

CONTROL THEOREM FOR GREENBERG'S SELMER GROUPS OF GALOIS DEFORMATIONS

TADASHI OCHIAI

ABSTRACT. We give sufficient conditions for the Selmer group of a p -adic deformation of a motive over a number field to be controlled. Then we apply this result to the Selmer groups of various Galois representations. For example, we treat the cyclotomic deformations and the Hida deformations of the representations associated to modular forms.

1. INTRODUCTION

In [M], Mazur discussed a generalization of classical Iwasawa theory for the class group of a number field to the Selmer group of an elliptic curve over a number field. Let F_∞/F be the cyclotomic $\mathbb{Z}_p$ -extension of an algebraic number field F . We denote the n -th layer of F_∞/F by F_n . For the p -primary Selmer group $\text{Sel}(E/F_n)\{p\}$ of an elliptic curve E over F , we have the following exact sequence:

$$0 \longrightarrow E(F_n) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \text{Sel}(E/F_n)\{p\} \longrightarrow \text{III}(E/F_n)\{p\} \longrightarrow 0,$$

where $E(F_n)$ is the F_n -valued points of E and $\text{III}(E/F_n)\{p\}$ is the p -primary subgroup of the Tate-Shafarevich group of E/F_n . Mazur proved the following theorem.

Mazur's Control Theorem ([M]). *Let E be an elliptic curve over a number field F . Assume that E has good ordinary reduction at all places of F dividing p . Let F_∞/F be the cyclotomic $\mathbb{Z}_p$ -extension and let Γ_n be $\text{Gal}(F_\infty/F_n)$. Then the kernel and the cokernel of the restriction map:*

$$\text{Sel}(E/F_n)\{p\} \xrightarrow{r_n} \text{Sel}(E/F_\infty)\{p\}^{\Gamma_n},$$

are finite groups whose orders are bounded independently of n .

We are interested in the behavior of the Selmer group $\text{Sel}(E/F_n)\{p\}$ in the cyclotomic $\mathbb{Z}_p$ -extension because $\text{Sel}(E/F_n)\{p\}$ contains important arithmetic informations of E/F_n such as the Mordell-Weil rank of $E(F_n)$. By Mazur's control theorem stated above, knowing the behavior of $\text{Sel}(E/F_n)\{p\}$ is equivalent to knowing the behavior of $\text{Sel}(E/F_\infty)\{p\}^{\Gamma_n}$. We denote by Λ the power series ring $\mathbb{Z}_p[[X]]$. Then $\text{Sel}(E/F_\infty)\{p\}$ is naturally regarded as a Λ -module via an isomorphism $\mathbb{Z}_p[[X]] \cong \mathbb{Z}_p[[\Gamma]]$. It is conjectured that the Pontrjagin dual $\widehat{\text{Sel}(E/F_\infty)\{p\}}$ of $\text{Sel}(E/F_\infty)\{p\}$ is a finitely generated torsion Λ -module and that the Fitting ideal is equal to the ideal generated by the p -adic L -function of E (Main Conjecture proposed by Mazur). Assuming the main conjecture, the behavior of $\text{Sel}(E/F_\infty)\{p\}^{\Gamma_n}$ when n varies is related to some invariants of the p -adic

L -function, which are computable compared to those of the Selmer group. Hence we will be able to know the behavior of $\text{Sel}(E/F_n)\{p\}$.

In the paper [Gr2], Greenberg proposed a vast generalization of the above framework for elliptic curves into a theory called Iwasawa theory of Galois deformation. This theory treats very general situations not necessarily coming from the cyclotomic $\mathbb{Z}_p$ -extension. In this paper, we discuss a generalization of Mazur's control theorem stated above to these situations.

Let $\mathcal{O}$ be a complete discrete valuation ring which is finite flat over $\mathbb{Z}_p$ and let R be a integral domain which is finite flat over $\Lambda_{\mathcal{O}} = \mathcal{O}[[X]]$. We denote the set of all primes of F above p by Σ_p . We define Σ to be a finite set of finite primes of F which contains Σ_p . Let us take a finite free R -module $\tilde{T}$ with a continuous G_F -action which is unramified outside Σ . For each prime v of F over p , we fix a filtration $0 \subset F_v^+ \tilde{T} \subset \tilde{T}$ as a D_v -module. We define $\tilde{A}$ by $\tilde{T} \otimes_R \text{Hom}_{\text{cont}}(R, \mathbb{Q}_p/\mathbb{Z}_p)$. The Selmer group $\text{Sel}(F, \tilde{A})$ (resp. the strict Selmer group $\text{Sel}^{\text{str}}(F, \tilde{A})$) for $\tilde{A}$ is defined as follows (cf. [Gr1], [Gr2]):

$$\text{Sel}(F, \tilde{A}) = \text{Ker}[H^1(F, \tilde{A}) \longrightarrow \prod_{v \notin \Sigma_p} H^1(I_v, \tilde{A}) \times \prod_{v \in \Sigma_p} H^1(I_v, \tilde{A}/F_v^+ \tilde{A})]$$

$$(\text{resp. } \text{Sel}^{\text{str}}(F, \tilde{A}) = \text{Ker}[H^1(F, \tilde{A}) \longrightarrow \prod_{v \notin \Sigma_p} H^1(I_v, \tilde{A}) \times \prod_{v \in \Sigma_p} H^1(D_v, \tilde{A}/F_v^+ \tilde{A})]).$$

Assuming certain conditions of criticalness and the non-vanishing of the p -adic L -function, Greenberg conjectures that $\widehat{\text{Sel}(F, \tilde{A})}$ is a cotorsion R -module and that the divisor associated to the Pontrjagin dual $\widehat{\text{Sel}(F, \tilde{A})}$ of $\text{Sel}(F, \tilde{A})$ is related to the divisor associated to the p -adic L -function (Iwasawa main conjecture for the Galois deformation $\tilde{T}$). Thus it is important to control the behavior of this Selmer group under restriction maps.

From now on through this introduction, we assume that R is equal to $\Lambda_{\mathcal{O}}$. Let $\mathcal{I} = \{(P_i)\}_{i \in I}$ be a set of principal ideals of $\Lambda_{\mathcal{O}}$ such that $\Lambda_{\mathcal{O}}/(P_i)$ is a free $\mathbb{Z}_p$ -module of finite rank. For the discrete $\Lambda_{\mathcal{O}}$ -module $\tilde{A}$, we define $\tilde{A}[P_i]$ to be the submodule of (P_i) -torsion elements in $\tilde{A}$. Since $\tilde{A}[P_i]$ has the filtration $F_v^+ \tilde{A}[P_i] = \tilde{A}[P_i] \cap F_v^+ \tilde{A}$ at each $v|p$, $\text{Sel}(F, \tilde{A}[P_i])$ (resp. $\text{Sel}^{\text{str}}(F, \tilde{A}[P_i])$) is defined in the same way as above. We consider the natural restriction map:

$$\text{Sel}(F, \tilde{A}[P_i]) \xrightarrow{r_i} \text{Sel}(F, \tilde{A})[P_i]$$

$$(\text{resp. } \text{Sel}^{\text{str}}(F, \tilde{A}[P_i]) \xrightarrow{r_i^{\text{str}}} \text{Sel}^{\text{str}}(F, \tilde{A})[P_i]).$$

Then we have the following:

Theorem A (Theorem 2.2). *Let $\tilde{T}, \tilde{A}$ be as above and let $(P_i) \in \mathcal{I}$. For each $v \in \Sigma$, we define torsion $\Lambda_{\mathcal{O}}$ -modules C_v, C_v^{str} in §2).*

(1) *Assume that $H^0(F, (\tilde{T}/P_i \tilde{T}) \otimes K) = 0$. Then the kernel of r_i (resp. r_i^{str}) is a finite group whose order is bounded by the order of the largest finite submodule of the coinvariant quotient $\text{Hom}_{\Lambda_{\mathcal{O}}}(\tilde{T}, \Lambda_{\mathcal{O}})_{G_F}$.*

(2) *Assume that the group $\bigoplus_{v \in \Sigma} C_v/P_i C_v$ (resp. $\bigoplus_{v \in \Sigma} C_v^{\text{str}}/P_i C_v^{\text{str}}$) is finite. Then the cokernel*

of r_i (resp. r_i^{str}) is a finite group whose order is bounded by an integer which does not depend on $i \in I$.

We give some applications of Theorem A. First, we treat the deformation arising from the cyclotomic $\mathbb{Z}_p$ -extension. Let V be an ordinary representation (see Definition 3.1 for the definition of ordinary deformation) of G_F and let T be a G_F -stable lattice of V . We denote the discrete Galois module $T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ by A . Let F_∞/F be the cyclotomic $\mathbb{Z}_p$ -extension of a number field F . Then the strict Selmer group $\text{Sel}^{\text{str}}(F_n, A)$ is defined by using the filtration coming from the assumption of ordinarity (see the beginning of §3). For T as above, we have the deformation $\tilde{T}$ of T which is rank 2 over Λ called the cyclotomic deformation of T (see Definition 3.4). The cyclotomic deformation $\tilde{T}$ is the deformation such that $\text{Sel}^{\text{str}}(F, \tilde{A}) = \text{Sel}^{\text{str}}(F_\infty, A)$ and that (see Proposition 3.3):

$$\begin{aligned}\text{Sel}^{\text{str}}(F, \tilde{A}[\omega_n]) &= \text{Sel}^{\text{str}}(F_n, A), \\ \text{Sel}^{\text{str}}(F_\infty, \tilde{A})[\omega_n] &= \text{Sel}^{\text{str}}(F_\infty, A)^{\Gamma_n},\end{aligned}$$

for the set of ideals $\mathcal{I} = \{(\omega_n)\}_{n \in \mathbb{Z}_{\geq 0}}$, where $\omega_n = (1+X)^{p^n} - 1$. By using this translation into the language of Galois deformations, we apply our Theorem A to the situation coming from the cyclotomic $\mathbb{Z}_p$ -extension. We have the following theorem as a corollary of Theorem A.

Theorem B (Theorem 3.5). *Let V be an ordinary p -adic representation of G_F and let T be a G_F -stable lattice of V . We denote $T \otimes \mathbb{Q}_p/\mathbb{Z}_p$ by A . Let F_∞/F be the cyclotomic $\mathbb{Z}_p$ -extension of F . Then the following statements hold:*

- (1) *If $H^0(F_n, V) = 0$, the kernel of the restriction map:*

$$\text{Sel}^{\text{str}}(F_n, A) \xrightarrow{r_n} \text{Sel}^{\text{str}}(F_\infty, A)^{\Gamma_n},$$

is a finite group whose order is bounded by an integer which is independent of n .

- (2) *Assume that the eigenvalues of the action of Frob_v on $(\text{Fil}_v^i V / \text{Fil}_v^{i+1} V) \otimes \mathbb{Q}_p(-i)$ are not roots of unity for all $v|p$ and each $i \leq 0$. Then the cokernel of the restriction map r_n is a finite group whose order is bounded independently of n .*

This theorem is applied especially to the representation associated to an ordinary modular form or an odd power symmetric product of the Tate module of an elliptic curve (see Proposition 3.8, Proposition 3.9).

Next, we discuss a deformation of a Galois representation which does not come from a Galois extension. Hida constructed a p -adic interpolation of representations associated to modular forms when their weights vary. We consider the set of principal ideals $\mathcal{I} = \{(P_k)\}_{k \in \mathbb{Z}_{\geq 2}}$ where $P_k = (1+T) - (1+p)^k$. He constructed a rank 2 free $\Lambda_{\mathcal{O}}$ -module $\tilde{T}$ with continuous $G_{\mathbb{Q}}$ -action such that $\tilde{T} \bmod P_k$ is equivalent to the representation associated to a weight k cusp form for each $k \geq 2$. We apply Theorem A also to the Selmer group for this Λ -adic representation.

