Introduction to non-commutative Iwasawa theory (I)–(IV)

Yoshitaka Hachimori (Keio University)

February 20, 2007
Revised on August 4, 2014 [1]

These notes are reports on a series of lectures given by John H. Coates and Yoshitaka Hachimori in UK-Japan Winter School 2007 held in Cambridge from January 7 to 10, 2007. This Winter School was organized by 21st Century COE Program of Keio University in cooperation with Centre for Mathematical Sciences, University of Cambridge.

In the lectures (I) and (III), John Coates discussed the arithmetic of Selmer groups of elliptic curves. In (II) and (IV), Hachimori reviewed some ring-theorertic properties of Iwasawa algebras and a formulation of the main conjecture.

(On August 4, 2014)
I revised the note on the lecture (II). I changed the definition of filtration on the ring A correctly, so that the filtration becomes a Zariskian filtration.

[1] revised on August 4, 2014

Introduction to non-commutative Iwasawa theory (I)

A lecture given by John H. Coates (Cambridge)

In this talk, what Iwasawa theory concerns about was briefly explained at the beginning and a bunch of interesting numerical examples were given. Then, a conjecture on complex L-functions coming out of non-commutative Iwasawa theory was mentioned. At the last part, some facts on Selmer groups were reviewed.

The following is based on a (handwritten) note prepared for this talk by John Coates himself.

By a p-adic Lie extension F_∞ of $\mathbb{Q}$, we mean a Galois extension of $\mathbb{Q}$, whose Galois group G is a p-adic Lie group. Roughly speaking, non-commutative Iwasawa theory can be defined as the study of the arithmetic behavior of motives over all extensions of $\mathbb{Q}$ contained in F_∞. It has three key ingredients. We recall that the Iwasawa algebra $\Lambda(G)$ is defined by

$$\Lambda(G) = \varprojlim_U \mathbb{Z}_p[G/U],$$

where U runs over all open normal subgroups of G. The three ingredients are:

(i) Purely algebraic questions about modules over $\Lambda(G)$.
(ii) Algebraic study of the specific $\Lambda(G)$-modules (dual of Selmer groups) which control the arithmetic.
(iii) Precise relationship of these arithmetic modules to special values of complex L-functions (Main conjecture, ...).

Classical Iwasawa theory is concerned with the case $F_\infty = \mathbb{Q}(\mu_{p^\infty})$ (μ_{p^∞} = the group of all p-power roots of unity) when $G = \mathbb{Z}_p^\times$ is abelian. Our four lectures will give a very brief introduction to the non-commutative theory. For simplicity, we shall take our motive always to be an elliptic curve E over $\mathbb{Q}$. We shall mainly consider the false Tate curve case where

$$F_\infty = \mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{m})$$

where m is an integer > 1, which is p-power free (if $p > 2$). Here $G = \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ is a semi-direct product.

We quickly recall the definition of the Selmer group $\mathcal{S}(E/L)$ for any field $L \subset \overline{\mathbb{Q}}$. E_{p^∞} denotes the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module of all p-power division points on E.

Definition.

$$\mathcal{S}(E/L) = \ker(H^1(L, E_{p^\infty}) \to \prod_w H^1(L_w, E(\overline{L}_w))(p)),$$

$$X(E/L) = \mathrm{Hom}(\mathcal{S}, \mathbb{Q}_p/\mathbb{Z}_p).$$

Here, $*(p)$ means the p-part of $*$.

Remarks. (i) We always have the exact sequence

$$0 \to E(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathcal{S}(E/L) \to Ш(E/L) \to 0.$$

(ii) If L is Galois over $\mathbb{Q}$, $\mathrm{Gal}(L/\mathbb{Q})$ has a natural action on $\mathcal{S}(E/L)$ and $X(E/L)$ (fundamental for Iwasawa theory).

Basic Fact. If $[L:\mathbb{Q}]<\infty$, $X(E/L)$ is always a finitely generated $\mathbb{Z}_p$-module.

This follows from well known arguments in Galois cohomology.

Definition. $t_{E/L}=\mathbb{Z}_p$-rank of $X(E/L)$ and $g_{E/L}=\mathbb{Z}$-rank of $E(L)$.

So $g_{E/L}\leq t_{E/L}$ and the equality holds if and only if $Ш(E/L)(p)$ is finite.

Notation. $p>2$ and $K_\infty=\mathbb{Q}(\mu_{p^\infty})$.

Numerical examples are important in all parts of number theory, and especially Iwasawa theory!

Numerical Example.

$E=X_1(11)$ is the first elliptic curve in nature.

$$E: y^2+y=x^3-x^2,\ \ N_E=11.$$

E has good reduction at all $p\neq 11$, split multiplicative at 11. $p=19$ is the first supersunguler odd prime for E. What do we know about the global arithmetic of E?

Theorem. *$\mathcal{S}(E/\mathbb{Q})=0$ for all odd prime p.*

Theorem (Kato)**.** *Assume p is not supersingular for E. Then $Y(E/K_\infty):=X(E/K_\infty)/X(E/K_\infty)(p)$ is a finitely generated $\mathbb{Z}_p$-module.*

Conjecture. *Assume p is not supersingular for E. Then $X(E/K_\infty)(p)$ is finite. It is equivalent to $X(E/K_\infty)(p)=0$ by a theorem of Matsuno.*

Here is some numerical evidence in support of this conjecture:–
(i) $p=3$, $X(E/K_\infty)=0$.
(ii) $p=5$, $X(E/K_\infty)=0$.
(iii) $p=7$, $X(E/K_\infty)\cong\mathbb{Z}_7$. $E(\mathbb{Q}(\mu_7))$ has the point of infinite order $(1+z,-z)$, $z=\zeta+\zeta^2+\zeta^4$, $\zeta^7=1$, $\zeta\neq 1$.
(iv) $p=11$, $X(E/K_\infty)$ has $\mathbb{Z}_p$-rank ≥ 1.

What happens when we pass to non-abelian p-adic Lie extensions? In general, we can have "many more points". Here are two examples. (Still $E=X_1(11)$.)

Case 1. $p=7$, $L_n=\mathbb{Q}(\sqrt[7^n]{m})$, $F_n=\mathbb{Q}(\mu_{7^n},\sqrt[7^n]{m})$.
(i) (V. Dokchitser and T. Dokchitser). For all 7-power free m, we have $t_{E/L_n}\geq n$ and $t_{E/F_n}\geq 7^n$ $(n=1,2,\cdots)$.
(ii) (CFKS). If m is divisible only by 2, 3, 7, we have $t_{E/L_n}=n$ and $t_{E/F_n}=7^n$ $(n=1,2,\cdots)$.
No point of infinite order has been found in L_1 for a single m!

