NOTES ON THE GL_2 MAIN CONJECTURE

WILLIAM B. HART

Introduction

After hearing John Coates speak at Iwasawa 2004 on the new GL_2 main conjecture for Iwasawa theory, a la Coates, Fukaya, Kato, Sujatha and Venjakob, I went away with a desire to learn about this non-commutative Iwasawa theory and give a talk on it for learning purposes. This set of notes is essentially a written version of my talk, given at the Intercity Number Theory Seminar, held in Leiden in September 2004.

The notes fall into three main sections.

The first section deals with the basic non-commutative setup for Iwasawa theory and covers the structure theory of Λ-modules in this setting. Along the way definitions of all the relevant non-commutative objects are given, including p-adic Lie groups and Auslander regular rings.

The second section is mainly about K-theory. The manner of defining characteristic elements of a Λ-module in the non-commutative setting is via K-theory. Actually it can be done this way in the commutative setting as well but many people aren't familiar with this, so the requisite K-theory is described from scratch.

The final section is about the GL_2 main conjecture itself. Here a certain p-adic L-series associated to an elliptic curve is defined and conjectured to be the same as a p-adic L-series coming from the characteristic element of a particular Λ-module, namely, the dual of the Selmer group of the elliptic curve.

It is not the purpose of these notes to introduce anything new, only to provide an introduction for mathematicians not familiar with all the theory needed to understand the original papers. Actually the original papers are extremely well written and eminently understandable, however as is always the case with such material, they occasionally presuppose a certain background knowledge, which not everyone possesses.

Proofs of the various results will be omitted and the reader is encouraged to consult the references at the end of the notes for these.

1. Non-commutative Iwasawa Theory: p-adic Lie Groups and Auslander Regularity

1.1. **Where does Non-commutative Iwasawa Theory come from?** Just as the classical case of Iwasawa theory can loosely be thought of as coming from a tower of number fields constructed by adjoining all the p-power torsion points of the exponential function (p-th power roots of unity) to a number field, so the elliptic curve version starts from adjoining all the p-power division points of an elliptic curve to a number field k.

However there is more than one case of the elliptic curve version. One version is for elliptic curves with CM. Just as for the classical case of Iwasawa theory, this case is inherently commutative. However there is also the elliptic curve case for elliptic curves *without complex multiplication.* This case involves non-commutative algebra and is the case we will be interested in throughout these notes. (Of course we are over-simplifying the situation here, since there are numerous different approaches to Iwasawa theory, even in the number field case, let alone the elliptic curve case. However this overview is not too misleading.)

In other words, we will be considering the extension $k_\infty = k(E(p^\infty))$ of k which arises from adjoining all the p-power division points of E without complex multiplication.

The following celebrated theorem of Serre is the starting point for this theory.

Theorem 1.1.1. *The galois group $G = Gal(k_\infty/k)$ is an open subgroup of $GL_2(\mathbb{Z}_p)$.*

We shall shortly see that the following is a corollary of this important result.

Corollary 1.1.2. *G is a p-adic Lie group of dimension 4.*

In the next part, we will define what we mean by a p-adic Lie group. Firstly however, we make the following additional comments for general orientation.

Remark: More generally than the above, we can adjoin the p-power torsion points of an Abelian variety, for a rational prime p, to a number field k. Note that we will not deal with this more general situation in these notes, but restrict ourselves to the elliptic curve case, or GL_2 case, as it is known.

Note: It is important that we include the condition that E be without complex multiplication in the above. In the case *with* complex multiplication, the Iwasawa algebra $\Lambda(G)$ of G is isomorphic to the ring of formal power series $\mathbb{Z}_p[[S,T]]$, in two variables. The structure of $\Lambda(G)$-modules in this case is almost completely understood, after the work of Coates and Wiles and Perrin-Riou. Also a two variable main conjecture was formulated essentially by Yager and then proved by Rubin.

1.2. p-adic Lie Groups.