Theorem C (Theorem 5.1). *The restriction map $\text{Sel}(\mathbb{Q}, \tilde{A}[P_k]) \xrightarrow{r_k} \text{Sel}(\mathbb{Q}, \tilde{A})[P_k]$, has finite kernel and cokernel whose orders are bounded independently of k .*

In general, Hida's deformation $\tilde{T}$ of the representation of a modular form is not necessarily defined over $\Lambda_{\mathcal{O}}$. Hida's Galois deformation $\tilde{T}$ is sometimes defined over a certain larger ring R which is finite flat over $\Lambda_{\mathcal{O}}$. By using results from Hida theory, we obtain a result similar to Theorem C for general base R (see §5 for the precise statements). Finally, we state a corollary of Theorem C, which is a partial result to the Iwasawa main conjecture for Hida's Galois deformation. By using a Kato's result on Selmer groups of a modular forms, we obtain the following corollary:

Corollary D (Corollary 5.7, Remark 5.8). *Let $\tilde{T}$ be a Hida's Galois deformation as stated above. Then the Selmer group $\text{Sel}(\mathbb{Q}, \tilde{A})$ is a cotorsion R -module.*

Plan. The plan of this paper is as follows. In §2, we shall give a sufficient condition for Greenberg's Selmer group to be controlled in general situations. We show some applications of our theorem in §3 -§5. In §3, we consider the behavior of the Selmer group for a modular form or the symmetric power of an elliptic curve in the cyclotomic $\mathbb{Z}_p$ -extension. In §4, we recall known results concerning Λ -adic forms and associated Galois deformations developed by Hida. After these preparations, we state some applications to the Hida deformation of the p -adic representation of a modular form in §5.

Notation. For a field K , we denote $\text{Gal}(\bar{K}/K)$ by G_K where $\bar{K}$ is the separable closure of K . For a number field F and a prime v of F , we denote by D_v (resp. I_v) the decomposition subgroup (resp. the inertia subgroup) of G_F at v . Throughout the paper, the Frobenius Frob_v at v denotes the arithmetic Frobenius at v .

For a commutative ring R , we denote by $R^\times$ the group of invertible elements in R . If M is a finitely generated free $\mathbb{Z}_p$ -module (resp. $\mathbb{Q}_p$ -module, Λ -module), we denote the linear dual $\text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$ (resp. $\text{Hom}_{\mathbb{Q}_p}(M, \mathbb{Q}_p)$, $\text{Hom}_{\Lambda}(M, \Lambda)$) by M^* . When we are given a character $\tilde{\kappa} : G_F \rightarrow \Lambda^\times$, we define $\Lambda(\tilde{\kappa})$ as the free Λ -module of rank 1 on which G_F acts by $\tilde{\kappa}$. For a commutative ring R , an R -module M and an ideal $\mathfrak{p}$ of R , we denote by $M[\mathfrak{p}]$ the set of elements of M annihilated by any element of $\mathfrak{p}$. If (P) is a principal ideal of R , we write $M[P]$ instead of $M[(P)]$ for simplicity. Similarly, we denote the quotient module $M/(P)M$ by M/PM . For a finite set S , we denote the cardinality of S by $\#S$. Throughout this paper, we assume that the fixed prime number p is odd.

Acknowledgment. The author is grateful to Prof. Takeshi Saito for reading the manuscript carefully and pointing out mathematical mistakes. He also thanks Kazuo Matsuno for valuable discussion. Thanks are also due to Prof. Haruzo Hida for reading the manuscript, giving him useful comments and correcting several historical and mathematical mistakes. He expresses his sincere gratitude to Prof. Ralph Greenberg for giving him useful advise concerning Hida deformations and warm encouragement.

2. CONTROL THEOREM FOR GREENBERG'S SELMER GROUP

In this section, we give a sufficient condition for Greenberg's Selmer group to be controlled (Theorem 2.2). Let Σ_p be the finite set of the primes of F dividing p and Σ a finite set of finite primes in F containing Σ_p . Let $\tilde{T}$ be a $\Lambda_{\mathcal{O}}$ -adic representation of G_F which is unramified outside Σ . That is, $\tilde{T}$ is a free $\Lambda_{\mathcal{O}}$ -module of finite rank with continuous G_F -action unramified outside Σ . We define $\tilde{A}$ by $\tilde{T} \otimes_{\Lambda_{\mathcal{O}}} \text{Hom}_{\text{cont}}(\Lambda_{\mathcal{O}}, \mathbb{Q}_p/\mathbb{Z}_p)$.

For each $v \in \Sigma_p$, we fix a filtration $0 \subset F_v^+ \tilde{T} \subset \tilde{T}$ by a D_v -module such that $F_v^+ \tilde{T}$ is a $\Lambda_{\mathcal{O}}$ -module direct summand of $\tilde{T}$. Then the filtration $F_v^+ \tilde{T}$ on $\tilde{T}$ induces the filtration $0 \subset F_v^+ \tilde{A} \subset \tilde{A}$. Following Greenberg [Gr2], we define Selmer groups as follows:

Definition 2.1. Let the notations be as above. The Selmer group (resp. the strict Selmer group) $\text{Sel}(F, \tilde{A})$ (resp. $\text{Sel}^{\text{str}}(F, \tilde{A})$) is defined as follows:

$$\text{Sel}(F, \tilde{A}) := \text{Ker} \left[H^1(F, \tilde{A}) \longrightarrow \prod_{v \notin \Sigma_p} H^1(I_v, \tilde{A}) \times \prod_{v \in \Sigma_p} H^1(I_v, \tilde{A}/F_v^+ \tilde{A}) \right],$$

$$(\text{resp. } \text{Sel}^{\text{str}}(F, \tilde{A}) := \text{Ker} \left[H^1(F, \tilde{A}) \longrightarrow \prod_{v \notin \Sigma_p} H^1(I_v, \tilde{A}) \times \prod_{v \in \Sigma_p} H^1(F_v, \tilde{A}/F_v^+ \tilde{A}) \right]).$$

Let $(P) \subset \Lambda_{\mathcal{O}}$ be an ideal of $\Lambda_{\mathcal{O}}$ such that $\Lambda_{\mathcal{O}}/(P)$ is finite flat over $\mathcal{O}$. Then the $\mathcal{O}$ -module $\tilde{A}[P]$ is cofree and of cofinite type over $\mathcal{O}$ and has the filtration $F_v^+ \tilde{A}[P] \subset \tilde{A}[P]$ as D_v -module for each $v \in \Sigma_p$ induced by that of $\tilde{A}$. We also define Selmer groups for $\tilde{A}[P]$ as follows:

$$\text{Sel}(F, \tilde{A}[P]) := \text{Ker} \left[H^1(F, \tilde{A}[P]) \longrightarrow \prod_{v \notin \Sigma_p} H^1(I_v, \tilde{A}[P]) \times \prod_{v \in \Sigma_p} H^1(I_v, \tilde{A}[P]/F_v^+ \tilde{A}[P]) \right],$$

$$(\text{resp. } \text{Sel}^{\text{str}}(F, \tilde{A}[P]) := \text{Ker} \left[H^1(F, \tilde{A}[P]) \longrightarrow \prod_{v \notin \Sigma_p} H^1(I_v, \tilde{A}[P]) \times \prod_{v \in \Sigma_p} H^1(F_v, \tilde{A}[P]/F_v^+ \tilde{A}[P]) \right]).$$

We fix a set of ideals $\mathcal{I} = \{(P_i)\}_{i \in I}$ of $\Lambda_{\mathcal{O}}$ such that $\Lambda_{\mathcal{O}}/(P_i)$ is finite flat over $\mathcal{O}$. For each $i \in I$, there exists a natural restriction map:

$$\text{Sel}(F, \tilde{A}[P_i]) \xrightarrow{r_i} \text{Sel}(F, \tilde{A})[P_i],$$

$$(\text{resp. } \text{Sel}^{\text{str}}(F, \tilde{A}[P_i]) \xrightarrow{r_i^{\text{str}}} \text{Sel}^{\text{str}}(F, \tilde{A})[P_i]).$$

For each $v \in \Sigma$, the $\Lambda_{\mathcal{O}}$ -module C_v is defined as follows:

$$C_v = \begin{cases} \Lambda_{\mathcal{O}}\text{-torsion part of the module } ((\tilde{T}/F_v^+ \tilde{T})^*)_{I_v} & \text{for } v \in \Sigma_p, \\ \Lambda_{\mathcal{O}}\text{-torsion part of the module } ((\tilde{T})^*)_{I_v} & \text{for } v \in \Sigma \setminus \Sigma_p, \end{cases}$$

where $(\)_{I_v}$ means the maximal I_v -coinvariant quotient and $(\)^*$ denotes the $\Lambda_{\mathcal{O}}$ -linear dual here. Similarly, C_v^{str} is defined as follows:

$$C_v^{\text{str}} = \begin{cases} \Lambda_{\mathcal{O}}\text{-torsion part of the module } ((\tilde{T}/F_v^+ \tilde{T})^*)_{D_v} & \text{for } v \in \Sigma_p, \\ \Lambda_{\mathcal{O}}\text{-torsion part of the module } ((\tilde{T})^*)_{I_v} & \text{for } v \in \Sigma \setminus \Sigma_p, \end{cases}$$

We have the following theorem:

Theorem 2.2. Let $\tilde{T}, \tilde{A}$ be as above and let $(P_i) \in \mathcal{I}$.

- (1) Assume that $H^0(F, (\tilde{T}/P_i \tilde{T}) \otimes_{\mathcal{O}} K) = 0$. Then the kernel of the restriction map r_i (resp. r_i^{str}) is a finite group whose order is bounded by the order of the largest finite submodule of $(\tilde{T}^*)_{G_F}$.

(2) Assume that the group $(\bigoplus_{v \in \Sigma} C_v / P_i C_v)$ (resp. $(\bigoplus_{v \in \Sigma} C_v^{\text{str}} / P_i C_v^{\text{str}})$) is finite. Then the cokernel of the restriction map r_i (resp. r_i^{str}) is a finite group whose order is bounded by $\sharp(\bigoplus_{v \in \Sigma} C_v[P_i])$ (resp. $\sharp(\bigoplus_{v \in \Sigma} C_v^{\text{str}}[P_i])$), where $\underline{C}_v$ (resp. $\underline{C}_v^{\text{str}}$) is the largest finite $\Lambda_{\mathcal{O}}$ -submodule of C_v (resp. C_v^{str}). Especially, the order of the cokernel of r_i (resp. r_i^{str}) is less than or equal to the integer $\sharp(\bigoplus_{v \in \Sigma} \underline{C}_v)$ (resp. $\sharp(\bigoplus_{v \in \Sigma} \underline{C}_v^{\text{str}})$), which is independent of i .

Proof of Theorem 2.2. We prove the assertion only for the usual Greenberg's Selmer group $\text{Sel}(F, \tilde{A})$. The proof for the strict Selmer group is done exactly in the same way.