Case 2. $p=11$, $F_n=\mathbb{Q}(E_{11^n})$.
(Delaunnay and Wuthrich). $g_{E/F_n}\geq 3\cdot 11^n+3\cdot 11^{n-1}-3$ $(n=1,2,\cdots)$.

We end this introduction by discussing a curious consequence for complex L-functions which emerges from p-adic Iwasawa theory. We return to a general elliptic curve E over $\mathbb{Q}$. Let $L(E,s)$ be the complex L-function of $E/\mathbb{Q}$. For $\rho: G\to GL(V_\rho)$, an Artin representation of G, let $L(E,\rho,s)$ be the complex L-function attached to $H^1_l(E)_{\mathbb{C}}\otimes_{\mathbb{C}}V_\rho$. When $G=\mathrm{Gal}(F_\infty/\mathbb{Q})$, $F_\infty=\mathbb{Q}(\mu_{p^\infty},\sqrt[p^\infty]{m})$,

G has infinitely many irreducible self-dual Artin representations ρ. We are interested in $\mathrm{ord}_{s=1}(L(E,\rho,s))$ as ρ runs over the set $\mathcal{T}$ of irreducible self-dual Artin representations of G.

Let $H = \mathrm{Gal}(F_\infty/K_\infty)$ $(\subset G)$. By the action of H, $\Lambda(H)$ acts continuously on $X(E/F_\infty)$. We assume the following.

Assumption: E has good ordinary reduction at p.

Conjecture. *$Y(E/F_\infty) := X(E/F_\infty)/X(E/F_\infty)(p)$ is finitely generated over $\Lambda(H)$.*

This is known to be true in many cases. Also $H \cong \mathbb{Z}_p$, and so $\Lambda(H) \cong \mathbb{Z}_p[[T]]$.

Definition. $\nu(E/F_\infty) = \Lambda(H)$-rank of $Y(E/F_\infty)$.

We can usually compute $\nu(E/F_\infty)$ with a simple explicit formula (see the lecture (III)).

Conjecture. *Assume E has good ordinary reduction at p, and that $Y(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module. Then*

$$\mathrm{ord}_{s=1}(L(E,\rho,s)) \leq \nu(E/F_\infty)\frac{p}{p-1}$$

for all ρ in $\mathcal{T}$.

BSD would be false if this conjecture failed! From the complex viewpoint this seems an unexpected result because $\mathcal{T}$ is infinite.

Study of $X(E/F_\infty)$ in the false Tate curve case

We assume always now that $p > 2$ and that E has good ordinary reduction at p. Denote $K_\infty = \mathbb{Q}(\mu_{p^\infty})$, $F_\infty = \mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{m})$, $G = \mathrm{Gal}(F_\infty/\mathbb{Q})$ and $H = \mathrm{Gal}(F_\infty/K_\infty)$. Put

$$Y(E/F_\infty) = X(E/F_\infty)/X(E/F_\infty)(p), Y(E/K_\infty) = X(E/K_\infty)/X(E/K_\infty)(p).$$

We investigate the structure of $X(E/F_\infty)$ and $Y(E/F_\infty)$ as $\Lambda(H)$-modules. Here are some steps towards underestanding these modules.

Step 1 (done by Kato). Prove that $Y(E/K_\infty)$ is a finitely generated $\mathbb{Z}_p$-module.

Step 2. Relate $X(E/F_\infty)_H$ to $X(E/K_\infty)$ and use Nakayama's Lemma.

Step 3. Show how to find $\nu(E/F_\infty) = \mathrm{rank}_{\Lambda(H)} Y(E/F_\infty)$.

We will concentrate on Steps 2 and 3 (continued to the lecture (III)).

Relationship of Selmer to cohomology groups with restricted ramification.

Before begining to study $X(E/F_\infty)$, we review some properties of Selmer groups briefly. E_{p^∞} denotes the group of all p-power division points on E. S is a finite set of primes containing p and all primes where E has bad reduction.

Lemma (Key Lemma)**.** *The extension $\mathbb{Q}(E_{p^\infty})/\mathbb{Q}$ is unramified outside S and the prime at ∞.*

Two key facts enable us to relate $\mathcal{S}(E/\mathbb{Q})$ to Galois cohomology with restricted ramification:–

Fact 1. If $q \neq p$, $E(\mathbb{Q}_q) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$.

Fact 2. $H^1(G(\mathbb{Q}_q^{\mathrm{nr}}/\mathbb{Q}_q), E(\mathbb{Q}_q^{\mathrm{nr}})) = 0$ if E has good reduction at q, where $\mathbb{Q}_q^{\mathrm{nr}}$ is the maximal unramified extension of $\mathbb{Q}_q$.

Definition. $\mathbb{Q}_S$ denotes the maximal extension of $\mathbb{Q}$ unramified outside primes in S and ∞. Let $G_S(\mathbb{Q}) := \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ and $G_S(L) := \mathrm{Gal}(\mathbb{Q}_S/L)$ for any subextension L in $\mathbb{Q}_S/\mathbb{Q}$.

We remark that no simple description of $\mathbb{Q}_S$ is known! However, $\mathbb{Q}_S \supset \mathbb{Q}(\mu_{p^\infty}) = K_\infty$ and $\mathbb{Q}_S \supset F_\infty$, provided S contains all prime divisors of m. We have the following second key lemma. Let W be a discrete $G_S(\mathbb{Q})$-module such that $W = (\mathbb{Q}_p/\mathbb{Z}_p)^r$ as an abelian group, e.g., $W = E_{p^\infty}$.

Lemma (Key Lemma)**.** *$H^1(G_S(\mathbb{Q}), W)$ is a cofinitely generated $\mathbb{Z}_p$-module.*

By definition, $\mathcal{S}(E/\mathbb{Q}) \subset H^1(\mathbb{Q}, E_{p^\infty}) \supset H^1(G_S(\mathbb{Q}), E_{p^\infty})$. How can we relate these two subgroups? We have the localization map

$$\lambda_q : H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E_{p^\infty}) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q), E(\overline{\mathbb{Q}}_q)).$$

Lemma. $H^1(G_S(\mathbb{Q}), E_{p^\infty}) = \cap_{q \notin S} \mathrm{Ker}(\lambda_q)$.