We can think of a p-adic Lie group as the following three things simultaneously:

i) A group;

ii) A topological space; and

iii) A p-adic manifold.

Firstly we remind ourselves of the following.

Definition 1.2.1. *A* topological group *G is a topological space with a group structure such that the multiplication map and inversion are continuous.*

Most readers will also be aware of the following definition.

Definition 1.2.2. *A topological group G is* profinite *if it is the inverse limit $\varprojlim G_i$ in the category of topological groups, of an inverse system of finite groups, G_i, with the discrete topology.*

However, the following equivalent definition, is less well known.

Definition 1.2.3. *A profinite group is a compact Hausdorff topological group G, whose open subgroups form a base for the neighbourhoods of the identity.*

In fact $G \cong \varprojlim G/N$ where N ranges over the open normal subgroups of G.

Example: $\mathbb{Z}_p$ is a profinite group, since $\mathbb{Z}_p = \varprojlim(\mathbb{Z}/p^n\mathbb{Z})$.

In actual fact, this last example is more special than a profinite group. It is an example of a *pro-p* group.

Definition 1.2.4. *A profinite group is a* pro-p *group if each open subgroup has index a power of p in the whole group. Alternatively, it is pro-p if it is the inverse limit of finite p-groups.*

In the example, the open subgroups of $\mathbb{Z}_p$ are all of the form $p^k\mathbb{Z}_p$ for $k \geq 0$, and so satisfy the given condition.

We will also make use of the following.

Definition 1.2.5. *A topological group G is* finitely generated *if there is a finite subset X of G such that G is equal to the closure in G of the subgroup generated by X.*

Now we come to our first definition of a p-adic Lie group.

Definition 1.2.6. *A topological group G is called a* p-adic Lie group *if G has the structure of an analytic manifold over $\mathbb{Q}_p$ and if the function $(x, y) \rightarrow xy^{-1}$ is analytic, i.e. it is locally homeomorphic to an open subgroup of $\mathbb{Q}_p^n$, with p-adic analytic functions for transition maps and such that multiplication and inversion are p-adic analytic functions.*

The number n is called the *dimension* of the p-adic Lie group.

But p-adic Lie groups have a feature which is not held in common with the better known Lie groups over $\mathbb{R}$ or $\mathbb{C}$. For p-adic Lie groups, there is a completely group theoretical way of describing them, without resorting to manifolds. This way of describing them is due to Lazard.

We need a few basic definitions first before giving this second definition of p-adic Lie groups.

Definition 1.2.7. *A pro-p group H is called* powerful *if $[H,H] \subseteq H^p$ (the group generated by all the p-th power elements of H), for an odd prime p (or $[H,H] \subseteq H^4$, for $p = 2$).*

Definition 1.2.8. *A pro-p group H is* uniform *if it is*

i) Finitely generated;

ii) Powerful; and

iii) Satisfies

$$[P_i(H) : P_{i+1}(H)] = [P_1(H) : P_2(H)],$$

where $P_1(H) = H$ and $P_{i+1}(H) = P_i(H)^p[P_i(H), H]$ (here $[P_i(H), H]$ means the subgroup generated by all commutators $[x, y]$ with $x \in P_i(H), y \in H$).

The descending sequence of groups

$$H = P_1(H) \supseteq P_2(H) \supseteq \cdots$$

is called the *lower central p-series* of H.

Finally we come to:

Theorem (Lazard) 1.2.9. *A topological group G is a p-adic Lie group iff G contains an open subgroup which is a uniform pro-p group.*

The minimum cardinality of the finite generating set of the uniform subgroup is referred to as the *dimension* of G. It of course agrees with the dimension of the p-adic Lie group as a $\mathbb{Q}_p$-manifold.

Examples: The following are examples of p-adic Lie groups.

