $H^0(\mathbb{Q}_S/\mathbb{Q}, \mathcal{A}) = 0$ by Nakayama's lemma. Thus, we have the following commutative diagram:

$$\begin{array}{ccccccc}
0 \to & Ш_S^1(\mathcal{A}[I]) & \longrightarrow & H^1(\mathbb{Q}_S/\mathbb{Q}, \mathcal{A}[I]) & \longrightarrow & \bigoplus_{v\in S} H^1(\mathbb{Q}_v, \mathcal{A}[I]) \\
& \downarrow & & \downarrow w_1 & & \downarrow w_2 \\
0 \to & Ш_S^1(\mathcal{A})[I] & \longrightarrow & H^1(\mathbb{Q}_S/\mathbb{Q}, \mathcal{A})[I] & \longrightarrow & \bigoplus_{v\in S} H^1(\mathbb{Q}_v, \mathcal{A})[I].
\end{array}$$

By the snake lemma, the kernel of the restriction map $Ш_S^1(\mathcal{A}[I]) \to Ш_S^1(\mathcal{A})[I]$ must be zero since the kernel of w_1 is

$$H^0(\mathbb{Q}_S/\mathbb{Q}, \mathcal{A})/IH^0(\mathbb{Q}_S/\mathbb{Q}, \mathcal{A}) = 0.$$

This proves the first statement 1).

For the statement 2), we remark that the Pontryagin dual of $\ker(w_2)$ is $\bigoplus_{v\in S}(\mathcal{T}^*)_{G_{\mathbb{Q}_v}}[I]$. By using again the snake lemma in the above commutative diagram, we see that the cokernel of $Ш^1_S(\mathcal{A}[I]) \to Ш^1_S(\mathcal{A})[I]$ is a subquotient of the Pontryagin dual of $\bigoplus_{v\in S}(\mathcal{T}^*)_{G_{\mathbb{Q}_v}}[I]$. Hence the kernel of $Ш^2_S(\overline{\mathcal{T}})/IШ^2_S(\overline{\mathcal{T}}) \to Ш^2_S(\overline{\mathcal{T}}_I)$ is a subquotient of $\bigoplus_{v\in S}(\mathcal{T}^*)_{G_{\mathbb{Q}_v}}[I]$. We see that $\bigoplus_{v\in S}(\mathcal{T}^*)_{G_{\mathbb{Q}_v}}[I]$ is a torsion $\Lambda_{\mathcal{O}}^{(n)}/I$-module if and only if I is relatively prime to the characteristic of a torsion $\Lambda_{\mathcal{O}}^{(n)}$-module $\bigoplus_{v\in S}(\mathcal{T}^*)_{G_{\mathbb{Q}_v}}$. Further, $\bigoplus_{v\in S}(\mathcal{T}^*)_{G_{\mathbb{Q}_v}}[I]$ is isomorphic to $\mathcal{P}[I]$ by Lemma 4.1. This completes the proof of 2). □

By Lemma 4.3, 1), the number k in the statement of Theorem 2.4 is well-behaved under the specialization argument.

By similar arguments using the snake lemma, we prove the following:

Lemma 4.4. — *Let the assumptions and the notations be as in Theorem* 2.4. *We have the following statements*:

1) *For any height* 1 *prime* I *of* $\Lambda_{\mathcal{O}}^{(n)}$, *the natural map*:

$$\left(H^1(\mathbb{Q}_S/\mathbb{Q},\overline{\mathcal{T}})/\mathcal{Z}(1)\Lambda_{\mathcal{O}}^{(n)}\right)/I\left(H^1(\mathbb{Q}_S/\mathbb{Q},\overline{\mathcal{T}})/\mathcal{Z}(1)\Lambda_{\mathcal{O}}^{(n)}\right) \xrightarrow{q_I} H^1(\mathbb{Q}_S/\mathbb{Q},\overline{\mathcal{T}}_I)/\mathcal{Z}(1)_I$$

is injective, *where we denote by* $\mathcal{Z}(1)_I$ *the image of* $\mathcal{Z}(1)$ *by* $H^1(\mathbb{Q}_S/\mathbb{Q},\overline{\mathcal{T}}) \to H^1(\mathbb{Q}_S/\mathbb{Q},\overline{\mathcal{T}}_I)$.