Corollary. $\mathcal{S}(E/\mathbb{Q}) = \ker(H^1(G_S(\mathbb{Q}), E_{p^\infty}) \to \bigoplus_{q \in S} H^1(\mathbb{Q}_q, E(\overline{\mathbb{Q}}_q))(p))$.

Corollary. *$\mathcal{S}(E/\mathbb{Q})$ is a cofinitely generated $\mathbb{Z}_p$-module.*

Introduction to non-commutative Iwasawa theory (II)

Yoshitaka Hachimori (Keio University)

In this talk, I reviewed some basic (ring-theoretic) properties of Iwasawa algebras first, and then introduced specific multiplicative closed sets of Iwasawa algebras which is needed for a formulation of the main conjecture.

1. Basic properties of Iwasawa algebras

Our situation is as follows: Let p be an odd prime number and m an integer > 1. Put $K_n = \mathbb{Q}(\mu_{p^n})$, $K_\infty = \mathbb{Q}(\mu_{p^\infty})$, $F_n = K_n(\sqrt[p^n]{m})$, and $F_\infty = K_\infty(\sqrt[p^\infty]{m})$. Denote $\mathrm{Gal}(F_\infty/\mathbb{Q})$, $\mathrm{Gal}(F_\infty/K_1)$ and $\mathrm{Gal}(F_\infty/K_\infty)$ by G, G_0 and H respectively. For $n \geq 1$, denote $\mathrm{Gal}(F_n/\mathbb{Q})$ and $\mathrm{Gal}(F_n/K_1)$ by G_n and $G_{0,n}$. Then $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ and $G_0 \cong \mathbb{Z}_p \rtimes (1+p\mathbb{Z}_p)$. G_0 is a pro-p open subgroup of G with $G/G_0 \cong (\mathbb{Z}/p)^\times$. G_0 is topologically generated by two elements, say, γ_1 and γ_2 with one relation: $\gamma_2\gamma_1 = \gamma_1^\varepsilon\gamma_2$ for some $\varepsilon \in 1+p\mathbb{Z}_p$. The Iwasawa algebra $\Lambda(G)$ of G is $\varprojlim_n \mathbb{Z}_p[G_n]$ and $\Lambda(G_0)$ is $\varprojlim_n \mathbb{Z}_p[G_{0,n}]$.

These $\Lambda(G)$ and $\Lambda(G_0)$ have the following properties. Both are left and right Noetherian, have finite global dimensions and satisfy the left and right Auslander condition. Further, $\Lambda(G_0)$ is a scaler local ring and has no non-zero zero-divisor. Here, the left Auslander condition for a ring A means the following (cf. [Ve1] Definition 3.3): For any left A-module M, any integer i and any right A-submodule $N \subset \mathrm{Ext}^i_A(M, A)$, $\mathrm{Ext}^j_A(N, A)$ vanishes for all $j < i$. We say that a ring is Auslander regular if it has a finite global dimension and satisfies the Auslander condition.

In this section, we will see which method enables us to deduce the above properties. We first focus on $\Lambda(G_0)$. To see how this ring looks like, we introduce a skew power series ring (cf. [Ve2]). Denote the one variable power series ring $\mathbb{Z}_p[[X]]$ by R. Let σ be the continuous ring automorphism on R defined by $\sigma(X) = (1+X)^\varepsilon - 1$. Put $\delta := \sigma - \mathrm{id}$. The skew power series ring $A := R[[Y; \sigma, \delta]]$ is defined as follows: The underlying set is just the set of all formal power series over R in a variable Y (hence two variable power series over $\mathbb{Z}_p$). Namely, elements in A are of the form $\sum_{n=0}^\infty r_n Y^n$ where r_n are in R. The addition rule is the usual one, but the multiplication rule is twisted as follows: We define the right multiplication of Y by $r \in R$ by the formula $Yr = \sigma(r)Y + \delta(r)$. Extending this rule in a natural way, we define the multiplication of two elements in A. Here, we need the convergence for well-defindness. This follows from the fact that $\delta((p, X)^n) \subset (p, X)^{n+1}$ where (p, X) is the maximal ideal of R.

It is not difficult to show that A is a scaler local ring with the maximal ideal $\mathfrak{m} = (p, X, Y)$. The residue field is $\mathbb{F}_p$. Looking at the relation $(1+Y)(1+X) = (1+X)^\varepsilon(1+Y)$, we can readily imagine that A is identified with $\Lambda(G_0)$. In fact, we have the isomorphisms

$$A \xrightarrow{\sim} \varprojlim_n A/((1+X)^{p^{n-1}} - 1, (1+Y)^{p^n} - 1) \xleftarrow{\sim} \varprojlim_n \mathbb{Z}_p[G_{0,n}] \ (= \Lambda(G_0)).$$

The second map is induced from $\mathbb{Z}_p[G_{0,n}] \xrightarrow{\sim} A/((1+X)^{p^{n-1}}-1, (1+Y)^{p^n}-1)$, defined by sending (the image of) γ_1 to $X+1$ and γ_2 to $Y+1$. We need the Weierstrass preparation theorem ([Ve2] Theorem 3.1) for this isomorphism.

Next, we give an ascending filtration of two sided ideals on A. Put $\Sigma_n = A$ for $n \geq 0$, $\Sigma_{-2k} := \sum_{i=0}^{k} p^i \mathfrak{m}^{2(k-i)}$ and $\Sigma_{-2k-1} := \sum_{i=0}^{k} p^i \mathfrak{m}^{2(k-i)+1}$ for $k \geq 0$. We can endow the graded module $\mathrm{gr}(A) := \bigoplus_n \Sigma_n/\Sigma_{n-1}$ with a ring structure in a standard way, since $\Sigma_n \Sigma_m \subset \Sigma_{n+m}$. The following is the key to see the properties of A:

Proposition 1.1. $\mathrm{gr}(A)$ *is isomorphic to* $\mathbb{F}_p[x_0, x_1, x_2]$*, the commutative polynomial ring with three variables over* $\mathbb{F}_p$*. Here,* x_0*,* x_1 *and* x_2 *correspond to the classes of* $p \in \Sigma_{-2}/\Sigma_{-3}$*,* X *and* Y *in* Σ_{-1}/Σ_{-2}*.*

Note that the commutativity of $\mathrm{gr}(A)$ is induced from the fact $XY - YX \in \Sigma_{-3}$. We have a general theory on filtered rings. This theory tells us the following (cf. [LO], see also [DdMS] §7.4): (1) If $\mathrm{gr}(A)$ is Noetherian, then so is A. (2) If $\mathrm{gr}(A)$ has no zero-divisor, then so is A. (3) If $\mathrm{gr}(A)$ is Auslander regular, then so is A with $\mathrm{gd}(A) = \mathrm{gd}(\mathrm{gr}(A))$. Here, $\mathrm{gd}(*)$ means the global dimension. (Precisely speaking, we need the fact that $\{\Sigma_n\}$ satisfies the "closure condition". It is easy to verify.) It is quite well known that $\mathbb{F}_p[x_0, x_1, x_2]$ is a Noetherian domain and have the finite global dimension 3. If a commutative ring is regular, then it satisfies the Auslander condition automatically. This is a way to see the properties of A (and hence $\Lambda(G_0)$).