(i) $\mathbb{Q}_p$ has dimension 1, with open uniform subgroup $\mathbb{Z}_p$;

ii) $G =\mathrm{GL}_n(\mathbb{Z}_p)$ has dimension n^2 with open uniform subgroup $H = \{X \in G : X \equiv I_n \pmod p\}$, where I_n is the $n \times n$ identity matrix;

iii) $G =\mathrm{SL}_n(\mathbb{Z}_p)$ has dimension n^2-1 with open uniform subgroup given by $G \bigcap H$, with H defined as in ii);

iv) In particular, from ii), note that $\mathbb{Z}_p^*$ is a p-adic Lie group.

Now that we have a feel for what it means for the group G that we defined in the first section to be a p-adic Lie group, we return to Iwasawa theory.

1.3. **Modules over the Iwasawa Algebra.** If G is a p-adic Lie group, then the *Iwasawa algebra* over G is defined as follows

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

where U runs through the open normal subgroups of G.

In particular, if G is a compact p-adic Lie group, such as the group G we defined associated to an elliptic curve, in the first section, then $\Lambda(G)$ is (left and right) Noetherian.

To mirror the commutative case, we'd now like a dimension theory for modules finitely generated over the ring $\Lambda = \Lambda(G)$. In analogy with the commutative case of Iwasawa theory, we'd also like to have a notion of pseudo-null modules.

Recall that in the commutative case the dimension of a module M, finitely generated over a ring R, is defined to be the Krull dimension of the support of M in spec R (where by support we mean the prime ideals $\mathfrak{p}$ such that $M_{\mathfrak{p}}$ is not zero). Then the module M is said to be *pseudo-null* if the codimension of M, with respect to the dimension of R over itself, is greater than or equal to 2.

A suitable dimension theory analogous to this, in the non-commutative case, has been found for Auslander regular rings, which we now proceed to define.

From now on, we restrict attention to (left) modules M over $\Lambda = \Lambda(G)$, which are finitely generated over Λ.

Firstly we need some definitions.

Definition 1.3.1. *The* Iwasawa adjoints *of a Λ-module M, are defined by*

$$E^i(M) = Ext^i_\Lambda(M, \Lambda); \;\; for \;\; i \geq 0.$$[1]

The Iwasawa adjoints are so-named, since if $G \cong \mathbb{Z}_p$, then for a $\Lambda(G)$-module M, $E^1(M)$ is isomorphic to a certain adjoint module $\alpha(M)$ which Iwasawa defined.

The Iwasawa adjoints we have defined, have an action of Λ on the right, however they can be construed as left Λ-modules via the involution of Λ.

These adjoints are important for the following definition.

Definition 1.3.2. *The* grade *of a module $M \neq 0$ is given by*

$$j(M) = min\{i : E^i(M) \neq 0\}.$$

By convention $j(\{0\}) = \infty$.

Now we can state the Auslander condition, which will be part of the definition of an Auslander regular ring.

Auslander Condition on Λ: For all Λ-modules M, integers m and submodules N of $E^m(M)$, require that $j(N) \geq m$.

Now we can finally define the class of rings which interests us.

[1] For the definition of Ext, the reader may refer to the notes on cohomology found on the author's website: http://www.math.leidenuniv.nl/~wbhart/, or simply refer to MacLane's book *Homology.*

Definition 1.3.3. *A Noetherian ring Λ is called Auslander regular if it has finite global homological dimension*[2] *and the Auslander condition holds.*

The usefulness of Auslander regularity in our situation is provided by the following result.

Theorem 1.3.4. *If G is a p-adic Lie group without p-torsion, then $\Lambda(G)$ is an Auslander regular ring.*

From now on, the following hypothesis must be made:

Hypothesis: G has no p-torsion.

Now the dimension theory for modules over an Auslander regular ring comes from results of Björk. For an Auslander regular ring, he defined a certain finite canonical filtration of modules for a Λ-module M

$$T_0(M) \subseteq T_1(M) \subseteq \ldots \subseteq T_{d-1}(M) \subseteq T_d(M) = M.$$

Now the dimension can be defined as follows.