Let us prove the assertion for the kernel. We have the following commutative diagram:

$$\begin{array}{ccc} \text{Sel}(F, \tilde{A}[P_i]) & \xrightarrow{r_i} & \text{Sel}(F, \tilde{A})[P_i] \\ \cap & & \cap \\ H^0(F, \tilde{A})/P_i H^0(F, \tilde{A}) & \hookrightarrow & H^1(F, \tilde{A}[P_i]) \longrightarrow H^1(F, \tilde{A})[P_i]. \end{array}$$

Hence, we have only to show that $H^0(F, \tilde{A})/P_i H^0(F, \tilde{A})$ is a finite group whose order is bounded by the order of the largest finite submodule of $(\tilde{T}^*)_{G_F}$. We have the following lemma:

Lemma 2.3. *Let Q be a finitely generated $\Lambda_{\mathcal{O}}$ -module. Assume that $Q/P_i Q$ is finite. Then the (P_i) -torsion part $Q[P_i]$ of Q is isomorphic to a finite group $\underline{Q}[P_i]$, where $\underline{Q}$ is the maximal finite submodule of Q .*

Proof. By the classification theorem of finitely generated Λ -modules due to Iwasawa and Serre, we have the following exact sequence of $\Lambda_{\mathcal{O}}$ -modules:

$$0 \longrightarrow \underline{Q} \longrightarrow Q \longrightarrow \tilde{Q} := \Lambda_{\mathcal{O}}^{\oplus r} \oplus \bigoplus_i \Lambda_{\mathcal{O}} / (\pi_{\mathcal{O}}^{\mu_i}) \oplus \bigoplus_j \Lambda_{\mathcal{O}} / (f_j^{\lambda_j}) \longrightarrow \overline{Q} \longrightarrow 0,$$

where $\overline{Q}$ is finite, μ_i, λ_j are integers, $\pi_{\mathcal{O}}$ is a prime element of $\mathcal{O}$ and f_j are distinguished irreducible polynomials (see [Wa] Thm. 13.12, for example). By the assumption that $Q/P_i Q$ is finite, the map $\tilde{Q} \xrightarrow{P_i} \tilde{Q}$ is injective. This implies that $Q[P_i] = \underline{Q}[P_i]$. $\square$

We see that $H^0(F, \tilde{A}[P_i]) = H^0(F, \tilde{A})[P_i]$ is the Pontrjagin dual of $(\tilde{T}^*)_{G_F}/P_i(\tilde{T}^*)_{G_F}$ and that $H^0(F, \tilde{A})/P_i H^0(F, \tilde{A})$ is the Pontrjagin dual of $(\tilde{T}^*)_{G_F}[P_i]$. By the assumption of Theorem 2.2 (1), $(\tilde{T}^*)_{G_F}/P_i(\tilde{T}^*)_{G_F}$ is finite. Thus $H^0(F, \tilde{A})/P_i H^0(F, \tilde{A})$ is a finite group whose order is bounded by the order of the largest finite $\Lambda_{\mathcal{O}}$ -submodule of $(\tilde{T}^*)_{G_F}$ by applying Lemma 2.3 to the $\Lambda_{\mathcal{O}}$ -module $(\tilde{T}^*)_{G_F}$. This completes the proof of Theorem 2.2 (1).

Next, we prove the assertion for the cokernel. Let us recall the following well-known lemma:

Lemma 2.4. *Let A be a discrete G_F -module and let Σ be a finite set of primes of F which contains all primes above p . Assume that A is unramified outside Σ . Then we*

have:

$$H^1(F_\Sigma/F, A) = \text{Ker} \left[H^1(F, A) \longrightarrow \prod_{v \notin \Sigma} H^1(I_v, A) \right],$$

as a submodule of $H^1(F, A)$, where F_Σ is the maximal extension of F which is unramified outside Σ and $H^1(F_\Sigma/F, A)$ is defined to be $H^1(\text{Gal}(F_\Sigma/F), A)$.

Thus we have the following commutative diagram due to Lemma 2.4:

$$\begin{array}{ccccccc} 0 & \rightarrow & \text{Sel}(F, \tilde{A}[P_i]) & \rightarrow & H^1(F_\Sigma/F, \tilde{A}[P_i]) & \xrightarrow{\gamma_i} & \prod_{v \in \Sigma_p} H^1(I_v, (\tilde{A}/F_v^+ \tilde{A})[P_i]) \\ & & & & & & \times \prod_{v \in \Sigma \setminus \Sigma_p} H^1(I_v, \tilde{A}[P_i]) \\ & & r_i \downarrow & & s_i \downarrow & & t_i \downarrow \\ 0 & \rightarrow & \text{Sel}(F, \tilde{A})[P_i] & \rightarrow & H^1(F_\Sigma/F, \tilde{A})[P_i] & \rightarrow & \prod_{v \in \Sigma_p} H^1(I_v, \tilde{A}/F_v^+ \tilde{A})[P_i] \\ & & & & & & \times \prod_{v \in \Sigma \setminus \Sigma_p} H^1(I_v, \tilde{A})[P_i]. \end{array}$$

Since the map s_i is surjective by the exactness of the sequence:

$$H^1(F_\Sigma/F, \tilde{A}[P_i]) \longrightarrow H^1(F_\Sigma/F, \tilde{A}) \xrightarrow{P_i} H^1(F_\Sigma/F, \tilde{A}),$$

The cokernel of the map r_i is a sub-quotient of the kernel of t_i by the snake lemma. From this, it suffices to bound the kernel of t_i . The module $\text{Ker}(t_i)$ is isomorphic to:

$$\text{Coker} \left[\prod_{v \in \Sigma \setminus \Sigma_p} H^0(I_v, \tilde{A}) \times \prod_{v \in \Sigma_p} H^0(I_v, \tilde{A}/F_v^+ \tilde{A}) \xrightarrow{P_i} \prod_{v \in \Sigma \setminus \Sigma_p} H^0(I_v, \tilde{A}) \times \prod_{v \in \Sigma_p} H^0(I_v, \tilde{A}/F_v^+ \tilde{A}) \right].$$

It is the Pontrjagin dual of

$$\text{Ker} \left[\prod_{v \in \Sigma \setminus \Sigma_p} (\tilde{T}^*)_{I_v} \times \prod_{v \in \Sigma_p} ((\tilde{T}/F_v^+ \tilde{T})^*)_{I_v} \xrightarrow{P_i} \prod_{v \in \Sigma \setminus \Sigma_p} (\tilde{T}^*)_{I_v} \times \prod_{v \in \Sigma_p} ((\tilde{T}/F_v^+ \tilde{T})^*)_{I_v} \right].$$

Hence the module $\text{Ker}(t_i)$ is the Pontrjagin dual of the module $\bigoplus_{v \in \Sigma} C_v[P_i]$ by the definition of C_v . On the other hand, $\bigoplus_{v \in \Sigma} C_v/P_i C_v$ is finite by the assumption of Theorem 2.2 (2). Then we complete the proof of Theorem 2.2 (2) by applying Lemma 2.3 to the module $\bigoplus_{v \in \Sigma} C_v$. $\square$

3. GALOIS THEORETIC DEFORMATION FOR GREENBERG'S SELMER GROUP

In this section, we apply Theorem 2.2 to the strict Selmer groups of ordinary Galois representations in the cyclotomic deformation case. As applications, we treat the representation associated to a modular form and the representation associated to the symmetric power of an elliptic curve.

Let V be a p -adic representation of G_F , that is V is a finite dimensional vector space over a finite extension K of $\mathbb{Q}_p$ equipped with continuous G_F -action. Let us fix a G_F -stable lattice T of V . We denote the discrete G_F -module $T \otimes_{\mathcal{O}} K/\mathcal{O}$ by A . Let Σ_p be the set of primes of F dividing p and let us fix a finite set Σ of finite primes of F which

contains Σ_p . We assume that the representation V of G_F is unramified outside Σ . We fix a filtration $0 \subset F_v^+ T \subset T$ by a D_v -module for all $v \in \Sigma_p$. The definition of the strict Selmer group is as follows:

$$\mathrm{Sel}^{\mathrm{str}}(F, A) := \mathrm{Ker} \left[H^1(F, A) \longrightarrow \prod_{v \notin \Sigma_p} H^1(I_v, A) \times \prod_{v \in \Sigma_p} H^1(D_v, A/F_v^+ A) \right].$$

As an important class of p -adic representations, we have ordinary representations. The definition is as follows:

Definition 3.1. A p -adic representation V of G_F is called *ordinary* (resp. *quasi ordinary*) if the following conditions are satisfied:

- (1) For each prime v of F over p , we have a decreasing filtration as a D_v -module:

$$\cdots \mathrm{Fil}_v^i V \supset \mathrm{Fil}_v^{i+1} V \supset \cdots,$$

such that $\mathrm{Fil}_v^i V = V$ for $i \ll 0$ and $\mathrm{Fil}_v^i V = 0$ for $i \gg 0$.

- (2) For each v and each i , I_v acts on $\mathrm{Fil}_v^i V / \mathrm{Fil}_v^{i+1} V$ via the character χ^i where χ is the cyclotomic character (resp. there exists an open subgroup of I_v which acts on $\mathrm{Fil}_v^i V / \mathrm{Fil}_v^{i+1} V$ via the character χ^i).

For a quasi ordinary representation V , we define the filtration $F_v^+ V$ to be $\mathrm{Fil}_v^1 V$. Hence we attach the strict Selmer group $\mathrm{Sel}^{\mathrm{str}}(F, A)$ to a G_F -stable lattice $T \subset V$ by Definition 2.1.

Let $\tilde{F}$ be an abelian extension of F which is contained in F_Σ . Here, we do not necessarily assume $\tilde{F}/F$ to be a finite extension. We denote the Galois group $\mathrm{Gal}(\tilde{F}/F)$ simply by $\mathcal{G}$. The Galois group $\mathcal{G}$ is written as the projective limit:

$$\mathcal{G} = \varprojlim_{\alpha} \mathcal{G}_{\alpha},$$

where $\mathcal{G}_{\alpha}$ runs through all finite quotients of $\mathcal{G}$, which corresponds to finite Galois extensions $F \subset F_{\alpha} (\subset \tilde{F})$. In case $\tilde{F}$ is not finite over $\mathbb{Q}$, the Selmer group $\mathrm{Sel}^{\mathrm{str}}(\tilde{F}, A)$ is defined by the inductive limit:

$$\mathrm{Sel}^{\mathrm{str}}(\tilde{F}, A) = \varinjlim_{\alpha} \mathrm{Sel}^{\mathrm{str}}(F_{\alpha}, A).$$

By Shapiro's lemma, we have:

Lemma 3.2. *For each α , we have an isomorphism:*

$$H^i(F_{\alpha}, A) \cong H^i(F, \mathrm{Hom}_{\mathrm{cont}}(\mathcal{O}[\mathcal{G}_{\alpha}], A)).$$

By taking the inductive limit of the equation given in the above lemma, we have:

$$\begin{aligned}
H^i(\tilde{F}, A) &= \varinjlim_{\alpha} H^i(F_{\alpha}, A) \\
&= \varinjlim_{\alpha} H^i(F, \text{Hom}_{\text{cont}}(\mathcal{O}[\mathcal{G}_{\alpha}], A)) \\
&= H^i(F, \varinjlim_{\alpha} \text{Hom}_{\text{cont}}(\mathcal{O}[\mathcal{G}_{\alpha}], A)) \\
&= H^i(F, \text{Hom}_{\text{cont}}(\varprojlim_{\alpha} \mathcal{O}[\mathcal{G}_{\alpha}], A)) \\
&= H^i(F, \text{Hom}_{\text{cont}}(\mathcal{O}[[\mathcal{G}]], A)).
\end{aligned}$$

The following proposition is essentially proved in Greenberg's paper ([Gr2] Proposition 3.2). But for our purpose we need the following precise form:

Proposition 3.3. *For each α , we have:*

$$\text{Sel}^{\text{str}}(F_{\alpha}, A) = \text{Sel}^{\text{str}}(F, \text{Hom}_{\text{cont}}(\mathcal{O}[\mathcal{G}_{\alpha}], A)).$$

By taking the inductive limit of this equality, we have:

$$\text{Sel}^{\text{str}}(\tilde{F}, A) = \text{Sel}^{\text{str}}(F, \text{Hom}_{\text{cont}}(\mathcal{O}[[\mathcal{G}]], A)).$$