2) *For all but finitely many height* 1 *prime ideals* I *of* $\Lambda_{\mathcal{O}}^{(n)}$, $\mathrm{Coker}(q_I)$ *is a torsion* $\Lambda_{\mathcal{O}}^{(n)}/I$*-module. Further*, $\mathrm{Coker}(q_I)$ *is isomorphic to* $\mathcal{Q}[I]$ *for all but finitely many height* 1 *primes* I, *where* $\mathcal{Q}$ *is the largest pseudo-null* $\Lambda_{\mathcal{O}}^{(n)}$*-module of* $H^2(\mathbb{Q}_S/\mathbb{Q},\overline{\mathcal{T}})$. *Especially*, *the order of* $\mathrm{Coker}(q_I)$ *is bounded by the order of a finite group* $\mathcal{Q}$ *for all but finitely many height* 1 *primes* I *of* $\Lambda_{\mathcal{O}}$ *when* $n = 1$.

Recall the following lemma, which is an immediate consequence of the definition of the characteristic ideal:

Lemma 4.5. — *Let* M *be a torsion* $\Lambda_{\mathcal{O}}^{(n)}$*-module and let* $\mathcal{O}'$ *be a complete discrete valuation ring which is finite flat over* $\mathcal{O}$. *Then*, *we have* $\mathrm{char}_{\Lambda_{\mathcal{O}'}^{(n)}}(M_{\mathcal{O}'}) = \mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}}(M)\Lambda_{\mathcal{O}'}^{(n)}$, *where* $M_{\mathcal{O}'}$ *is the extension* $M \otimes_{\mathcal{O}} \mathcal{O}'$.

By this lemma, we may take an extension of the coefficient ring $\mathcal{O}$ freely to prove Theorem 2.4.

Let us return to the proof of Theorem 2.4. Our strategy for the proof is an induction argument with respect to n by using the results in §3. The case of $n = 0$ is already studied by several people. Let T be a free $\mathcal{O}$-module of rank 2 with continuous $G_{\mathbb{Q}}$-action and denote by $\overline{T}$ the Kummer dual $\mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O}) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1)$ of T. We assume that T is unramified outside a finite set of primes S containing p and ∞. In this situation, we define an Euler system as follows:

DEFINITION 4.6. — Let $\mathcal{R}$ be the set of all square-free natural numbers which are prime to S. An Euler system for $\overline{T}$ is a collection of cohomology classes $\{z(r) \in H^1(\mathbb{Q}(\mu_r), \overline{T})\}_{r \in \mathcal{R}}$ with the following properties:

1) The element $z(r)$ is unramified outside p for each $r \in \mathcal{R}$.

2) The norm $\mathrm{Norm}_{\mathbb{Q}(\mu_{rq})/\mathbb{Q}(\mu_r)} z(rq)$ is equal to $P_q(\mathrm{Frob}_q) z(r)$, where $P_q(X) \in \mathcal{O}[X]$ is a polynomial $\det(1 - \mathrm{Frob}_q X; V)$ and Frob_q is (the conjugacy class of) a geometric Frobenius element at q in the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_r)/\mathbb{Q})$.

Let us recall the following result on the Euler system theory over discrete valuation rings ($n = 0$ case):

THEOREM 4.7. — *Let the notations be as above and let* $\{z(r) \in H^1(\mathbb{Q}(\mu_r), \overline{T})\}_{r \in \mathcal{R}}$ *be an Euler system for* $\overline{T}$. *Assume the following conditions*:

(i) *The element* $z(1)$ *is not contained in the* $\mathcal{O}$*-torsion part of* $H^1(G_S, \overline{T})$.

(ii) *For each finite place* $v \in S$, $H^2(\mathbb{Q}_v, \overline{T})$ *is finite.*

(iii) *The images of the determinant representations* $G_{\mathbb{Q}} \to \mathrm{Aut}(\overset{2}{\wedge} T) \cong \mathcal{O}^{\times}$ *and* $G_{\mathbb{Q}} \to \mathrm{Aut}(\overset{2}{\wedge} \overline{T}) \cong \mathcal{O}^{\times}$ *both contain elements of infinite order.*

(iv) *The residual representation* $T/\pi T \cong \mathbb{F}^{\oplus 2}$ *is an irreducible representation of* $G_{\mathbb{Q}}$.