Definition 1.3.5. *The minimum i for which $T_i(M) = M$ is called the dimension $\delta(M)$ of $M \neq 0$. By convention, $\delta(\{0\}) = -\infty$.*

Also one can naturally define:

Definition 1.3.6. *A Λ-module M is called* pseudo-null *if it is at least of codimension 2, with respect to the dimension of the ring Λ over itself, i.e.:*

$$\delta(M) \leq d - 2.$$

As usual we say that two modules M and N are pseudo-isomorphic if the kernel and cokernel of a homomorphism between them are pseudo-null. We write $M \sim N$.

The only difficulty is that in the non-commutative case, this is not an equivalence relation. The way that we get around this difficulty is to take the quotient category of Λ-modules with respect to the Serre subcategory $\mathcal{PN}$ of pseudo-null Λ-modules. Thus we speak of modules mod $\mathcal{PN}$. (We will define Serre subcategories and quotient categories in the K-theory section of these notes.)

Furthermore, let us define Λ-mod(p) to be the subcategory of Λ-mod consisting of $\mathbb{Z}_p$-torsion modules and define $\mathcal{PN}(p) = \mathcal{PN} \bigcap \Lambda\text{-mod}(p)$.

Now we can state the structure theorems that have been proved for Λ-modules.

Firstly there is the fairly restrictive:

Theorem 1.3.7. *If G is a p-adic Lie group without p-torsion such that Λ and Λ/p are integral, and if M is in Λ-mod(p), then there exist unique $n_1, \ldots, n_r \in \mathbb{N}$ such that*

$$M \cong \bigoplus_{1 \leq i \leq r} \Lambda/p^{n_i} \quad (\text{mod } \mathcal{PN}).$$

[2] Recall that a Λ-module M has finite left (right) homological dimension if there is a finite projective resolution of M, i.e. an exact sequence

$$0 \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

with P_i left (resp. right) projective Λ-modules (direct summands of free Λ-modules). Note that for Noetherian Λ, left and right homological dimension coincide. Then the ring Λ has finite *global* homological dimension if all Λ-modules have finite homological dimension.

Note: from this definition, it is possible to define a μ-invariant:

$$\mu \cong \sum_i n_i(\mathrm{tor}_{\mathbb{Z}_p} M).$$

Finally we state the much more general structure theorem for Λ-modules.

Theorem 1.3.8. *Let G be an extra powerful ($[G,G] \subseteq G^{p^2}$) uniform pro-p group. Then for any finitely generated $\Lambda(G)$-torsion module M, there exist finitely many left ideals $J_1, \dots, J_r$ such that*

$$M \cong \bigoplus_{1 \le i \le r} \Lambda/J_i \pmod{\mathcal{PN}}.$$

Note that by a Λ-torsion module M, here, we mean a module such that the canonical map

$$M \xrightarrow{\phi_M} M^{++} = E^0(E^0(M)),$$

is the zero map. Note that if Λ is a Noetherian integral domain, then ker ϕ_M is precisely the set of torsion elements of M.

2. K-theory: Characteristic Elements

In this section, we introduce the basics of K-theory. The main aim is to explain a particular long exact sequence of K-theory called the localization sequence, and apply it to the localization of our ring Λ at a certain multiplicative subset called an Ore subset. This leads to us being able to define a characteristic element of a Λ-module M as an inverse image of the class of M in a certain K-group, under one of the maps of the localization sequence.

2.1. K_0 **of a Ring.** Let M be a commutative monoid. Then there exists an abelian group $K(M)$ and a monoid homomorphism (preserves identity and addition),

$$\gamma : M \to K(M),$$

such that any homomorphism into an abelian group $f : M \to A$ induces a unique homomorphism $f_* : K(M) \to A$ such that $f = f_* \circ \gamma$. That is to say, $K(M)$ is universal for homomorphisms of M into abelian groups.