As further topics on $\Lambda(G_0)$, we should mention about (1) the Weierstrass preparation theorem ([Ve2]) and (2) the notion of pseudo-null modules ([Ve1]) and the structure theorem of $\Lambda(G_0)$-modules ([CSS]), but we omit these.

$\Lambda(G)$ is a "crossed product" (cf. [MR] 1.5.8) of $\Lambda(G_0)$ and G/G_0, denoted by $\Lambda(G_0) * (G/G_0)$. This is similar as the group ring $\Lambda(G_0)[G/G_0]$, but elements in $\Lambda(G)$ and in G/G_0 do not commute. More precisely, an injective ring homomorphism $\Lambda(G_0) \to \Lambda(G)$ and an injective map $G/G_0 \hookrightarrow \Lambda(G)^\times$ (which is not necessarily a group homomorphism) are given so that the following properties hold: $\Lambda(G)$ is a free left $\Lambda(G_0)$-module with basis G/G_0

$$\Lambda(G) \cong \oplus_{\tau \in G/G_0} \Lambda(G_0)\overline{\tau},$$

where $\overline{\tau}$ denotes the image of $\tau \in G/G_0$ in $\Lambda(G)^\times$. Further, $\overline{\tau}\Lambda(G_0) = \Lambda(G_0)\overline{\tau}$ and $(\Lambda(G_0)\overline{\tau_1})\overline{\tau_2} = \Lambda(G_0)\overline{\tau_1\tau_2}$ hold for any τ and τ_i in G/G_0. Then, for such a ring, the Noetherian property is easy to see. Since the order of G/G_0 is prime to p, we have $\mathrm{gd}(\Lambda(G)) = \mathrm{gd}(\Lambda(G_0))$ (cf. [MR] 7.5.6). We can also show $\Lambda(G)$ satisfies the Auslander condition.

For this section, I refer [AB] as a good survey on the Iwasawa algebras.

2. Ore set and non-commutative localization

$\Lambda(G)$ is the ring as the previous section. Let

$$S := \{s \in \Lambda(G) \mid \Lambda(G)/\Lambda(G)x \text{ is finitely generated as a } \Lambda(H)\text{-module}\}.$$

Identifying $\Lambda(G_0)$ with A, $\Lambda(G)$ is a crossed product $A*(G/G_0)$. So its element x is expressed as $x = \sum_g a_{\overline{g}}\overline{g}$, where $a_{\overline{g}} = \sum_n r_{\overline{g},n}Y^n \in A$. Then, by the Nakayama's lemma, we can see that x is in S if and only if for every $\overline{g} \in G/G_0$ there exists some n such that $r_{\overline{g},n}$ is not contained in the maximal ideal (p, X) of R . Put $S^* := \cup_{n\geq 0}\ p^n S$. We have

Theorem 2.1 ([CFKSV] Theorem 2.4)**.** *S^* is a multiplicatively closed set, contains no zero-divisor, and satisfies the left and right Ore condition.*

Here, the left Ore condition is as follows: For any $s \in S^*$ and $x \in \Lambda(G)$, there exist some $t \in S^*$ and $y \in \Lambda(G)$ satisfying $tx = ys$. We have a nice (noncommutative) localization of $\Lambda(G)$ with respect to S^* (cf. [GW] Chapter 9, [MR] 2.1). There exists a ring $\Lambda(G)_{S^*}$ and a ring homomorphism $\varphi : \Lambda(G) \to \Lambda(G)_{S^*}$ with the following universal property: If $f : \Lambda(G) \to B$ is any ring homomorphism such that $f(S^*) \subset B^\times$, then f factors uniquely through φ. $\Lambda(G)_{S^*}$ is unique up to isomorphisms over $\Lambda(G)$. Such a ring can be constructed in a similar manner as that to construct the localizations of commutative rings because of the Ore condition. We define

$$\Lambda(G)_{S^*} := S^* \times \Lambda(G)/\sim$$

where $\sim$ is a relation on $S^* \times \Lambda(G)$: $(s, x) \sim (s', x')$ if and only if there exist r and r' in $\Lambda(G)$ such that $rs = r's' \in S^*$ and $rx = r'x'$. The left Ore condition assures that this is an equivalence relation. The condition also enables us to define addition and multiplication rules on the set $S^* \times \Lambda(G)/\sim$ suitably. The class of (s, x) is written as $s^{-1}x$. $\Lambda(G)_{S^*}$ is flat as a left (and right) $\Lambda(G)$-module.

This $\Lambda(G)_{S^*}$ plays an important role in the formulation of the main conjecture.

References

[AB] K. Ardakov and K. A. Brown, *"Ring-Theoretic Properties of Iwasawa Algebras: A Survey"*, Documenta Math., Extra Volume: John H. Coates' Sixtieth Birthday (2006), 7–33.

[CFKSV] J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob, *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. IHES **101** (2005), 163–208.

[CSS] J. Coates, P. Schneider and R. Sujatha, *Modules over Iwasawa algebras*, J. Inst. Math. Jussieu **2** (2003), 73–108.

[DdMS] J. Dixon, M. du Sautoy, A. Mann and D. Segal, *Analytic pro-p groups*, second edition, Cambridge Studies in Advanced Mathematics 61, Cambridge University Press (1999).

[GW] K. Goodearl and R. Warfield *An introduction to noncommutative Noetherian rings*, LMS Student Texts 16, Cambridge University Press (1989).

[LO] H. Li and F. van Oystaeyen, *Zariskian filtrations*, K-Monographs in Mathematics 2, Kluwer Academic Publishers, (1996).