Proof. We have the following commutative diagram:

$$\begin{array}{ccccc}
0 \rightarrow \text{Sel}^{\text{str}}(F_{\Sigma}/F_{\alpha}, A) & \rightarrow & H^1(F_{\alpha}, A) & \xrightarrow{\gamma} & \prod_{w \nmid p, w \in \Sigma_{\alpha}} H^1(I_{\alpha, w}, A) \times \prod_{w|p} H^1(D_{\alpha, w}, A/F_v^+ A) \\
r_{\alpha} \downarrow & & s_{\alpha} \downarrow & & t_{\alpha} \downarrow \\
0 \rightarrow \text{Sel}^{\text{str}}(F, D_{\alpha}(A)) & \rightarrow & H^1(F_{\Sigma}/F, D_{\alpha}(A)) & \rightarrow & \prod_{v \nmid p, v \in \Sigma} H^1(I_v, D_{\alpha}(A)) \times \prod_{v|p} H^1(D_v, D_{\alpha}(A/F_v^+ A)),
\end{array}$$

where the module $D_{\alpha}(A)$ (resp. $D_{\alpha}(A/F_v^+ A)$) is the discrete G_F -module $\text{Hom}_{\mathcal{O}}(\mathcal{O}[\mathcal{G}_{\alpha}], A)$ (resp. $\text{Hom}_{\mathcal{O}}(\mathcal{O}[\mathcal{G}_{\alpha}], A/F_v^+ A)$), Σ_{α} is the set of primes of F_{α} which are over Σ and $D_{\alpha, w}$ (resp. $I_{\alpha, w}$) is the decomposition (resp. inertia) subgroup of $G_{F_{\alpha}}$ at w . In the above diagram, the map t_{α} on the right is defined as follows. Let $\mathcal{D}_{\alpha, v}$ (resp. $\mathcal{I}_{\alpha, v}$) be the decomposition (resp. inertia) subgroup of $\mathcal{G}_{\alpha}$ at v . The map t_{α} restricted to the first factor is induced by the map:

$$\begin{aligned}
\prod_{w|v} H^1(I_{\alpha, w}, A) &\longrightarrow H^1(I_v, D_{\alpha}(A)) = H^1(I_v, \text{Hom}_{\mathcal{O}}(\mathcal{O}[\mathcal{I}_{\alpha, v}], A))^{\oplus [\mathcal{D}_{\alpha} : \mathcal{I}_{\alpha, v}]} \\
&= \left(\prod_{w|v} H^1(I_{\alpha, w}, A)^{\oplus [\mathcal{D}_{\alpha, v} : \mathcal{I}_{\alpha, v}]} \right),
\end{aligned}$$

$$\{e_w\}_{w|v} \longmapsto \{e_w\}_{w|v} \times \{e_w\}_{w|v} \times \cdots \times \{e_w\}_{w|v} \text{ (} [\mathcal{D}_{\alpha, v} : \mathcal{I}_{\alpha, v}] \text{ times)}.$$

From this description, the map $t_{\alpha}|_{\prod_{w \nmid p} H^1(I_{\alpha, w}, A)}$ is injective. The map $t_{\alpha}|_{\prod_{w|p} H^1(K_{\alpha, w}, A/F_v^+ A)}$ is described similarly and is checked to be an isomorphism. Thus t_{α} is injective. By Lemma 3.2, the map s_{α} is an isomorphism. Hence the map r_{α} must be an isomorphism. $\square$

We consider the cyclotomic $\mathbb{Z}_p$ -extension F_∞/F of F . Let $\Gamma = \text{Gal}(F_\infty/F)$. We denote by F_n the unique sub-extension of F_∞/F which corresponds to the unique subgroup $\Gamma_n \subset \Gamma$ with index p^n . Let $\tilde{\kappa} : \Gamma \longrightarrow \mathcal{O}[[\Gamma]]^\times$ be the inclusion map $\Gamma \hookrightarrow \mathcal{O}[[\Gamma]]$. Let us fix a topological generator γ of Γ and fix an isomorphism $\mathcal{O}[[\Gamma]] \cong \Lambda_{\mathcal{O}}$ so that γ maps to the element $1 + X$ of $\Lambda_{\mathcal{O}}$. We denote by $\Lambda_{\mathcal{O}}(\tilde{\kappa})$ the free $\Lambda_{\mathcal{O}}$ -module of rank 1 on which $G_{\mathbb{Q}}$ acts by $\tilde{\kappa}$.

Definition 3.4 (Greenberg [Gr2]). We define $\tilde{T}$ (resp. $\tilde{T}/F_p^+ \tilde{T}$) to be $T \otimes_{\mathcal{O}} \Lambda_{\mathcal{O}}(\tilde{\kappa}^{-1})$ (resp. $(T/F_p^+ T) \otimes_{\mathcal{O}} \Lambda_{\mathcal{O}}(\tilde{\kappa}^{-1})$). This $\tilde{T}$ is called *the cyclotomic deformation* of T .

Then we have the following commutative diagram due to Proposition 3.3:

$$\begin{array}{ccc} \text{Sel}^{\text{str}}(F_n, A) & \cong & \text{Sel}^{\text{str}}(F, \tilde{A}[\omega_n]) \\ \downarrow & & \downarrow \\ \text{Sel}^{\text{str}}(F_\infty, A)^{\Gamma_n} & \cong & \text{Sel}^{\text{str}}(F, \tilde{A})[\omega_n], \end{array}$$

where $\tilde{A}$ is $\tilde{T} \otimes_{\Lambda_{\mathcal{O}}} \text{Hom}_{\text{cont}}(\Lambda_{\mathcal{O}}, \mathbb{Q}_p/\mathbb{Z}_p)$ and $\omega_n = (1 + X)^{p^n} - 1$. Thus we translated the problem into the language of deformation theory. Applying Theorem 2.2 to this situation, we obtain the following result:

Theorem 3.5. *Let V be an ordinary (resp. a quasi ordinary) p -adic representation of G_F and let T be a G_F -stable lattice of V . We denote $T \otimes_{\mathbb{Q}_p/\mathbb{Z}_p}$ by A . Let F_∞/F be the cyclotomic $\mathbb{Z}_p$ -extension of F . Then the following statements hold:*

- (1) *If $H^0(F_n, V) = 0$, the kernel of the restriction map:*

$$\text{Sel}^{\text{str}}(F_n, A) \xrightarrow{r_n} \text{Sel}^{\text{str}}(F_\infty, A)^{\Gamma_n},$$

is a finite group. Further, if $H^0(F_n, V) = 0$ for all $n \geq 0$, the order of the kernel of r_n is bounded independently of n .

- (2) *Assume that the eigenvalues of the action of Frob_v (resp. the eigenvalues of the action of a lift of Frob_v to D_v) on $(\text{Fil}_v^i V / \text{Fil}_v^{i+1} V) \otimes \mathbb{Q}_p(\chi^{-i})$ are not roots of unity for all $v|p$ and all $i \leq 0$. Then the cokernel of the restriction map r_n is a finite group whose order is bounded independently of n .*

Before proving the theorem, We give a remark on the relation between the above theorem and Mazur's control theorem stated in §1. Let E be an elliptic curve over $\mathbb{Q}$ which has good ordinary reduction at p . Then $V = T_p(E) \otimes \mathbb{Q}_p$ is an ordinary representation of $G_{\mathbb{Q}}$. Hence we attach $\text{Sel}^{\text{str}}(\mathbb{Q}, A)$ to the discrete $G_{\mathbb{Q}}$ -module $A = E[p^\infty] = T_p(E) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. It is easy to see that the above representation A of $G_{\mathbb{Q}}$ satisfies the assumptions of Theorem 3.5 (1) and (2). Hence the kernel and the cokernel of the restriction map $\text{Sel}^{\text{str}}(\mathbb{Q}_n, A) \xrightarrow{r_n} \text{Sel}^{\text{str}}(\mathbb{Q}_\infty, A)^{\Gamma_n}$ are bounded independently of n . As for the relation between this strict Selmer group and the classical Selmer group $\text{Sel}(E/\mathbb{Q}_n)\{p\}$ for the elliptic curve E , the following result is known:

Proposition 3.6 (Greenberg, [Gr1], [CG]). *Let E be an elliptic curve over $\mathbb{Q}$ which has good ordinary reduction at p . Let us denote $E[p^\infty]$ by A . For each n , we have a natural injection $\text{Sel}(E/\mathbb{Q}_n)\{p\} \xrightarrow{i_n} \text{Sel}^{\text{str}}(\mathbb{Q}_n, A)$. The order of the cokernel of the map i_n is a finite group whose order is bounded independently of n .*

Hence we recover the result of Mazur (Mazur's control theorem) in this case.

Let us return to the proof.

Proof of Theorem 3.5. By the assumption, $H^0(F, (\tilde{T}/\omega_n \tilde{T}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = 0$. Thus (1) follows by applying Theorem 2.2 (1).

Let us prove the assertion for the cokernel. We have only to check that the group $\bigoplus_{v \in \Sigma} C_v^{\text{str}}$ which is defined in §2 satisfies the condition of Theorem 2.2 (2).

First, we investigate the support of C_v^{str} for $v \nmid p$. For a prime $v \nmid p$ of F , the action of I_v on $\Lambda_{\mathcal{O}}(\tilde{\kappa})$ is trivial since primes not dividing p are unramified for any $\mathbb{Z}_p$ -extension of a number field. From this we see that $(\tilde{T}^*)_{I_v}$ is equal to $(T^*)_{I_v} \otimes_{\mathcal{O}} \Lambda_{\mathcal{O}}(\tilde{\kappa})$ and that C_v^{str} is equal to the $\Lambda_{\mathcal{O}}$ -torsion part of $((\tilde{T}^*)_{I_v}) = ((T^*)_{I_v})_{\mathcal{O}\text{-tor}} \otimes_{\mathcal{O}} \Lambda_{\mathcal{O}}(\tilde{\kappa})$, where $((T^*)_{I_v})_{\mathcal{O}\text{-tor}}$ is the $\mathcal{O}$ -torsion part of $(T^*)_{I_v}$. The module $C_v^{\text{str}}/\omega_n C_v^{\text{str}}$ is finite for each n since the ideal (ω_n) of $\Lambda_{\mathcal{O}}$ is relatively prime to the ideal $(\pi_{\mathcal{O}})$. Thus the assumption of Theorem 2.2 (2) is satisfied.

Next, we consider the case $v|p$. By definition, the filtration $F_v^+ T$ (resp. $F_v^+ \tilde{T}$) is $\text{Fil}_v^1 T$ (resp. $\text{Fil}_v^1 T \otimes_{\mathcal{O}} \Lambda_{\mathcal{O}}(\tilde{\kappa}^{-1})$). As for the cokernel part, it suffices to show that the D_v -coinvariant quotient of $(\tilde{T}/\text{Fil}_v^1 \tilde{T})^*$ is a $\Lambda_{\mathcal{O}}$ -module of finite length. In fact, the module $\bigoplus_{v \in \Sigma} C_v^{\text{str}}$ is finite and the condition of Theorem 2.2 (2) is satisfied. Let $i \leq 0$ be an integer. By the definition of $\tilde{T}$, we see that:

$$\begin{aligned} (\text{Fil}_v^i \tilde{T}/\text{Fil}_v^{i+1} \tilde{T})^* &= (\text{Fil}_v^i T/\text{Fil}_v^{i+1} T)^* \otimes_{\mathcal{O}} \Lambda(\tilde{\kappa}) \\ &= ((\text{Fil}_v^i T/\text{Fil}_v^{i+1} T) \otimes_{\mathcal{O}} \mathcal{O}(\chi^{-i}))^* \otimes_{\mathcal{O}} (\mathcal{O}(\chi^{-i}) \otimes_{\mathcal{O}} \Lambda(\tilde{\kappa})). \end{aligned}$$