To construct $K(M)$, start with the free abelian group generated by M, $F_{\mathrm{ab}}(M)$. Let $[x]$ correspond to the element of $F_{\mathrm{ab}}(M)$ coming from the generator $x \in M$. Let B be the subgroup of $F_{\mathrm{ab}}(M)$ generated by elements of the form

$$[x+y] - [x] - [y] \quad \text{where} \quad x, y \in M.$$

Let $K(M) = F_{\mathrm{ab}}(M)/B$.

Thus we have transferred the monoid operation to the abelian group.

Now we can let $\gamma : M \to K(M)$ be given by

$$\begin{array}{rcccl} \gamma : M & \to & F_{\mathrm{ab}}(M) & \to & F_{\mathrm{ab}}(M)/B \\ x & \mapsto & [x] & \mapsto & [x] + B. \end{array}$$

The abelian group $K(M)$ is called the *Grothendieck group* of M.

Given a ring A, we can define the monoid of isomorphism classes of finitely generated projective A-modules. We let $[P]$ denote the isomorphism class of P and define the monoid operation by

$$[P] + [Q] = [P \oplus Q].$$

Now we can take the Grothendieck of this monoid. It is denoted $K_0(A)$.

2.2. K_0 **of a Symmetric Monoidal Category.** We can do better than just defining $K_0(A)$ for a ring A. In fact K-theory is best viewed as taking K-groups of various categories.

Thus we define a *symmetric monoidal category* to be a category S with a functor

$$\Box : S \times S \to S,$$

a distinguished object e and the following natural isomorphisms

$$e \,\Box\, s \cong s, \quad s \,\Box\, e \cong s,$$
$$s \,\Box\, (t \,\Box\, u) \cong (s \,\Box\, t) \,\Box\, u, \quad s \,\Box\, t \cong t \,\Box\, s.$$

We also need "coherency", so that $s_1 \,\Box \ldots \Box\, s_n$ can be written unambiguously without parentheses.

Examples: $\Box = \oplus =$ direct sum, $\Box = \coprod =$ finite coproduct or $\Box = \times =$ finite product.

Now, in fact, we can define $K_0^{\Box}$ exactly as we defined $K_0(A)$, so long as the isomorphism classes of objects of S form a set.

It is of course the case that the two definitions agree, i.e. $K_0(A) = K_0^{\bigoplus}(\mathbf{P}(A))$, where $\mathbf{P}(A)$ is the category of finitely generated projective A-modules.

We can think of $K_0^{\Box}$ via its presentation, with a generator $[s]$ for each isomorphism class of objects, subject to relations

$$[s \,\Box\, t] = [s] + [t].$$

It is clear from this that each element of $K_0^{\Box}$ can be written $[s]-[t]$ for some objects s and t.

Example: The category of finite sets, $\mathbf{Set}_f$, with coproduct the disjoint sum $\coprod$. We then have $K_0^{\coprod}(\mathbf{Set}_f) = \mathbb{Z}$.

2.3. K_0 **of Skeletally Small Abelian Categories.** This whole idea of taking K-groups of categories can be vastly expanded. In particular, we can take K_0 of a skeletally small abelian category.

i) A category is said to be *skeletally small* if the objects in the category form a set, or the category is equivalent to one in which they do.

ii) A category is *abelian* if it is *additive*,

(i) It contains a 0 object (both initial and terminal);

(ii) It contains all products $A \times B$;

(iii) Every set $\mathrm{Hom}(A, B)$ has the structure of an abelian group (with operation denoted $+$); and

(iv) Morphisms satisfy

$$\beta(\alpha_1 + \alpha_2) = \beta\alpha_1 + \beta\alpha_2, \;\; (\beta_1 + \beta_2)\alpha = \beta_1\alpha + \beta_2\alpha,$$

(when defined).

AND

(v) Every morphism has a kernel and cokernel; and

(vi) Every monic arrow is a kernel and every epic arrow is a cokernel.