(v) *The* $\pm$*-eigen spaces* $T^{\pm}$ *of a complex conjugate element are both rank one modules over* $\mathcal{O}$.

Assume further that there exist $\tau \in G_{\mathbb{Q}(\mu_{p^\infty})}$ *and* $\tau' \in G_{\mathbb{Q}}$ *such that the image of* τ *under the representation* $G_{\mathbb{Q}} \to \mathrm{Aut}(T) \cong \mathrm{GL}_2(\mathcal{O})$ *has a presentation* $\left(\begin{smallmatrix} 1 & p_\tau \\ 0 & 1 \end{smallmatrix}\right)$ *by* $p_\tau \neq 0$ *under certain choice of basis of* T *and that* τ' *acts on* T *via the multiplication by* -1. *Then the following statements hold*:

1) *The group* $Ш^2_S(\overline{T})$ *is finite.*

2) $\sharp\left(Ш^2_S(\overline{T})\right)$ *divides* $\sharp(\mathcal{O}/(p_\tau^k)) \cdot \sharp\left(H^1(\mathbb{Q}_S/\mathbb{Q},\overline{T})/\mathcal{O}z\right)$, *where* k *is the number of cyclic* $\mathcal{O}$*-factors of* $Ш^2_S(\overline{T})$.

We omit the proof of the above result since the case over discrete valuation rings with finite residue field was already discussed by several authors. We refer the reader to [Ru2], Theorem 2.2.10. Though the statement of [Ru2], Theorem 2.2.10 treats only the case where p_τ is a unit, careful reading of the argument of the proof in [Ru2], Chapter 5, gives us the above slightly generalized version.

Let $M = Ш^2_S(\overline{T}) \oplus \mathcal{P}$ and $N = \Lambda_{\mathcal{O}}^{(n)}/(P_\tau^k) \oplus H^1(\mathbb{Q}_S/\mathbb{Q},\overline{T})/\mathcal{Z}(1) \oplus \mathcal{Q}$. For the proof of Theorem 2.4, we need to show the following two statements:

1) The module M is a torsion $\Lambda_{\mathcal{O}}^{(n)}$-module.

2) The ideal $\mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}}(N)$ is contained in $\mathrm{char}_{\Lambda_{\mathcal{O}}^{(n)}}(M)$.

First, we prove the case where $n = 1$. We assume the conditions from (i) to (v) and the condition (**Im**) which appeared in the statement of Theorem 2.4. Let us take a complete discrete valuation ring $\mathcal{O}'$ which is finite flat over $\mathcal{O}$. For height 1 prime ideals $I \in \mathcal{L}_{\mathcal{O}'}$, let us consider the following conditions:

(I) The groups $N_{\mathcal{O}'}/IN_{\mathcal{O}'}$ and $H^2(\mathbb{Q}_S/\mathbb{Q},\overline{\mathcal{T}}\otimes_{\mathcal{O}}\mathcal{O}')[I]$ are torsion $\Lambda_{\mathcal{O}'}/I$-modules.

(II) The module $\bigoplus_{v\in S} H^2(\mathbb{Q}_v,(\overline{\mathcal{T}}\otimes_{\mathcal{O}}\mathcal{O}')_I)$ is a torsion $\Lambda_{\mathcal{O}'}/I$-module.

(III) The images of the determinant representations

$$G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(\overset{2}{\wedge}(\mathcal{T}\otimes_{\mathcal{O}}\mathcal{O}')_I) \cong (\Lambda_{\mathcal{O}'}/I)^\times \quad \text{and}$$
$$G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(\overset{2}{\wedge}(\overline{\mathcal{T}}\otimes_{\mathcal{O}}\mathcal{O}')_I) \cong (\Lambda_{\mathcal{O}'}/I)^\times$$

contain elements of infinite order.