By the assumption that V is quasi ordinary, there exists a non empty open subgroup J_v of I_v such that J_v acts non trivially on $((\text{Fil}_v^i T/\text{Fil}_v^{i+1} T) \otimes_{\mathcal{O}} \mathcal{O}(\chi^{-i}))^*$. For this J_v , the J_v -coinvariant quotient of $(\text{Fil}_v^i \tilde{T}/\text{Fil}_v^{i+1} \tilde{T})^*$ is given by:

$$((\text{Fil}_v^i \tilde{T}/\text{Fil}_v^{i+1} \tilde{T})^*)_{J_v} = ((\text{Fil}_v^i T/\text{Fil}_v^{i+1} T) \otimes_{\mathcal{O}} \mathcal{O}(\chi^{-i}))^* \otimes_{\mathcal{O}} ((\mathcal{O}(\chi^{-i}) \otimes_{\mathcal{O}} \Lambda_{\mathcal{O}}(\tilde{\kappa}))_{J_v}).$$

The eigenvalues of the action of a lift $\widetilde{\text{Frob}}_v \in D_v/J_v$ of the Frobenius element $\text{Frob}_v \in D_v/I_v$ on the second factor $((\mathcal{O}(\chi^{-i}) \otimes_{\mathcal{O}} \Lambda_{\mathcal{O}}(\tilde{\kappa}))_{J_v})$ are roots of unity. On the other hand, the eigenvalues of $\widetilde{\text{Frob}}_v$ on the first factor $((\text{Fil}_v^i \tilde{T}/\text{Fil}_v^{i+1} \tilde{T})^*)_{J_v} = ((\text{Fil}_v^i T/\text{Fil}_v^{i+1} T) \otimes_{\mathcal{O}} \mathcal{O}(\chi^{-i}))^*$ are not roots of unity. The D_v -coinvariant $((\text{Fil}_v^i \tilde{T}/\text{Fil}_v^{i+1} \tilde{T})^*)_{D_v}$ is finite for any $i \leq 0$ and so is the D_v -coinvariant $((\tilde{T}/\text{Fil}_v^1 \tilde{T})^*)_{D_v}$. Thus this completes the proof of (2) by the preceding remark. $\square$

As an attempt to generalize classical Iwasawa theory to Iwasawa theory for motives, explicit examples, primarily being the representations associated to modular forms or the symmetric powers of elliptic curves, are actively studied. We apply our Theorem 3.5 to these representations.

Let $f = \sum_{n=1}^{\infty} a_n q^n \in S_k(\Gamma_0(N), \psi)$ be a normalized newform of weight $k \geq 2$ and of level N prime to p where ψ is a Dirichlet character mod N . Deligne attached a $\mathfrak{p}$ -adic representation $\rho_f : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Q}_{f,\mathfrak{p}})$ to f where $\mathbb{Q}_f$ is the number field generated by $\{a_n\}_n$ over $\mathbb{Q}$ and $\mathfrak{p}$ is a prime of $\mathbb{Q}_f$ over p . We denote this 2-dimensional $\mathbb{Q}_{f,\mathfrak{p}}$ -vector space by V_f . We assume further that a_p is a $\mathfrak{p}$ -adic unit. Let us recall the following result, which was originally proved by Deligne in his letter to Serre. Later, Mazur and Wiles gave another proof by using Hida theoretic method. Since the original proof by Deligne is unpublished, we refer to [Wi] Theorem 2.1.4 and [Gro].

Proposition 3.7 (Deligne, Mazur-Wiles). *Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a normalized newform of weight $k \geq 2$ for $\Gamma_1(N)$. Assume that a_p is a $\mathfrak{p}$ -unit. Then the representation*

$$\rho_f : G_{\mathbb{Q}} \rightarrow GL(V_f) = GL_2(\mathbb{Q}_{f,\mathfrak{p}}),$$

restricted to the decomposition group D_p of p is equivalent to the representation of the form:

$$\begin{pmatrix} \epsilon_1 & * \\ 0 & \epsilon_2 \end{pmatrix},$$

Here, ϵ_2 is the unramified character such that $\epsilon_2(\text{Frob}_p) = \alpha$ where α is the $\mathfrak{p}$ -adic unit root of $x^2 - a_p x + \psi(p)p^{k-1}$, ψ is the Nebentypus character for f , and Frob_p is the p -th power arithmetic Frobenius.

From the Iwasawa theoretic view point, important ones among Tate twists $V_f(r)$ of V_f are those such that $V_f(r)$ are critical (we do not give the definition of critical representations here, but see [De2] for example). It is known that $V_f(r)$ is critical when $2 - k \leq r \leq 0$. Let V be $V_f(r)$ with $2 - k \leq r \leq 0$. Let us fix a $G_{\mathbb{Q}}$ -stable lattice T of V . By Proposition 3.7, $V_f(r)$ is a quasi ordinary representation of $G_{\mathbb{Q}}$. So $V_f(r)$ is quasi ordinary as a representation of $G_{\mathbb{Q}_n}$ for each $n \geq 0$. Therefore we associate a strict Selmer group $\text{Sel}^{\text{str}}(\mathbb{Q}_n, A)$ to $A = T \otimes \mathbb{Q}_p/\mathbb{Z}_p$ for each $n \geq 0$. By taking the inductive limit with respect to n , we define $\text{Sel}^{\text{str}}(\mathbb{Q}_{\infty}, A) = \varinjlim_n \text{Sel}^{\text{str}}(\mathbb{Q}_n, A)$.

Proposition 3.8. *Let $\mathbb{Q}_{\infty}/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$ -extension of $\mathbb{Q}$. We denote $V_f(r)$ with $2 - k \leq r \leq 0$ by V . Let T be a $G_{\mathbb{Q}}$ -stable lattice of V . We denote $T \otimes \mathbb{Q}_p/\mathbb{Z}_p$ by A . Then the kernel and the cokernel of the restriction map*

$$\text{Sel}^{\text{str}}(\mathbb{Q}_n, A) \xrightarrow{r_n} \text{Sel}^{\text{str}}(\mathbb{Q}_{\infty}, A)^{\Gamma_n},$$

are finite groups whose orders are bounded independently of n .

Proof of Proposition 3.8. We have only to check the conditions of Theorem 3.5 for these representations.

In order to prove the assertion for the kernel of r_n , we have only to show that $H^0(\mathbb{Q}_n, V) = 0$ for each n according to Theorem 3.5 (1).

First, consider the case where the weight of the Galois representation $V_f(r)$ is not zero, that is, we consider the case where $1 - k - 2r$ is not zero. Then we see that $H^0(\mathbb{Q}_n, V_f(r)) = 0$ by considering the action of the Frobenius Frob_l for $l \nmid Np$.

Next, consider the case where f is not of CM -type (We do not give the definition for a cusp form f to be of CM -type, but we refer [R1] for the definition). If f is not of

CM -type, the image of $G_{\mathbb{Q}}$ in $\text{Aut}(V_f(r))$ is an open subgroup of $\text{Aut}(V_f(r))$ (cf. [R1], [R2]). Since $G_{\mathbb{Q}_n}$ is open in $G_{\mathbb{Q}}$, the image of $G_{\mathbb{Q}_n}$ is also an open subgroup of $\text{Aut}(V_f(r))$. Hence, even in the case where the Galois representation $V_f(r)$ has weight zero, we see that $H^0(\mathbb{Q}_n, V_f(r)) = 0$.

Now the case left for us is $V_f(r)$ such that f is of CM -type and $1 - k - 2r = 0$. In this case, there exists a quadratic imaginary extension K of $\mathbb{Q}$ with the property that for any open subgroup H of $G_{\mathbb{Q}}$, the action of H on $V_f(r)$ is irreducible if and only if $H \not\subset G_K$ (cf. [R1] Proposition 4.4). Now since we are assuming that p is odd, $G_{\mathbb{Q}_n}$ is not contained in G_K for any n . This completes the proof of the assertion for $\ker(r_n)$.

The graded quotient $\text{Fil}_p^i V / \text{Fil}_p^{i+1} V$ for $i \leq 0$ is non zero only when $i = r$. The Frobenius element Frob_p acts on $(\text{Fil}_p^r V / \text{Fil}_p^{r+1} V) \otimes_{\mathbb{Q}_p} (\chi^{-r})$ via the character ϵ_2 . Recall that $\alpha = \epsilon_2(\text{Frob}_p)$ is the p -adic unit root of the equation $x^2 - a_p x + \psi(p)p^{k-1}$. Since α has complex absolute value $p^{(k-1)/2}$, α is not a root of unity. $\square$

We also treat the symmetric power of the representation associated to an elliptic curve. Let E be an elliptic curve over $\mathbb{Q}$ which has good ordinary reduction at p . We denote the p -unit root of $x^2 - a_p x + p$ by α_E . Then $V_d := \text{Sym}^d V_p(E)$ is also an ordinary representation and we have $\text{Fil}_p^i V / \text{Fil}_p^{i+1} V = \mathbb{Q}_p(\chi^i \cdot \epsilon^{2i-1})$, where ϵ is the unramified character of D_p such that $\epsilon(\text{Frob}_p) = \alpha_E$. As in the previous case, we concentrate on critical Tate twists of $V_d(r)$. It is known that the only critical Tate twist $V_d(r)$ of V_d is $V_d(\frac{d+1}{2})$ when d is odd (cf. [Da]). So we treat only the case $r = \frac{d+1}{2}$. We have the following theorem as a corollary of Theorem 2.2:

Proposition 3.9. *Let V be $V_d(\frac{-d+1}{2})$ where d is an odd positive integer. Then the restriction map*

$$\text{Sel}^{\text{str}}(\mathbb{Q}_n, A) \xrightarrow{r_n} \text{Sel}^{\text{str}}(\mathbb{Q}_{\infty}, A)^{\Gamma_n},$$

has finite kernel and cokernel which are bounded independently of n .

Proof. The module $H^0(\mathbb{Q}_n, V)$ is zero for all n since $V_d(\frac{-d+1}{2})$ has weight -1 . Thus the assertion for the kernel follows from Theorem 3.5 (1).

Let us prove the finiteness and boundedness of the cokernel. The eigenvalues of the action of the arithmetic Frobenius Frob_p on $(\text{Fil}_p^i V / \text{Fil}_p^{i+1} V) \otimes_{\mathbb{Q}_p} (\chi^{-i}) \cong \mathbb{Q}_p(\epsilon^{2i-1})$ are not roots of unity since α_E has complex absolute value $p^{\frac{1}{2}}$. Thus the condition of Theorem 3.5 (2) is satisfied. $\square$

Remark 3.10. Our method can not treat the d -th symmetric power for an even d . In fact, $((\tilde{T}/\text{Fil}_p^1 \tilde{T})^*)_{D_p}$ may not be finite for an even d . In the case $d = 2$, there is an interesting work by Hida, which describes the behavior of Greenberg's Selmer groups for the adjoint representations associated to ordinary modular forms assuming the irreducibility of the mod p representations (see [H3] for the precise statement of the result).

4. Λ -ADIC FORMS AND ASSOCIATED GALOIS REPRESENTATIONS

In this section, we recall some fundamental results on Λ -adic form and its Galois representation which is necessary in the next section for applications of our theorem to Hida deformations. For more detail on this theory, the reader can refer to Chap.7 of [H4].

We fix a prime number $p \geq 5$, a positive integer N which is prime to p and an integer $r \geq 0$. Throughout the section, we fix a complex embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and a p -adic embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$ and let ψ be a Dirichlet character modulo Np^r . We denote by $M_k(\Gamma_1(Np^r), \psi; \mathcal{O})$ (resp. $S_k(\Gamma_1(Np^r), \psi; \mathcal{O})$) the space of p -adic modular (resp. cusp) forms defined by Serre and Katz. Consider a formal q -expansion:

$$\mathcal{F} = \sum_{0 \leq n < \infty} A(n, \mathcal{F}) q^n,$$

where each $A(n, \mathcal{F})$ is an element of a fixed algebraic closure of $\text{Frac}(\mathbb{Z}_p[[X]])$. We assume that the ring $R_{\mathcal{F}}$ generated by all $A(n, \mathcal{F})$'s over $\mathbb{Z}_p[[X]]$ is finite flat over $\mathbb{Z}_p[[X]]$. For an ideal $\mathfrak{p}$ of $R_{\mathcal{F}}$, we denote by $\mathcal{F}_{/\mathfrak{p}}$ the formal q -expansion $\sum_{0 \leq n < \infty} A(n, \mathcal{F})_{/\mathfrak{p}} q^n$, where $A(n, \mathcal{F})_{/\mathfrak{p}}$ is the image of $A(n, \mathcal{F})$ under the map $R_{\mathcal{F}} \rightarrow R_{\mathcal{F}}/\mathfrak{p}$.