[MR] J. C. McConnell and J. C. Robson, *Noncommutative Noetherian Rings*, Wiley series in pure and applied mathematics, A Wiley-Interscience Publications (1988).

[Ve1] O. Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, J. Eur. Math. Soc. **4** (2002), 271–311.

[Ve2] O. Venjakob, *A noncommutative Weierstrass preparation theorem and applications to Iwasawa theory*, with an appendix by D. Vogel, J. Reine angew. Math. **559** (2003), 153–191.

E-mail: `yhachi@math.keio.ac.jp`

Introduction to non-commutative Iwasawa theory (III)

A lecture given by John H. Coates (Cambridge)

In this talk, continued from the lecture (I), a basic fact on the Selmer groups over $\mathbb{Q}$ was reviewed first. Then a fundamental commutative diagram in Iwasawa theory was introduced. The main topic of this talk was the $\Lambda(H)$-rank of the Pontrjagin dual of the Selmer group $X(E/F_\infty)$.

This report is written by Yoshitaka Hachimori, based on the notes taken by Kazuo Matsuno and Yasuko Hasegawa. He thanks for their cooperations.

Let $E/\mathbb{Q}$ be an elliptic curve. Take a prime number $p \neq 2$. E_{p^∞} is a basic module of p-power division points of E. Denote by S a finite set of primes containing p and primes of bad reduction. $\mathbb{Q}_S$ is the maximal extension of $\mathbb{Q}$ unramified outside S and $G_S(\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$. For a prime q, let

$$\lambda_q : H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E_{p^\infty}) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q), E(\overline{\mathbb{Q}}_q)).$$

$H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E_{p^\infty})$ contains the Selmer group $\mathcal{S}(E/\mathbb{Q})$ and $H^1(G_S(\mathbb{Q}), E_{p^\infty})$ as subgroups.

Lemma. $H^1(G_S(\mathbb{Q}), E_{p^\infty}) = \cap_{q \notin S} \mathrm{Ker}(\lambda_q)$.

This is based on the facts $E(\mathbb{Q}_q) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ and $H^1(G(\mathbb{Q}_q^{\mathrm{nr}}/\mathbb{Q}_q), E(\mathbb{Q}_q^{\mathrm{nr}})) = 0$ for $q \notin S$.

Corollary. *The following is exact:*

$$0 \to \mathcal{S}(E/\mathbb{Q}) \to H^1(G_S(\mathbb{Q}), E_{p^\infty}) \overset{\lambda_{S,\mathbb{Q}}}{\to} \bigoplus_{q \in S} H^1(\mathbb{Q}_q, E(\overline{\mathbb{Q}}_q)).$$

As in the previous talks, $K_\infty = \mathbb{Q}(\mu_{p^\infty})$ and $F_\infty = \mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{m})$ with some integer m. Assume that every prime factor of m is in S. Now we see the "Step 2" of the lecture (I) in detail. S^{cyc} denotes the set of all places v of K_∞ dividing some q in S. We have an exact sequence

$$0 \to \mathcal{S}(E/K_\infty) \to H^1(G_S(K_\infty), E_{p^\infty}) \overset{\lambda_{S,K_\infty}}{\to} \bigoplus_{v \in S^{\mathrm{cyc}}} H^1(K_{\infty,v}, E)(p).$$

For a finite extension L/K_∞ and for $v \in S^{\mathrm{cyc}}$, put $J_v(L) = \bigoplus_{w|v} H^1(L_w, E)(p)$. We set $J_v(F_\infty) := \varinjlim_L J_v(L)$ where L runs over all finite subextensions of F_∞/K_∞. The map λ_{S,F_∞} is defined similarly as λ_{S,K_∞} by replacing K_∞ with F_∞. Then we have the following fundamental commutative diagram:

$$\begin{array}{ccccc} 0 \longrightarrow \mathcal{S}(E/F_\infty)^H & \longrightarrow & H^1(G_S(F_\infty), E_{p^\infty})^H & \xrightarrow{\varphi} & \bigoplus_{v \in S^{\mathrm{cyc}}} J_v(F_\infty)^H \\ \uparrow \alpha & & \uparrow \beta & & \uparrow \gamma = \oplus \gamma_v \\ 0 \longrightarrow \mathcal{S}(E/K_\infty) & \longrightarrow & H^1(G_S(K_\infty), E_{p^\infty}) & \xrightarrow{\lambda_{S,K_\infty}} & \bigoplus_{v \in S^{cyc}} H^1(K_{\infty,v}, E)(p). \end{array}$$

Here, $H := \mathrm{Gal}(F_\infty/K_\infty)$ and φ is the map induced from λ_{S,F_∞}.

Proposition. $\ker\ \alpha$ *and* $\mathrm{coker}\ \alpha$ *are always cofinitely generated* $\mathbb{Z}_p$*-modules.*

Since $H \cong \mathbb{Z}_p$, β and γ are surjective. Hence,

$$0 \to \ker \alpha \to \ker \beta \to \mathrm{Im}(\lambda_{S,K_\infty}) \cap \ker \gamma \to \mathrm{coker}\ \alpha \to 0$$

is exact. We have $\ker \beta \cong H^1(H, E_{p^\infty}(F_\infty))$. This group is finite because of the fact that $E_{p^\infty}(K_\infty)$ is always finite and the exact sequence

$$0 \to E_{p^\infty}(K_\infty) \to E_{p^\infty}(F_\infty) \overset{h-1}{\to} E_{p^\infty}(F_\infty) \to H^1(H, E_{p^\infty}(F_\infty)) \to 0.$$

Here h is a topological generator of H. Since S^{cyc} is finite, $\ker \gamma$ is also a finitely generated as a $\mathbb{Z}_p$-module. The proposition follow from these.

For any extension $L/\mathbb{Q}$, denote $X(E/L) := \mathrm{Hom}(\mathcal{S}(E/L), \mathbb{Q}_p/\mathbb{Z}_p)$. Recall $\Lambda(H) \cong \mathbb{Z}_p[[T]]$. By looking at $\hat{\alpha} : X(E/F_\infty)_H \to X(E/K_\infty)$, the dual of α and the proposition, we have

Corollary. *$X(E/F_\infty)$ is finitely generated over $\Lambda(H)$ if and only if $X(E/K_\infty)$ is a finitely generated $\mathbb{Z}_p$-module.*

If E has potentially supersingular reduction at p, then $X(E/K_\infty)$ is never finitely generated $\mathbb{Z}_p$-module. Thus, from now on, we make the following assumption.