Clearly (I) holds for all but finitely many $I \in \mathcal{L}_{\mathcal{O}'}$. Since we have an exact sequence:

$$\bigoplus_{v\in S} H^2(\mathbb{Q}_v,\overline{\mathcal{T}}\otimes_{\mathcal{O}}\mathcal{O}') \xrightarrow{\times I} \bigoplus_{v\in S} H^2(\mathbb{Q}_v,\overline{\mathcal{T}}\otimes_{\mathcal{O}}\mathcal{O}') \longrightarrow \bigoplus_{v\in S} H^2(\mathbb{Q}_v,(\overline{\mathcal{T}}\otimes_{\mathcal{O}}\mathcal{O}')_I) \to 0,$$

the condition (II) also holds for all but finitely many $I \in \mathcal{L}_{\mathcal{O}'}$. By the condition (iii) of Theorem 2.4 in the case $n = 1$, there exists an element

$g \in G_{\mathbb{Q}}$ such that the image $U_g \in (\Lambda_{\mathcal{O}'})^{\times}$ of g via

$$G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}\big(\overset{2}{\wedge}(\mathcal{T} \otimes_{\mathcal{O}} \mathcal{O}')\big) \cong (\Lambda_{\mathcal{O}'})^{\times}$$

is of infinite order. The image $U_{g,I} \in (\Lambda_{\mathcal{O}'}/I)^{\times}$ of g via

$$G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}\big(\overset{2}{\wedge}(\mathcal{T} \otimes_{\mathcal{O}} \mathcal{O}')_I\big) \cong (\Lambda_{\mathcal{O}'}/I)^{\times}$$

is the specialization of U_g modulo I. Note that we have

$$\big\{\text{the group of roots of unity in } \Lambda_{\mathcal{O}'}/I\big\} = \big\{\text{the group of roots of unity in } \mathcal{O}'\big\}$$

for any $I \in \mathcal{L}_{\mathcal{O}'}^{(n)}$. Take a sufficiently big natural number r such that $\zeta^r = 1$ for any root of unity ζ in $\mathcal{O}'$. Hence $U_{g,I} \in (\Lambda_{\mathcal{O}'})^{\times}$ is of finite order if and only if I divides $U_g^r - 1$. Since there are only finitely many I which divide $(U_g^r - 1)$, $G_{\mathbb{Q}} \to \mathrm{Aut}(\overset{2}{\wedge}(\mathcal{T} \otimes_{\mathcal{O}} \mathcal{O}')_I)$ contains an element of infinite order for all but finitely many $I \in \mathcal{L}_{\mathcal{O}'}$. By the exactly same argument, we see that $G_{\mathbb{Q}} \to \mathrm{Aut}(\overset{2}{\wedge}(\overline{\mathcal{T}} \otimes_{\mathcal{O}} \mathcal{O}')_I)$ contains an element of infinite order for almost all $I \in \mathcal{L}_{\mathcal{O}'}$. Hence (III) holds for all but finitely many $I \in \mathcal{L}_{\mathcal{O}'}$.

The conditions (iv) and (v) in Theorem 4.7 are trivially satisfied for all $\mathcal{T}_I$ by the conditions (iv) and (v) for $n = 1$ case of Theorem 2.4. By Lemma 4.3, 3) and by Lemma 4.4, 3), the conditions from (I) to (III) imply all assumptions in Theorem 4.7 for all but finitely many $I \in \mathcal{L}_{\mathcal{O}'}$. By Theorem 4.7, the following statements hold for all but finitely many $I \in \mathcal{L}_{\mathcal{O}'}$ for arbitrary complete discrete valuation ring $\mathcal{O}'$ which is finite flat over $\mathcal{O}$:

1) The module $M_{\mathcal{O}'}/IM_{\mathcal{O}'}$ is a torsion $\Lambda_{\mathcal{O}'}^{(n)}/I$-module.

2) $\sharp(M_{\mathcal{O}'}/IM_{\mathcal{O}'})$ divides $c \cdot \sharp(N_{\mathcal{O}'}/IN_{\mathcal{O}'})$, where c is the order of the finite group $\mathcal{P} \otimes_{\mathcal{O}} \mathcal{O}'$.

Since c is a constant which is independent of $I \in \mathcal{L}_{\mathcal{O}'}$, we deduce that M is a torsion $\Lambda_{\mathcal{O}}$-module and that there exists an integer h such that we have the inclusion $\mathrm{char}_{\Lambda_{\mathcal{O}}}(M) \supset (\pi_{\mathcal{O}}^h)\mathrm{char}_{\Lambda_{\mathcal{O}}}(M)$ by using Proposition 3.11, 1).