Definition 4.1. Let the notations be as above. Assume that $r \geq 1$. We call $\mathcal{F}$ a Λ -adic form of level Np^r with Dirichlet character ψ if for all $k \geq 2$ and for all prime ideal $\mathfrak{p}$ of $R_{\mathcal{F}}$ which is over the prime ideal $(P_k) = (X + 1 - (1 + p)^{k-2})$ of Λ , the power series $\mathcal{F}_{/\mathfrak{p}}$ is the q -expansion of a modular form in $M_k(\Gamma_1(Np^r), \psi \omega^{2-k}; R_{\mathcal{F}}/\mathfrak{p})$.

Definition 4.2. Assume that $r \geq 1$. Then a p -adic cusp form $f \in S_k(\Gamma_1(Np^r), \psi; \mathcal{O})$ is called a p -stabilized newform of tame conductor N with Dirichlet character ψ if

- (1) f is an eigenform of $S_k(\Gamma_1(Np^r), \psi; \mathcal{O})$ for all Hecke operators $T_l(l \nmid Np)$ and $U_{l'}(l' | Np)$ which belong to $\text{End}(S_k(\Gamma_1(Np^r), \psi; \mathcal{O}))$.
- (2) The newform associated to f has level Np^{r_0} for some r_0 , $0 \leq r_0 \leq r$.
- (3) The eigenvalue a_p of f for $U_p \in \text{End}(S_k(\Gamma_1(Np^r), \psi; \mathcal{O}))$ is a p -adic unit.

Let f be a newform in $S_k(\Gamma_1(N), \psi; \mathcal{O})$. Assume that the eigenvalue a_p of f for the Hecke operator T_p is a p -adic unit. We define f^* by $f^* = f(z) - \beta f(pz)$, where β is the unique root of $x^2 - a_p x + \psi(p)p^{k-1}$ with $|\beta| < 1$. Then f^* is the p -stabilized newform and the n -th Fourier coefficient of f equals to the n -th Fourier coefficient of f^* if p does not divide n . We call this f^* the p -stabilized newform associated to f .

Definition 4.3. A normalized Λ -adic eigenform $\mathcal{F}$ is a Λ -adic newform of tame conductor N if for all $k \geq 2$ and all height one ideals $\mathfrak{p} \subset R_{\mathcal{F}}$ over the ideal $(P_k) = ((1 + X) - (1 + p)^{k-2})$ of $\Lambda_{\mathcal{O}}$, the modular form $\mathcal{F}_{/\mathfrak{p}}$ is a p -stabilized newform of tame conductor N .

Theorem 4.4 (Hida [H1] Corollary 3.2, Corollary 3.7). *Let $f \in S_k(\Gamma_0(Np^r), \psi; \mathcal{O})$ be a p -stabilized newform of tame conductor N . Then there exists a Λ -adic newform $\mathcal{F}$ of tame conductor N with Dirichlet character $\psi \omega^k$ such that $\mathcal{F}_{/\mathfrak{p}}$ equals to f for some ideal $\mathfrak{p}$ of $R_{\mathcal{F}}$ which is over the ideal $((1 + X) - (1 + p)^{k-2})$ of $\Lambda_{\mathcal{O}}$.*

Definition 4.5. Let $\mathcal{K}_{\mathcal{F}}$ be the field of fraction of $R_{\mathcal{F}}$. The representation $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{K}_{\mathcal{F}})$ is *continuous* if there exists a finitely generated $R_{\mathcal{F}}$ -module $L \subset \mathcal{K}_{\mathcal{F}}^{\oplus 2}$ which is stable under $G_{\mathbb{Q}}$ -action such that $\rho : G_{\mathbb{Q}} \rightarrow \text{Aut}(L)$ is continuous with respect to the topology of L defined by the maximal ideal of $R_{\mathcal{F}}$ and that $L \otimes_{R_{\mathcal{F}}} \mathcal{K}_{\mathcal{F}} \cong \mathcal{K}_{\mathcal{F}}^{\oplus 2}$.

Theorem 4.6 (Hida [H2]). *Let $\mathcal{F}$ be a Λ -adic newform. Then, there exists a continuous irreducible representation $\rho_{\mathcal{F}} : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{K}_{\mathcal{F}})$ satisfying the following properties:*

- (1) $\rho_{\mathcal{F}}$ is unramified outside Np .
- (2) For $l \nmid Np$, we have:

$$\begin{aligned} \text{Trace}(\rho_{\mathcal{F}}(\text{Frob}_l)) &= A(l, \mathcal{F}), \\ \det(\rho_{\mathcal{F}}(\text{Frob}_l)) &= \psi(l)\kappa(\langle l \rangle)l^{-1}, \end{aligned}$$

where ψ is the Dirichlet character of $\mathcal{F}$, $d \rightarrow \langle d \rangle$ is the projection $\mathbb{Z}_p^{\times} \cong (\mathbb{Z}/p\mathbb{Z})^{\times} \times (1 + p\mathbb{Z}_p) \rightarrow (1 + p\mathbb{Z}_p)$ and κ is the character $1 + p\mathbb{Z}_p \rightarrow \Lambda_{\mathcal{O}}^{\times}$, $(1 + p)^s \mapsto (1 + X)^s$.

We have the following proposition due to Mazur and Wiles:

Proposition 4.7 ([Wi] Theorem 2.2.2). *Let the assumptions be as in Theorem 4.6. Then the restriction $\rho_{\mathcal{F}}|_{D_p}$ to the decomposition group D_p of $\rho_{\mathcal{F}}$ is equivalent to the representation of the form:*

$$\begin{pmatrix} \tilde{\epsilon}_1 & * \\ 0 & \tilde{\epsilon}_2 \end{pmatrix},$$

where $\tilde{\epsilon}_2$ is the unramified character such that $\tilde{\epsilon}_2(\text{Frob}_p) = A(p, \mathcal{F})$.

In order to study the Iwasawa theory for Hida deformations, we will always assume the following condition:

(**Int**) The representation $\rho_{\mathcal{F}} : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{K}_{\mathcal{F}})$ has a $G_{\mathbb{Q}}$ -stable lattice $\tilde{T}$ which is isomorphic to $R_{\mathcal{F}}^{\oplus 2}$.

The condition (**Int**) is satisfied in fairly general situations. Before stating some sufficient conditions for (**Int**) to be satisfied (Proposition 4.9), we introduce some necessary notations.

Definition 4.8. Let $k_{\mathcal{F}}$ be the residue field of $R_{\mathcal{F}}$ modulo the maximal ideal $m_{\mathcal{F}}$ of $R_{\mathcal{F}}$. A semi-simple representation $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(k_{\mathcal{F}})$ is called *the residual representation* associated to $\mathcal{F}$ if $\bar{\rho}$ is unramified outside Np and the characteristic polynomial of the arithmetic Frobenius Frob_l for each prime $l \nmid Np$ is congruent to

$$X^2 - A(l; \mathcal{F})X - \psi(l)\kappa(\langle l \rangle)l^{-1} \text{ modulo } m_{\mathcal{F}}.$$

Such residual representation is always known to exist and it is unique up to isomorphism.

Proposition 4.9 (Mazur-Wiles, Tilouine, Mazur-Tilouine). *Let the notations be as above. Then the condition (**Int**) holds if one of the following conditions is satisfied:*

- (1) *The tame conductor N of $\mathcal{F}$ is equal to 1 and the ring $R_{\mathcal{F}}$ is Gorenstein (Mazur-Wiles [MW] §9).*
- (2) *Let a be a number such that $\psi|_{(\mathbb{Z}/p\mathbb{Z})^{\times}} = \omega^a$ where ω is Teichmüller character. Then $a \not\equiv 0, -1 \text{ modulo } p-1$ and the ring $R_{\mathcal{F}}$ is Gorenstein (Tilouine [Ti] Theorem 4.4).*
- (3) *The residual representation is irreducible (Mazur-Tilouine [MT] §2, Corollary 6).*

5. CONTROL THEOREM FOR HIDA DEFORMATION

In this section, we apply Theorem 2.2 to the Selmer group for the Λ -adic representation $\tilde{T}$ associated to a Λ -adic form $\mathcal{F}$. We continue to use the notations of the previous section. Throughout this section, we assume the condition **(Int)**. By Proposition 4.7, $\tilde{T}$ has the decreasing filtration $0 \subset F_p^+ \tilde{T} = R_{\mathcal{F}}(\tilde{\epsilon}_1) \subset \tilde{T}$ as $R_{\mathcal{F}}[D_p]$ -module, where $R_{\mathcal{F}}(\tilde{\epsilon}_1)$ is a rank 1 $R_{\mathcal{F}}$ -module on which D_p acts via the character $\tilde{\epsilon}_1$. By using this filtration $F_p^+ \tilde{T}$, the Selmer group $\text{Sel}(\mathbb{Q}, \tilde{A})$ is defined (see Definition 2.1). Let us define the set of ideals $\mathcal{I}$ of $R_{\mathcal{F}}$ as follows:

$$\mathcal{I} = \{\mathfrak{p} \in \text{Spec}(R_{\mathcal{F}}) \mid \exists k \geq 2 \text{ such that } \mathfrak{p} \text{ divides the ideal } ((1+X) - (1+p)^k)\}.$$

We control the Selmer group $\text{Sel}(\mathbb{Q}, \tilde{A})$ under the specialization at the ideals in $\mathcal{I}$ by applying Theorem 2.2. The result is as follows:

Theorem 5.1. *Let $\tilde{T}$ be the Λ -adic representation associated to a Λ -adic newform $\mathcal{F}$ of tame conductor N and Dirichlet character ψ . Then the kernel and the cokernel of the restriction map:*

$$\text{Sel}(\mathbb{Q}, \tilde{A}[\mathfrak{p}]) \xrightarrow{r_{\mathfrak{p}}} \text{Sel}(\mathbb{Q}, \tilde{A})[\mathfrak{p}],$$

are finite groups for each $\mathfrak{p} \in \mathcal{I}$.

Further, let us assume that $R_{\mathcal{F}}$ is equal to $\Lambda_{\mathcal{O}}$. Then the order of the kernel of $r_{\mathfrak{p}}$ is bounded by the order of the largest finite submodule of $(\tilde{T}^)_{G_{\mathbb{Q}}}$ and the order of the cokernel of $r_{\mathfrak{p}}$ are bounded by the order of the finite group $\bigoplus_{l|N} \underline{C}_l$, where $\underline{C}_l$ is the largest finite submodule of the $\Lambda_{\mathcal{O}}$ -torsion part C_l of $(\tilde{T}^*)_{I_l}$ for each $l|N$.*

Remark 5.2. Let $\mathcal{F}$ be the Λ -adic newform which extends a p -stabilized newform $f \in S_k(\Gamma_1(Np^r); \psi)$. Then $R_{\mathcal{F}}$ is equal to $\Lambda_{\mathcal{O}}$ if there is no other p -stabilized newform $f' \in S_k(\Gamma_1(Np^r); \psi)$ which is congruent to f modulo $(\pi_{\mathcal{O}})$. Especially, $R_{\mathcal{F}}$ is equal to $\Lambda_{\mathcal{O}}$ if the dimension of the ordinary part of $S_k(\Gamma_1(Np^r); \psi)$ is one.