Assumption: E has good ordinary reduction at p.

Kato showed that $Y(E/K_\infty) = X(E/K_\infty)/X(E/K_\infty)(p)$ is a finitely generated $\mathbb{Z}_p$-module under this assumption.

We go to the "Step 3" in the lecture (I). We investigate the $\Lambda(H)$-rank of $Y(E/F_\infty) = X(E/F_\infty)/X(E/F_\infty)(p)$ (under the assumption E has good ordinary reduction at p). $Y(E/F_\infty)$ is finitely generated as a $\Lambda(H)$-module if and only if

$$\mu_{G_0}(X(E/F_\infty)) = \mu_\Gamma(X(E/K_\infty)).$$

Here, $G_0 = \mathrm{Gal}(F_\infty/\mathbb{Q}(\mu_p))$ and $\Gamma = \mathrm{Gal}(K_\infty/\mathbb{Q}(\mu_p))$. $\mu_{G_0}(M)$ (resp. $\mu_\Gamma(N)$) is the μ-invariant of a $\Lambda(G_0)$-module M (resp. $\Lambda(\Gamma)$-module N).

Proposition. *For a finitely generated $\Lambda(H)$-module M,*

$$\mathrm{rank}_{\Lambda(H)}(M) = \mathrm{rank}_{\mathbb{Z}_p} H_0(H, M) - \mathrm{rank}_{\mathbb{Z}_p} H_1(H, M).$$

We apply this to $M = Y(E/F_\infty)$. The assumption that $X(E/F_\infty)$ is finitely generated over $\Lambda(H)$ is stronger. Here, we do not assume this. We first have

Proposition. $H_1(H, X(E/F_\infty)) = 0$.

To prove this, we need the following:

Proposition. *λ_{S,K_∞} and λ_{S,F_∞} are both surjective. Both $H^2(G_S(K_\infty), E_{p^\infty})$ and $H^2(G_S(F_\infty), E_{p^\infty})$ vanish.*

It is not in general true that $\lambda_{S,\mathbb{Q}}$ is surjective. The proof uses the fact that $X(E/K_\infty)$ is $\Lambda(\Gamma)$-torsion by Kato. We can deduce that $X(E/F_\infty)$ is $\Lambda(G_0)$-torsion. By this proposition, φ is surjective because γ is surjective. This enables us to prove the previous proposition.

Lemma (Local Lemma)**.** $\ker \gamma_v$ *is finite except the following cases:*
(i) *If* $v|m$ *and* E *has split multiplicative reduction at* v*, then* $\mathrm{corank}_{\mathbb{Z}_p}(\ker \gamma_v) = 1$.
(ii) *If* $v|m$*,* $v \not| p$*,* E *has good reduction at* v *and* $\tilde{E}_v(\kappa_{\infty,v})(p) \neq 0$*, then we have* $\mathrm{corank}_{\mathbb{Z}_p}(\ker \gamma_v) = 2$.

Finally we have the following:

Formula. If $Y(E/F_\infty)$ is finitely generated over $\Lambda(H)$, then

$$\mathrm{rank}_{\Lambda(H)} Y(E/F_\infty) = \lambda + r + 2s$$

where λ is the $\mathbb{Z}_p$-rank of $Y(E/K_\infty)$, r is the number of v of K_∞ of type (i) in the lemma and s is the number of v of K_∞ of type (ii).

Examples. Let $E = X_1(11)$, and $p = 7$. Then $X(E/K_\infty) \cong \mathbb{Z}_p$ and $\lambda = 1$. If $m = 7$, then $\mathrm{rank}_{\Lambda(H)} X(E/F_\infty) = 1$. If m is divisible only by 2, 3 and 7, $\mathrm{rank}_{\Lambda(H)} X(E/F_\infty) = 1$. If $m = 5$, $\mathrm{rank}_{\Lambda(H)} X(E/F_\infty) = 3$. If $m = 11$, $\mathrm{rank}_{\Lambda(H)} X(E/F_\infty) = 4$.

At the end of the talk, the following theorem which relates the $\Lambda(H)$-rank with the root numbers was mentioned:

Theorem. *The* $\Lambda(H)$*-rank of* $Y(E/F_\infty)$ *is odd if and only if the root number* $w(E, \rho) = -1$ *for all irreducible self-dual Artin representation* ρ *of* $G = G(F_\infty/\mathbb{Q})$ *with* $\dim \rho > 1$.

Introduction to non-commutative Iwasawa theory (IV)

Yoshitaka Hachimori (Keio University)

In this talk, I first gave a formulation of the main conjecture in non-commutative Iwasawa theory according to [CFKSV]. Then I discussed how the p-adic L-function should be characterized. At the end of the talk, I introduced one of Zábrádi's remarkable results.

1. Main conjecture

The situation is the same as the one in the previous talks. Let p be an odd prime number and m an integer. Put $K_n = \mathbb{Q}(\mu_{p^n})$, $K_\infty = \mathbb{Q}(\mu_{p^\infty})$, $F_n = K_n(\sqrt[p^n]{m})$ and $F_\infty = K_\infty(\sqrt[p^\infty]{m})$. Denote $\mathrm{Gal}(F_\infty/\mathbb{Q})$ and $\mathrm{Gal}(F_\infty/K_\infty)$ by G and H. Let $\Lambda(G)$ be the Iwasawa algebra of G. Let $\mathbb{Q}_{\mathrm{cyc}}$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and $\Gamma := \mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})$. Put

$$S = \{x \in \Lambda(G) \mid \Lambda(G)/\Lambda(G)x \text{ is finitely generated as a } \Lambda(H)\text{-module}\}.$$

and $S^* = \cup_{n\geq 0}\, p^n S$. S^* is an Ore set. $\Lambda(G)_{S^*}$ is the localization of $\Lambda(G)$ at S^*.

A left $\Lambda(G)$-module M is S^*-torsion if every element of M is killed by some element in S^*. A finitely generated left $\Lambda(G)$-module M is S^*-torsion if and only if $M/M[p^\infty]$ is finitely generated over $\Lambda(H)$ (see [CFKSV]). Let $\mathfrak{M}_H(G)$ be the category of finitely generated S^*-torsion left $\Lambda(G)$-modules.