To finish the proof of Theorem 2.4 for $n = 1$ case, we have to show that the above constant h is zero. We take a sequence of ideals $\mathcal{E}_{\mathcal{O}} = \{I_m \mid m \in \mathbb{Z}_{\geq 1}\}$ of Eisenstein type in the sense of Proposition 3.11, 2). As in the above argument, we consider the following conditions:

(I) The groups N/I_mN and $H^2(\mathbb{Q}_S/\mathbb{Q}, \overline{\mathcal{T}})[I_m]$ are torsion $\Lambda_{\mathcal{O}}/I_m$-modules.

(II) The module $\bigoplus_{v\in S} H^2(\mathbb{Q}_v, \overline{\mathcal{T}}_{I_m})$ is a torsion $\Lambda_{\mathcal{O}}/I_m$-module.

(III) The images of the determinant representations $G_{\mathbb{Q}} \to \mathrm{Aut}(\overset{2}{\wedge}\, \mathcal{T}_{I_m}) \cong (\Lambda_{\mathcal{O}}/I_m)^{\times}$ and $G_{\mathbb{Q}} \to \mathrm{Aut}(\overset{2}{\wedge}\, \overline{\mathcal{T}}_{I_m}) \cong (\Lambda_{\mathcal{O}}/I_m)^{\times}$ contain elements of infinite order.

The properties (I) and (II) hold for all but finitely many I_m by exactly the same argument as above. The difference from the above argument is that (III) might fail to be true for infinitely many m if we take arbitrary set of ideals $\mathcal{E}_{\mathcal{O}}$ of Eisenstein type. So we have to choose a set of ideals $\mathcal{E}_{\mathcal{O}}$ of Eisenstein type so that

$$\begin{aligned}\big\{&\text{the group of roots of unity in } \Lambda_{\mathcal{O}}/I_m\big\}\\ &= \big\{\text{the group of roots of unity in } \mathcal{O}\big\}\end{aligned}$$

holds for all m. We may choose $\mathcal{E}_{\mathcal{O}} = \{I_m = (X^m - \pi_{\mathcal{O}})\}_{m\in\mathbb{Z}_{\geq 1}}$ for example for $\mathcal{E}_{\mathcal{O}}$ with the above conditions. Then, we show that (III) holds for all but finitely many I_m by the same argument as in the case of $\mathcal{L}_{\mathcal{O}'}$. By Lemma 4.3, 3) and by Lemma 4.4, 3), the conditions from (I) to (III) imply all assumptions in Theorem 4.7 for all but finitely many I_m. By Theorem 4.7, the following statements hold for all but finitely many I_m:

1) The module M/I_mM is a torsion $\Lambda_{\mathcal{O}}^{(n)}/I_m$-module.

2) $\sharp(M/I_mM)$ divides $c' \cdot \sharp(N/I_mN)$, where c' is the order of the finite group $\mathcal{P}$.

Since c' is a constant which is independent of I_m, we deduce that h is zero by Proposition 3.11, 2). This completes the proof of Theorem 2.4 when $n = 1$.

For general n, we reduce the proof of Theorem 2.4 for $n \geq 2$ to the case $n-1$ by induction. The induction argument for $n \geq 2$ proceeds basically in the same way as the proof of the case $n = 1$ by using Proposition 3.6 instead of Proposition 3.11. So we omit writing the process of arguments for $n \geq 2$.

BIBLIOGRAPHY

[BK] S. Bloch, K. Kato, L-functions and Tamagawa numbers of motives, in The Grothendieck Festschrift I, Progress in Math., 86 (1990), 333–400.

[Bo] N. Bourbaki, Éléments de mathématique, Algèbre commutative, Chapitres 5–7, 1985.

[Bu] J.M. Fontaine (éd.), Périodes p-adiques, Séminaire de Bures (1988), Astérisque 223, 1994.

[De1] P. Deligne, Formes modulaires et représentations ℓ-adiques, Séminaire Bourbaki 355, p. 139–172, Lecture Notes in Math. 179, Springer Verlag, 1969.