Proof of Theorem 5.1. The $\Lambda_{\mathcal{O}}$ -module $\tilde{T}$ is free of rank $2d$ over $\Lambda_{\mathcal{O}}$ where $d = \text{rank}_{\Lambda_{\mathcal{O}}} R_{\mathcal{F}}$. Let (P_k) be the principal ideal $((1+X) - (1+p)^k)$ of $\Lambda_{\mathcal{O}}$. $\tilde{A}[P_k]$ is cofree of corank 2 over $R_{\mathcal{F}}/(P_k)$. Hence $\tilde{A}[P_k]$ is cofree of corank $2d$ over $\mathcal{O}$.

First, we show that the kernel (resp. cokernel) of the restriction map:

$$\text{Sel}(\mathbb{Q}, \tilde{A}[P_k]) \xrightarrow{r_k} \text{Sel}(\mathbb{Q}, \tilde{A})[P_k],$$

is a finite group whose order is bounded by the order of the largest finite subgroup of $(\tilde{T}^*)_{G_{\mathbb{Q}}}$ (resp. the order of the finite group $\bigoplus_{l|N} \underline{C}_l$).

Let us prove the assertion for the kernel of r_k . By Theorem 2.2 (1), we have only to show that $H^0(\mathbb{Q}, (\tilde{T}/P_k \tilde{T}) \otimes K)$ is zero for each $k \geq 2$. The following lemma is easily seen from [H1] Corollary 3.7:

Lemma 5.3. *Let $\mathcal{F}$ be a Λ -adic newform of tame conductor N . Then the following statements hold:*

- (1) For each $k \geq 2$, there exists exactly d primes dividing (P_k) and the kernel and cokernel of the natural map

$$R_{\mathcal{F}}/(P_k) \longrightarrow \bigoplus_{\mathfrak{p} | (P_k)} R_{\mathcal{F}}/\mathfrak{p}$$

are finite groups.

- (2) For each $k \geq 2$ and each $\mathfrak{p} | (P_k)$, the tame conductor of the cusp form $\mathcal{F}_{/\mathfrak{p}}$ is N .

By the above lemma, the representation $(\tilde{T}/P_k \tilde{T}) \otimes_{\mathcal{O}} K$ is isomorphic to the representation $\bigoplus_{\mathfrak{p} | (P_k)} ((\tilde{T}/\mathfrak{p} \tilde{T}) \otimes_{\mathcal{O}} K)$. Since the action of $G_{\mathbb{Q}}$ on $(\tilde{T}/\mathfrak{p} \tilde{T}) \otimes_{\mathcal{O}} K$ is irreducible by a work of Ribet [R1], $H^0(\mathbb{Q}, (\tilde{T}/\mathfrak{p} \tilde{T}) \otimes_{\mathcal{O}} K)$ is zero for each prime $\mathfrak{p} | (P_k)$. Hence the group $H^0(\mathbb{Q}, (\tilde{T}/P_k \tilde{T}) \otimes_{\mathcal{O}} K)$ is also zero.

Next, let us prove the assertion for the cokernel of the restriction map r_k . By Theorem 2.1 (2), we have only to show that $\bigoplus_{v | Np} C_v/P_k C_v$ is a finite group for each $k \geq 2$. Let us recall the following result on Fourier coefficients of newforms due to Ogg:

Proposition 5.4 (Ogg [Og]). *Let $M \geq 1$ be an integer. Let $f = \sum a_n q^n \in S_k(\Gamma_1(M); \psi)$ be a weight k newform of conductor M with Dirichlet character ψ and let l be a prime number dividing M . We denote by $\mathfrak{f}(\psi)$ the conductor of Dirichlet character ψ .*

- (1) *Assume that l divides M but l^2 does not divide M . Then a_l is not zero. If ψ comes from a Dirichlet character defined modulo M/l , then $a_l^2 = \psi(l)l^{k-2}$ or $a_l^2 = l^{k-2}$. If ψ does not come from a Dirichlet character defined modulo M/l , then a_l has the complex absolute value $l^{\frac{k-1}{2}}$.*
- (2) *Assume that l^2 divides M . Then a_l is not zero if and only if ψ does not come from a Dirichlet character defined modulo M/l . Further, in this case, the complex absolute value of a_l is $l^{\frac{k-1}{2}}$.*

A theorem of Carayol ([Ca]) guarantees the equality of the automorphic L -function of a modular form and the L -function of the l -adic representation associated to the modular form. On the other hand, Proposition 5.4 gives the description of l -th Fourier coefficients of a modular form f only in terms of the conductor and the Dirichlet character of f . Combining these results with Lemma 5.3 (2), we obtain the following:

$$\text{rank}_{\mathcal{O}}((\tilde{T}^*)_{I_l}/\mathfrak{p}(\tilde{T}^*)_{I_l}) = \text{rank}_{\mathcal{O}}(\tilde{T}^*/\mathfrak{p} \tilde{T}^*)_{I_l} = \begin{cases} 1 & \text{if } \text{ord}_l(N) = \text{ord}_l(\mathfrak{f}(\psi)) \text{ or } \text{ord}_l(N) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

On the other hand, the kernel and the cokernel of the natural map

$$\tilde{T}^*/P_k \tilde{T}^* \longrightarrow \bigoplus_{\mathfrak{p} | (P_k)} (\tilde{T}^*/\mathfrak{p} \tilde{T}^*),$$

are finite groups by Lemma 5.3 (1). Hence, we have:

$$\text{rank}_{\mathcal{O}}((\tilde{T}^*)_{I_l}/P_k(\tilde{T}^*)_{I_l}) = \begin{cases} d & \text{if } \text{ord}_l(N) = \text{ord}_l(\mathfrak{f}(\psi)) \text{ or } \text{ord}_l(N) = 1 \\ 0 & \text{otherwise,} \end{cases}$$

for each $k \geq 2$. Thus we have the following lemma:

Lemma 5.5. *We see that*

$$\text{rank}_{\Lambda_{\mathcal{O}}}(\tilde{T}^*)_{I_l} = \begin{cases} d & \text{if } \text{ord}_l(N) = \text{ord}_l(\mathfrak{f}(\psi)) \text{ or } \text{ord}_l(N) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Further, the module $C_l/P_k C_l$ is finite for each $k \geq 2$ and each $l|N$, where C_l is the $\Lambda_{\mathcal{O}}$ -torsion part of the $\Lambda_{\mathcal{O}}$ -module $(\tilde{T}^*)_{I_l}$.

Let us denote by C_p the $\Lambda_{\mathcal{O}}$ -torsion part of the I_p coinvariant quotient $((\tilde{T}/F_p^+ \tilde{T})^*)_{I_p}$. I_p acts trivially on $(\tilde{T}/F_p^+ \tilde{T})$ due to Proposition 4.7. Thus we have $((\tilde{T}/F_p^+ \tilde{T})^*)_{I_p} = (\tilde{T}/F_p^+ \tilde{T})^*$. This implies that C_p is zero. Thus we conclude that the cokernel of the restriction map:

$$\text{Sel}(\mathbb{Q}, \tilde{A}[P_k]) \xrightarrow{r_k} \text{Sel}(\mathbb{Q}, \tilde{A})[P_k],$$

is a finite group whose order is bounded by the order of the finite group $\bigoplus_{l|N} C_l$.

In the case where $R_{\mathcal{F}}$ is equal to $\Lambda_{\mathcal{O}}$, this completes the proof of the theorem.

In case $R_{\mathcal{F}}$ is not equal to $\Lambda_{\mathcal{O}}$, we need more argument. We have the following commutative diagram:

$$\begin{array}{ccc} \text{Sel}(\mathbb{Q}, \tilde{A}[P_k]) & \xrightarrow{r_k} & \text{Sel}(\mathbb{Q}, \tilde{A})[P_k] \\ v_1 \uparrow & & \uparrow v_2 \\ \bigoplus_{\mathfrak{p}|(P_k)} \text{Sel}(\mathbb{Q}, \tilde{A}[\mathfrak{p}]) & \xrightarrow{\bigoplus_{\mathfrak{p}|(P_k)} r_{\mathfrak{p}}} & \bigoplus_{\mathfrak{p}|(P_k)} \text{Sel}(\mathbb{Q}, \tilde{A})[\mathfrak{p}] \end{array}$$

The following lemma is well-known:

Lemma 5.6. *Let V be a p -adic representation of $G_{\mathbb{Q}}$ unramified outside a finite set Σ of primes of $\mathbb{Q}$. Let us fix a filtration $F^+ V \subset V$ as D_p -module. We take two $G_{\mathbb{Q}}$ -stable lattices $T \subset T'$ of V . Then the natural map $\text{Sel}(\mathbb{Q}, A) \rightarrow \text{Sel}(\mathbb{Q}, A')$ induced from the map $T \rightarrow T'$ has a finite kernel and a finite cokernel.*

Hence the kernel and the cokernel of the map v_1 are finite groups. On the other hand, the kernel and the cokernel of the map v_2 are finite groups since $\text{Supp}_{R_{\mathcal{F}}}(R_{\mathcal{F}}/(P_k)) = \bigcup_{\mathfrak{p}|(P_k)} \text{Supp}_{R_{\mathcal{F}}}(R_{\mathcal{F}}/\mathfrak{p})$. Consequently, the kernel and the cokernel of the restriction map

$\text{Sel}(\mathbb{Q}, \tilde{A}[\mathfrak{p}]) \xrightarrow{r_{\mathfrak{p}}} \text{Sel}(\mathbb{Q}, \tilde{A})[\mathfrak{p}]$ are finite groups. This completes the proof of Theorem 5.1. $\square$

From the above theorem, we deduce the following corollary:

Corollary 5.7. *Let the notations be as in Theorem 5.1. Then the following three conditions are equivalent:*

- (1) *The Selmer group $\text{Sel}(\mathbb{Q}, \tilde{A}[\mathfrak{p}])$ is finite for some $\mathfrak{p} \in \text{mc}I$.*
- (2) *The Selmer groups $\text{Sel}(\mathbb{Q}, \tilde{A}[\mathfrak{p}])$ are finite for all but finitely many $\mathfrak{p} \in \mathcal{I}$.*
- (3) *The Selmer group $\text{Sel}(\mathbb{Q}, \tilde{A})$ is a cotorsion $R_{\mathcal{F}}$ -module.*

Remark 5.8. The condition (3) is a part of Iwasawa Main Conjecture for Hida deformations proposed by Greenberg (cf. [Gr2] Conjecture 2.2). By Kato's deep result ([K1] and [K2]), Selmer groups $\text{Sel}(\mathbb{Q}, \tilde{A}[p])$ are finite for each $k \geq 3$. Hence, by Corollary 5.7, Selmer groups $\text{Sel}(\mathbb{Q}, \tilde{A})$ are cotorsion $R_{\mathcal{F}}$ -modules assuming Kato's result.

In some special cases, we know more about the restriction map. For example, we have the following corollary:

Corollary 5.9. *Let the notations be as in Theorem 5.1. Let $\mathbb{Z}_l^{\text{ur}}$ be the integer ring of the maximal unramified extension $\mathbb{Q}_l^{\text{ur}}$ of $\mathbb{Q}_l$. Let E be a modular elliptic curve over $\mathbb{Q}$ which has good ordinary reduction or multiplicative reduction at p . Let $\mathcal{F}_E$ be the Λ -adic newform which extends the p -stabilized newform f_E^* associated to the newform f_E corresponding to E (see Definition 4.2 and Theorem 4.4). Assume that $R_{\mathcal{F}}$ is equal to $\Lambda_{\mathcal{O}}$. Then the following statements hold.*

- (1) *If the elliptic curve E has no non-zero p -torsion points over $\mathbb{Q}$, the restriction map r_k is injective for all k .*
- (2) *Assume that the number $\tilde{n}_{E,l}$ of the components of the special fiber of the Neron model $\mathcal{E}_l$ of E over $\mathbb{Z}_l^{\text{ur}}$ is not divisible by p for all prime l which divide N exactly. Then the restriction map r_k is surjective for all $k \geq 2$.*

Proof. As for the statement (1), we have only to show that $(\tilde{T}^*)_{G_{\mathbb{Q}}} = 0$ by using Theorem 5.1. Now $(\tilde{T}^*)_{G_{\mathbb{Q}}}/P_2(\tilde{T}^*)_{G_{\mathbb{Q}}} = (\tilde{T}^*/P_2\tilde{T}^*)_{G_{\mathbb{Q}}} = (T_p E^*)_{G_{\mathbb{Q}}}$. But the group $(T_p E^*)_{G_{\mathbb{Q}}}$ is zero by the assumption of (1). Hence $(\tilde{T}^*)_{G_{\mathbb{Q}}}$ is zero.