For a ring R, the K_1-group of R is $K_1(R) := [\varinjlim_n GL_n(R)]^{\mathrm{ab}}$. K-theory tells us there is an exact sequence

$$K_1(\Lambda(G)) \to K_1(\Lambda(G)_{S^*}) \xrightarrow{\partial} K_0(\mathfrak{M}_H(G)).$$

Here, ∂ is defined as follows. Let $x = [A] \in K_1(\Lambda(G)_{S^*})$ where $A \in GL_n(\Lambda(G)_{S^*})$. Then by the left Ore condition, there exist some $s \in S^*$ and $B \in M_n(\Lambda(G))$ such that $A = (sI_n)^{-1}B$ where I_n is the identity matrix. Both sI_n and B give rise to linear maps on the left $\Lambda(G)$-module $\Lambda(G)^n$. (We consider $\Lambda(G)^n$ as the set of row vectors. The linear map corresponding to B is defined by $v \mapsto vB$ for $v \in \Lambda(G)^n$.) Then we define $\partial(x) := [\mathrm{cok}(B)] - [\mathrm{cok}(sI_n)] \in K_0(\mathfrak{M}_H(G))$. ∂ is surjectve ([CFKSV] Proposition 3.4).

Let E be an elliptic curve defined over $\mathbb{Q}$ with good ordinary reduction at p. Let $X(E/F_\infty) = \mathrm{Sel}(E/F_\infty)^\vee$ be the Pontrjagin dual of the Selmer group of E over F_∞. We can state the main conjecture now.

Conjecture 1.1 (Main Conjecture, [CFKSV] Conjectures 5.1, 5.7 and 5.8)**.**
(1) *$X(E/F_\infty)$ is in $\mathfrak{M}_H(G)$.*
(2) *There exists a p-adic L-function $\mathcal{L}_p(E/F_\infty)$ in $K_1(\Lambda(G)_{S^*})$.*
(3) *$\partial(\mathcal{L}_p(E/F_\infty)) = [X(E/F_\infty)]$ in $K_0(\mathfrak{M}_H(G))$.*

We have to explain what the p-adic L-function $\mathcal{L}_p(E/F_\infty)$ means.

2. p-adic L-functions

The p-adic L-function $\mathcal{L}_p(E/F_\infty)$ should be characterized by specializations. We explain the definition of specialization first. Let L be a finite extension of $\mathbb{Q}_p$ and $\mathcal{O}$ its integer ring. Let $\rho : G \to GL_n(\mathcal{O})$ be an Artin representation,

i.e. a continuous homomorphism with a finite image. We now want to define the specialization $K_1(\Lambda(G)_{S^*}) \to L \cup \{\infty\}$ associated to ρ. Naively, this should be as follows: The map ρ naturally extends to a ring homomorphism $\rho : \Lambda(G) \to M_n(\mathcal{O})$. On the other hand, we have a map $\phi : [\Lambda(G)^\times_{S^*}]^{\mathrm{ab}} \to K_1(\Lambda(G)_{S^*})$ which is surjective ([CFKSV] Theorem 4.4). For $s^{-1}f \in \Lambda(G)^\times_{S^*}$, we want to define the specialization of $\phi(s^{-1}f)$ by $\det(\rho(f))/\det(\rho(s))$. One of the problems is that this might become an indeterminate form $0/0$. So we proceed as follows: Define $\tilde{\rho} : G \to \{M_n(\mathcal{O}) \otimes_{\mathbb{Z}_p} \Lambda(\Gamma)\}^\times$ by $g \mapsto \rho(g) \otimes \overline{g}$, where $\overline{g}$ is the image of g under $G \twoheadrightarrow \Gamma$. Then, $\tilde{\rho}$ naturally extends to a ring homomorphism

$$\tilde{\rho} : \Lambda(G) \to M_n(\mathcal{O}) \otimes_{\mathbb{Z}_p} \Lambda(\Gamma) \cong M_n(\Lambda_{\mathcal{O}}(\Gamma)) \subset M_n(Q_{\mathcal{O}}(\Gamma)).$$

Here, $\Lambda(\Gamma)$ is the Iwasawa algebra of Γ, $\Lambda_{\mathcal{O}}(\Gamma) = \mathcal{O} \otimes_{\mathbb{Z}_p} \Lambda(\Gamma)$ and $Q_{\mathcal{O}}(\Gamma)$ is the quotient field of $\Lambda_{\mathcal{O}}(\Gamma)$. The point is the following:

Proposition 2.1 ([CFKSV] Lemma 3.3)**.** *$\tilde{\rho}(S^*) \subset M_n(Q_{\mathcal{O}}(\Gamma))^\times$, i.e., the determinant of each elements in $\tilde{\rho}(S^*)$ does not vanish.*

From this and the universality of the localization, $\tilde{\rho}$ extends uniquely to $\tilde{\rho} : \Lambda(G)_{S^*} \to M_n(Q_{\mathcal{O}}(\Gamma))$. Then, by the functoriality, we have $\tilde{\rho} : K_1(\Lambda(G)_{S^*}) \to K_1(M_n(Q_{\mathcal{O}}(\Gamma)))$. By the Morita equivalence, there is a canonical isomorphism $K_1(M_n(Q_{\mathcal{O}}(\Gamma))) \cong K_1(Q_{\mathcal{O}}(\Gamma))$. We also have $K_1(Q_{\mathcal{O}}(\Gamma)) \cong Q_{\mathcal{O}}(\Gamma)^\times$ canonically. Using the augmentation map $\pi : \Lambda_{\mathcal{O}}(\Gamma) \to \mathcal{O}$, we define $\pi : Q_{\mathcal{O}}(\Gamma)^\times \to L \cup \{\infty\}$ by $\pi(a/b) := \pi(a)/\pi(b)$. Here, we can avoid the indeterminate forms since $\Lambda_{\mathcal{O}}(\Gamma) \cong \mathcal{O}[[T]]$ is a UFD. Compositing all these maps, we can define $\rho : K_1(\Lambda(G)_{S^*}) \to L \cup \{\infty\}$, the specialization associated to ρ.

We can show that this map coincides with the above naive definition if either $\det(\rho(f))$ or $\det(\rho(s))$ does not vanish. This map also commutes with the natural map $\rho : K_1(\Lambda(G)) \to K_1(M_n(\mathcal{O})) \cong K_1(\mathcal{O}) \cong \mathcal{O}^\times$.