(Recall: An arrow f is monic if $e_1 \neq e_2 \implies fe_1 \neq fe_2$. An arrow f is epic if $g_1 \neq g_2 \implies g_1 f \neq g_2 f$. The kernel of an arrow α is a monic arrow x such that $\alpha x = 0$ and for any other β, $\alpha\beta = 0 \implies \beta = x\beta'$, (i.e. β factors through x). Of course a cokernel of α is then an arrow σ such that $\sigma\alpha = 0$ and $\gamma\alpha = 0 \implies \gamma = \gamma'\sigma$.)

Given an abelian category $\mathcal{A}$, $K_0(A)$ is the abelian group having one generator $[A]$ for each object A of $\mathcal{A}$, with a relation

$$[A] = [A'] + [A''],$$

for every short exact sequence

$$0 \to A' \to A \to A'' \to 0.$$

As a consequence of this definition, we have the following:

i) $[0] = 0$;

ii) If $A \cong A'$, then [A] = [A']; and

iii) $[A' \oplus A''] = [A'] + [A'']$.

If two abelian categories are equivalent, their Grothendieck groups are naturally isomorphic.

If $\mathcal{A}$ is considered also as a symmetric monoidal category, $K_0(\mathcal{A})$ is a quotient group of $K_0^{\oplus}(\mathcal{A})$ in general. In the case of the category of finitely generated projective R-modules, for a ring R, all exact sequences are split, and thus the list of conditions i)-iii) above is in fact exhaustive. This is precisely the set of conditions we had in the definition of $K_0(R)$, and thus in this particular case, the two definitions of K_0 in fact agree.

2.4. **Quotient Categories.**

The main reason for defining K_0 of abelian categories, is that we can take quotient categories by Serre subcategories.

Definition 2.4.1. *A* Serre subcategory *of an abelian category $\mathcal{A}$ is a subcategory $\mathcal{B}$ which is closed under subobjects, quotients and extensions, i.e. if*

$$0 \to B \to C \to D \to 0,$$

is exact in $\mathcal{A}$, then $C \in \mathcal{B} \iff B, D \in \mathcal{B}$.

If $\mathcal{A}$ is a small abelian category, with Serre subcategory $\mathcal{B}$, we define the quotient category $\mathcal{A}/\mathcal{B}$ as:

i) The objects of $\mathcal{A}/\mathcal{B}$ are the objects of $\mathcal{A}$;

ii) If M, N are objects of $\mathcal{A}$, and M', N' subobjects of M, N repsectively, then the canonical morphisms $\iota : M' \to M$ and $\rho : N \to N/N'$ yield a natural homomorphism $\mathrm{Hom}_{\mathcal{A}}(M, N) \to \mathrm{Hom}_{\mathcal{A}}(M', N/N')$.

As M', N' range over the subobjects of M, N such that M/M' and N' are objects of $\mathcal{B}$, then the abelian groups $\mathrm{Hom}_{\mathcal{A}}(M', N/N')$ form a directed system of abelian groups. Thus we define

$$\mathrm{Hom}_{\mathcal{A}/\mathcal{B}}(M, N) = \varinjlim \mathrm{Hom}_{\mathcal{A}}(M', N/N').$$

The following theorem makes quotient categories a useful and elegant one.

Theorem 2.4.2. *$\mathcal{A}/\mathcal{B}$ is also an abelian category.*

The following is also useful to bear in mind when dealing with quotient categories.

Theorem 2.4.3. *For the quotient category $\mathcal{A}/\mathcal{B}$*

(i) If $u : M \to N$ then $Tu : TM \to TN$ is null iff im $u \in$ Ob $\mathcal{B}$;

(ii) Tu is a monomorphism iff ker $u \in$ Ob $\mathcal{B}$;

(iii) Tu is an epimorphism iff coker $u \in$ Ob $\mathcal{B}$.