Let us show the statement (2). For $l|N$, let the module $\underline{C}_l$ be as in Theorem 5.1. We have only to show that $\underline{C}_l$ is zero for all $l|N$.

First, consider the case where l exactly divides N . In this case, $(\tilde{T}^*)_{I_l}$ has Λ -rank 1. For the Λ -torsion part C_l of $(\tilde{T}^*)_{I_l}$, the quotient $C_l/P_2 C_l$ is isomorphic to the $\mathbb{Z}_p$ -torsion part of $(T_p E^*)_{I_l}$. By the theory of Tate curves, the $\mathbb{Z}_p$ -torsion part of $(T_p E^*)_{I_l}$ is isomorphic to $\mathbb{Z}_p/\tilde{n}_{E,l}\mathbb{Z}_p$. Since $\tilde{n}_{E,l}$ is a p -unit by the assumption, $C_l/P_2 C_l$ is zero and so are the modules C_l and $\underline{C}_l$.

Next, we consider the case where l^2 divides N . In this case, $(\tilde{T}^*)_{I_l}$ is a torsion Λ -module. By definition, C_l is $(\tilde{T}^*)_{I_l}$. The module $C_l/P_2 C_l$ is $(T_p E^*)_{I_l}$. Since E has additive reduction at l and $p \geq 5$, $(T_p E^*)_{I_l}$ is zero. So the modules C_l and $\underline{C}_l$ are also zero. $\square$

In some cases, the control theorem (Theorem 5.1) and its corollary (Corollary 5.9) are useful to calculate the Selmer group $\text{Sel}(\mathbb{Q}, \tilde{A})$ of a Hida deformation $\tilde{T}$. Let us give an example. Consider Ramanujan's cusp form:

$$\Delta = q \prod_{1 \leq m \leq \infty} (1 - q^m)^{24} = \sum_{1 \leq n \leq \infty} \tau(n) q^n,$$

which has weight 12 and level 1. The p -th coefficient $\tau(p)$ is a p -unit except $p = 2, 3, 5, 7, 2411$ for primes $\leq 10,000$. Let us consider the first ordinary prime $p = 11$. Let us denote by Δ^* the p -stabilized newform of level p associated to Δ and let $\mathcal{F}$ be the Λ -adic newform which extends Δ^* . In this case, we have $R_{\mathcal{F}} = \Lambda_{\mathcal{O}}$ since the dimension

of the ordinary part of $S_{12}(\Gamma_0(11))$ is one (see Remark 5.2). Let $\tilde{T}$ be the Galois deformation associated to $\mathcal{F}$. This $\tilde{T}$ is the Hida deformation which specializes at weight 2 to the p -Tate module $T_p E$ of the modular elliptic curve $E = X_0(11)$. We will show that $\text{Sel}(\mathbb{Q}, \tilde{A})$ is zero.

It is easy to check that $E = X_0(11)$ satisfies the assumption of Corollary 5.9. Hence, by using Nakayama's lemma, we see that

$$\text{Sel}(\mathbb{Q}, A) = 0 \iff \text{Sel}(\mathbb{Q}, \tilde{A}) = 0,$$

where $A = E[p^\infty]$. Let us recall the following result:

Proposition 5.10 (Greenberg, [Gr3] p20). *Let E be an elliptic curve over $\mathbb{Q}$ with split multiplicative reduction at p . We denote the discrete $G_{\mathbb{Q}}$ -module $E[p^\infty]$ by A . Then the classical Selmer group $\text{Sel}(E/\mathbb{Q})\{p\}$ and the strict Selmer group $\text{Sel}^{\text{str}}(\mathbb{Q}, A)$ are isomorphic to each other.*

By using Kolyvagin's Euler system method, the 11-primary part $\text{Sel}(X_0(11)/\mathbb{Q})\{11\}$ of the classical Selmer group for $E = X_0(11)$ is known to be zero. Hence the strict Selmer group $\text{Sel}^{\text{str}}(\mathbb{Q}, A)$ is also zero by Proposition 5.10. Next, we compare $\text{Sel}^{\text{str}}(\mathbb{Q}, A)$ and $\text{Sel}(\mathbb{Q}, A)$. Let us consider the following diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Sel}^{\text{str}}(\mathbb{Q}, A) & \longrightarrow & H^1(\mathbb{Q}_{\Sigma}/\mathbb{Q}, A) & \longrightarrow & \frac{H^1(D_p, A)}{\text{Im}(H^1(D_p, F^+ A))} \\ & & v \downarrow & & \parallel & & \downarrow v' \\ 0 & \longrightarrow & \text{Sel}(\mathbb{Q}, A) & \longrightarrow & H^1(\mathbb{Q}_{\Sigma}/\mathbb{Q}, A) & \longrightarrow & \frac{H^1(I_p, A)}{\text{Im}(H^1(I_p, F^+ A))}, \end{array}$$

where $\text{Im}(H^1(D_p, F^+ A))$ (resp. $\text{Im}(H^1(I_p, F^+ A))$) is the image of $H^1(D_p, F^+ A)$ (resp. $H^1(I_p, F^+ A)$) under the long exact sequence:

$$\cdots \longrightarrow H^1(D_p, F^+ A) \longrightarrow H^1(D_p, A) \longrightarrow H^1(D_p, A/F^+ A) \longrightarrow \cdots$$

$$(\text{resp. } \cdots \longrightarrow H^1(I_p, F^+ A) \longrightarrow H^1(I_p, A) \longrightarrow H^1(I_p, A/F^+ A) \longrightarrow \cdots).$$

In the above diagram, the cokernel of the map v is a sub-quotient of the kernel of the map v' . We have the following diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Im}(H^1(D_p, F^+ A)) & \longrightarrow & H^1(D_p, A) & \longrightarrow & \frac{H^1(D_p, A)}{\text{Im}(H^1(D_p, F^+ A))} \longrightarrow 0 \\ & & \downarrow & & \downarrow v'' & & \downarrow v' \\ 0 & \longrightarrow & \text{Im}(H^1(I_p, F^+ A)) & \longrightarrow & H^1(I_p, A) & \longrightarrow & \frac{H^1(I_p, A)}{\text{Im}(H^1(I_p, F^+ A))} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & & 0 & & 0 \end{array}$$

The module $\text{Ker}(v'')$ is isomorphic to $H^1(D_p/I_p, A^{I_p}) \cong \mathbb{Z}_p/n_{E,p}\mathbb{Z}_p$, where $n_{E,p}$ is the number of the components of the special fiber of the Neron model $\mathcal{E}_p$ of E over $\mathbb{Z}_p$. This module $\text{Ker}(v'')$ is zero since $n_{E,p}$ is a p -adic unit for $E = X_0(11)$ and $p = 11$. Hence $\text{Ker}(v'')$ and $\text{Coker}(v)$ are zero. In conclusion, the Selmer group $\text{Sel}(\mathbb{Q}, \tilde{A})$ is zero.

Thus we calculated the Selmer group for a Hida deformation in purely algebraic way. In a forthcoming paper, we will present a number of algebraic properties of the Selmer groups of the Hida deformation and give more examples.

REFERENCES

- [Ca] H. Carayol, *Sur les représentations l -adiques associées aux formes modulaires de Hilbert*, Ann. Sci. Ecole Norm. Sup. (4) **19**, no. 3, 409–468, 1986.
- [CG] J. Coates, R. Greenberg, *Bummer theory for abelian varieties over local fields*, Invent. Math. **124**, no. 1-3, 129–174, 1996.
- [Da] A. Dabrowski, *On the symmetric power of an elliptic curve*, Algebraic K -theory, 59–82, Contemp. Math., **199**, Amer. Math. Soc., Providence, RI, 1996.
- [De1] P. Deligne, *Formes modulaires et représentations l -adiques*, Séminaires Bourbaki **355**, 139–172, Lecture notes in Math., **179**, Springer Verlag, 1969.
- [De2] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, Automorphic forms, representations and L -functions, Proc. Sympos. Pure Math., XXXIII Part 2, Amer. Math. Soc., Providence, R.I., 247–289, 1979.
- [Gr1] R. Greenberg, *Iwasawa theory for p -adic representations*, Advanced studies in Pure Math. **17**, 97–137, 1987.
- [Gr2] R. Greenberg, *Iwasawa theory for p -adic deformations of motives*, Proceedings of Symposia in Pure Math. **55** Part 2, 193–223, 1994.
- [Gr3] R. Greenberg, *Iwasawa theory for elliptic curves*, preprint, 1998.
- [Gro] B. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. Jour. **61**, 445–517, 1990.
- [H1] H. Hida, *Iwasawa modules attached to congruences of cusp forms*, Ann. Sci. Ecole Normal. sup., **19**, 231–273, 1986.
- [H2] H. Hida, *Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms*, Invent. Math. **85**, 545–613, 1986.
- [H3] H. Hida, *On Selmer Groups of Adjoint Galois Representations*, Séminaire de Théorie des Nombres de Paris, 1993–1994, London Mathematical Society Lecture Note Series **235**, 89–132, Cambridge University Press, 1996.
- [H4] H. Hida, *Elementary theory of L -functions and Eisenstein series*, London Mathematical Society Student Texts **26**, Cambridge University Press, 1993.
- [K1] K. Kato, *Series of lectures on Iwasawa main conjectures for modular elliptic curves*, at Tokyo University, September, 1998.
- [K2] K. Kato, *p -adic Hodge theory and values of zeta functions of modular forms*, preprint, 1998.
- [M] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math., **18**, 183–266, 1972.
- [MT] B. Mazur, J. Tilouine, *Représentations galoisiennes, différentielles de Kähler et "conjectures principales"*, Inst. Hautes Etudes Sci. Publ. Math. **71**, 65–103, 1990.
- [MW] B. Mazur, A. Wiles, *On p -adic analytic families of Galois representations*, Compositio Math. **59**, no. 2, 231–264, 1986.
- [Og] A. Ogg *On the eigenvalues of Hecke operators*, Math. Ann. **179** 101–108, 1969.
- [R1] K. Ribet, *Galois representations attached to eigenforms with Nebentypus*, Modular functions of one variable, V 17–51. Lecture Notes in Math., **601**, Springer, 1977.
- [R2] K. Ribet, *On l -adic representations attached to modular forms. II*, Glasgow Math. Jour. **27**, 185–194, 1985.
- [Ti] J. Tilouine, *Un sous-groupe p -divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algèbre de Hecke*, Bull. Soc. Math. France **115**, no. 3, 329–360, 1987.
- [Wa] L. Washington, *Introduction to cyclotomic fields (2nd edition)*, Graduate texts in Mathematics **83**, Springer, 1996.
- [Wi] A. Wiles, *On λ -adic representations associated to modular forms*, Invent. Math. **94**, 529–573, 1988.

GRADUATE SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY OF TOKYO, 3-8-1, KOMABA, MEGURO-KU, TOKYO-TO, JAPAN, 153-8914.

E-mail address: `ochiai@ms.u-tokyo.ac.jp`