[De2] P. Deligne, Valeurs des fonctions L et périodes d'intégrales, in Automorphic forms, representations and L-functions, p. 247–289, Proc. Sympos. Pure Math., XXXIII, Part 2, Amer. Math. Soc., 1979.

[Fl] M. Flach, A generalisation of Cassels-Tate pairing, J. reine angew. Math., 412 (1990), 113–127.

[Gr1] R. Greenberg, Iwasawa theory for p-adic representations, Advanced studies in Pure Math., 17 (1987), 97–137.

[Gr2] R. Greenberg, Iwasawa theory for p-adic deformations of motives, Proceedings of Symposia in Pure Math., 55-2 (1994), 193–223.

[GS] R. Greenberg, G. Stevens, p-adic L-functions and p–adic periods of modular forms, Invent. Math., 111-2 (1993), 407–447.

[Hi1] H. Hida, Galois representations into $\mathrm{GL}_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, Invent. Math., 85 (1986), 545–613.

[Hi2] H. Hida, Elementary theory of L-functions and Eisenstein series, London Math. Society Student Texts 26, Cambridge University Press, 1993.

[Ka1] K. Kato, Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}, I, in Arithmetic algebraic geometry, p. 50–163, Lecture Notes in Math. 1553, Springer, 1993.

[Ka2] K. Kato, Series of lectures on Iwasawa main conjectures for modular elliptic curves, given at Tokyo University, September 1998.

[Ka3] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, Preprint.

[Ka4] K. Kato, Euler systems, Iwasawa theory, and Selmer groups, Kodai Math. J., 22-3 (1999), 313–372.

[Ki] K. Kitagawa, On standard p-adic L-functions of families of elliptic cusp forms, in p-adic monodromy and the Birch and Swinnerton-Dyer conjecture, p. 81–110, Contemp. Math. 165, Amer. Math. Soc., 1994.

[Ma] H. Matsumura, Commutative ring theory, Cambridge Studies in Advanced Mathematics 8, Cambridge University Press, 1986.

[MR] B. Mazur, K. Rubin, Kolyvagin systems, Preprint, 2001.

[MT] B. Mazur, J. Tilouine, Représentations galoisiennes, différentielles de Kähler et "conjectures principales", Inst. Hautes Études Sci. Publ. Math., 71 (1990), 65–103.

[MW1] B. Mazur, A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, Invent. Math., 76-2 (1984), 179–330.

[MW2] B. MAZUR, A. WILES, On p-adic analytic families of Galois representations, Compos. Math., 59-2 (1986), 231–264.

[Mi] J.S. MILNE, Arithmetic duality theorems, Perspectives in Math. 1, Academic Press, 1986.

[NSW] J. NEUKIRCH, A. SCHMIDT, K. WINGBERG, Cohomology of number fields, Grundlehren Math. Wiss. 323, Springer-Verlag, Berlin, 2000.

[Oc1] T. OCHIAI, Control theorem for Greenberg's Selmer groups for Galois deformations, J. Number Theory,, 88 (2001), 59–85.

[Oc2] T. OCHIAI, A generalization of the Coleman map for Hida deformations, Amer. J. Math., 125 (2003), 849–892.

[Oc3] T. OCHIAI, On the two-variable Iwasawa Main conjecture for Hida deformations, in preparation.

[Pe] B. PERRIN-RIOU, Systèmes d'Euler p-adiques et théorie d'Iwasawa, Ann. Inst. Fourier, 48-5 (1998), 1231–1307.

[Ru1] K. RUBIN, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Invent. Math., 103-1 (1991), 25–68.

[Ru2] K. RUBIN, Euler systems, Annals Math. Studies, 147 (2000).

[Se] J.-P. SERRE, Cohomologie galoisienne, 5th ed., Lecture Notes in Math. 5, Springer-Verlag, 1994.

[Ta] J. TATE, Relations between K_2 and Galois cohomology, Invent. Math., 36 (1976), 257–274.

[Wi] A. WILES, On λ-adic representations associated to modular forms, Invent. Math., 94 (1988), 529–573.

Manuscrit reçu le 30 avril 2004,
accepté le 14 septembre 2004.

Tadashi OCHIAI,
Osaka University
Department of Mathematics
1-16 Machikaneyama
Toyonaka, Osaka, 560–0043 (Japan)
ochiai@math.wani.osaka-u.ac.jp