An important property of this specialization is the compatibility with the Euler characteristics. Let $\mathcal{O}^n(\rho)$ be the free $\mathcal{O}$-module of row vectors with rank n, on which $\Lambda(G)$ acts from the right via $\rho : \Lambda(G) \to M_n(\mathcal{O})$. Let $M \in \mathfrak{M}_H(G)$ and $x \in K_1(\Lambda(G)_{S^*})$ with $\partial(x) = [M]$. Then $\rho(x)$ is related with $\prod_{i \geq 0} \sharp \mathrm{Tor}_i^{\Lambda(G)}(\mathcal{O}^n(\rho), M)^{(-1)^i}$ (see [CFKSV] Theorem 3.6).

Recall $K_\infty = \mathbb{Q}(\mu_{p^\infty})$ and $F_\infty = K_\infty(\sqrt[p^\infty]{m})$. Let $\mathcal{P}_0$ denote the set of all primes l of $\mathbb{Q}$ which is prime to p and dividing m. For an elliptic curve $E/\mathbb{Q}$, set

$$\mathcal{P}_1 := \{l \in \mathcal{P}_0 |\ E/K_{\infty,v} \text{ has split multiplicative reduction for any prime } v|l\},$$
$$\mathcal{P}_2 := \{l \in \mathcal{P}_0 |\ E/K_{\infty,v} \text{ has good reduction and } E(K_{\infty,v})[p] \neq 0 \text{ for any } v|l\}$$

and $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$. Now we give a characterization of the p-adic L-function.

Conjecture 2.2 ([CFKSV] Conjecture 5.7)**.** *If E has good ordinary reduction at p, then there exists an element $\mathcal{L}_p = \mathcal{L}_p(E/F_\infty)$ in $K_1(\Lambda(G)_{S^*})$ satisfying*

$$\rho(\mathcal{L}_p) = \frac{L(E, \hat{\rho}, 1)}{\Omega_E^{+d^+(\hat{\rho})} \Omega_E^{-d^-(\hat{\rho})}} \cdot e_p(\rho) \cdot \frac{P_p(\rho, \alpha^{-1})}{P_p(\hat{\rho}, \beta^{-1})} \cdot P_p(E, \hat{\rho}, p^{-1}) \cdot \alpha^{-f_\rho} \cdot \prod_{l \in \mathcal{P}} P_l(E, \hat{\rho}, l^{-1}).$$

for any Artin representation ρ of G. Here, $\hat{\rho}$ denotes the contragradient of ρ. $L(E, \hat{\rho}, s)$ is the Hasse-Weil L-function and $P_l(E, \hat{\rho}, X)$ is its l-Euler factor for the twist of E by $\hat{\rho}$. For the other notations, look at [CFKSV].

There are few evidences for the existence of $\mathcal{L}_p(E/F_\infty)$. Even the following thing is not known. There is the case when $\mathrm{Sel}_{p^\infty}(E/F_\infty)$ vanishes (see [HV] §4.6). In such a case, the main conjecture predicts that $\rho(\mathcal{L}_p)$ is a p-adic unit for any ρ. Hence so is the RHS of the equation for any ρ in Conjecture 2.2. But we do not know whether this is the case or not in general.

If $\mathcal{L}_p(E/F_\infty)$ is contained in $\mathrm{Im}(\Lambda(G)\cap\Lambda(G)^\times_{S^*})$ under the surjection $\Lambda(G)^\times_{S^*} \twoheadrightarrow K_1(\Lambda(G)_{S^*})$ (we expect this) and if two Artin representations ρ and ρ' are congruent modulo p, then we have $\rho(\mathcal{L}_p) \equiv \rho'(\mathcal{L}_p)$ modulo p. T. Dokchitser and V. Dokchitser verified numerically the latter congruence ([DD]) for several specific p, E, F_∞, ρ and ρ''s.

Kato ([Ka]) showed the following: $K_1(\Lambda(G)_{S^*}) \cong K_1(\Lambda(G)_S) \oplus \mathbb{Z}^d$ canonically where $d = \sharp(G/G_0)$ ([Ka] Proposition 8.6). Note that the set S is also an Ore set. We denote by $\Lambda(G)_S$ the localization at S. Then Kato constructed a homomorphism

$$\theta = \prod_{n\geq 0} \theta_n : K_1(\Lambda(G)_S) \to \prod_{n\geq 0} Q(\Gamma_n)^\times$$

where $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$ and $Q(\Gamma_n)$ is the quotient field of $\Lambda(\Gamma_n)$, and showed that $\mathrm{Im}(\theta)$ is contained in a certain subgroup $\Phi_S(G)$ of $\prod_{n\geq 0} Q(\Gamma_n)$, consisting of all the elements $(a_n)_n$ such that there exist certain type of congruences between a_n's ([Ka] Proposition 8.9). The congruences are very much complicated, but stronger than naively expected.

From the construction, $\theta_n(\mathcal{L}_p(E/F_\infty)) = L_p(E/K_n, \chi_n) \times$ (error term) should hold. Here, $L_p(E/K_n, \chi_n) \in Q(\Gamma_n)$ is the (conjecturally existing) cyclotomic p-adic L-function of E over K_n twisted by χ_n, where χ_n is a character of $\mathrm{Gal}(F_n/K_n)$ of order p^n. We do not know whether θ is injective nor surjective, but still Kato obtained the following:

Theorem 2.3 (Kato)**.** *Assume that $L_p(E/K_n, \chi_n)$ exists for all n. If the collection $(L_p(E/K_n, \chi_n) \times (\text{error term}))_{n\geq 0}$ is contained in $\Phi_S(G)$, then $\mathcal{L}_p$ exists.*

3. Zábrádi's result

G. Zábrádi gave an explicit $\Lambda(G)$-module structure of the dual of Selmer group $X(E/F_\infty)$ and its characteristic element in $K_0(\Lambda(G)_{S^*})$, when $X(E/F_\infty)$ has rank one over $\Lambda(H)$. See [Za].

References

[CFKSV] J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob, *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. IHES **101** (2005), 163–208.

[DD] T. Dokchitser and V. Dokchitser, *"Computations in non-commutative Iwasawa theory"*, preprint (2004).

[HV] Y. Hachimori and O. Venjakob, *Completely faithful Selmer groups over Kummer extensions*, Documenta Math., Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 443–478.

[Ka] K. Kato, *"K_1 of some non-commutative completed group ring"*, K-theory **34**(2005), 99–140.

[Za] G. Zábrádi *"The characteristic elements of certain Iwasawa-modules in false Tate curve extensions"*, preprint (2006).

E-mail: yhachi@math.keio.ac.jp