2.5. K_1 **of a Ring.** Now we must define the Whitehead group K_1 for a ring R.

If $G \in \mathrm{GL}_n(R)$ then there is an injection

$$\begin{array}{rcl} \iota : \mathrm{GL}_n(R) & \to & \mathrm{GL}_{n+1}(R) \\ G & \mapsto & \begin{pmatrix} G & 0 \\ 0 & 1 \end{pmatrix}. \end{array}$$

We let $\mathrm{GL}(R)$ be the union of the sequence

$$\mathrm{GL}_1(R) \overset{\iota}{\hookrightarrow} \mathrm{GL}_2(R) \overset{\iota}{\hookrightarrow} \cdots \mathrm{GL}_n(R) \overset{\iota}{\hookrightarrow} \cdots .$$

It is called the *infinite general linear group.*

Now we can define K_1 of a ring R.

Definition 2.5.1. *The* Whitehead group $K_1(R)$ *of a ring R is defined to be $GL(R)/[GL(R), GL(R)]$.*

$K_1(R)$ has the following universal property: every homomorphism from $\mathrm{GL}(R)$ to an abelian group A, must factor through the natural quotient $\mathrm{GL}(R) \to K_1(R)$.

A ring homomorphism $R \to S$ induces a natural map $\mathrm{GL}(R) \to \mathrm{GL}(S)$ and hence $K_1(R) \to K_1(S)$. So K_1 is a functor from rings to abelian groups.

The following theorem is also useful in calculating various K_1 groups.

Theorem 2.5.2. *If $R = R' \times R''$ then $K_1(R) = K_1(R') \oplus K_1(R'')$.*

Now it is actually possible to give another interpretation to K_1 of a ring, via elementary matrices. Firstly we define:

Definition 2.5.3. *If $i \neq j$ and $r \in R$ then $e_{ij}(r)$ is the* elementary matrix *in $GL(R)$ with 1 in every diagonal position, and zero elsewhere.*

Note: Such a matrix can be thought of as an elementary row operation.

Let $E_n(R)$ be the subgroup of $\mathrm{GL}_n(R)$ generated by the $e_{ij}(r)$. Let $E(R)$ be the union of the $E_n(R)$ over all n. Then we have the following identification.

Theorem 2.5.4. *We have*

$$E(R) = [GL(R), GL(R)].$$

Thus

$$K_1(R) = GL(R)/E(R).$$

In terms of the elementary row operations $e_{ij}(r)$, $E_n(R)$ is the set of matrices in $\mathrm{GL}_n(R)$ which can be reduced to the identity. Thus $K_1(R)$ measures how far from achieving this that we are.

Example: If $R = F$, a field, then the obstruction is simply $F^\times$, measured by the determinant. So we have

$$E_n(F) = \mathrm{SL}_n(F) \quad \text{and} \quad K_1(F) = F^\times.$$

2.6. **K_1 of a Skeletally Small Abelian Category.** Now we can define K_1 of a skeletally small abelian category.

We define first an auxilliary category $\mathcal{A}_{aut}$ which is defined as follows. The objects of $\mathcal{A}_{aut}$ are pairs (A, f) where $A \in \text{Ob}\,\mathcal{A}$ and $f \in \text{Aut}(A)$, and whose morphisms $(A, f) \to (B, g)$ are given by maps $h : A \to B$ such that $h \circ f = g \circ h$.

Note: A sequence

$$0 \to (A', f') \to (A, f) \to (A'', f'') \to 0,$$

is exact in $\mathcal{A}_{aut}$ iff $0 \to A' \to A \to A'' \to 0$ is exact in $\mathcal{A}$.

Now we define $K_1(\mathcal{A})$ to be the abelian group whose generators are $[(A, f)] \in \text{Ob}\,\mathcal{A}_{aut}$ and whose relations are

i) If

$$0 \to (A', f') \to (A, f) \to (A'', f'') \to 0,$$

is exact in $\mathcal{A}_{aut}$ then $[(A, f)] = [(A', f')] + [(A'', f'')]$; and

ii) For all $f, g \in \text{Aut}(A)$

$$[(A, fg)] = [(A, f)] + [(A, g)].$$

Theorem 2.6.1. *The definition of K_1 just given agrees with $K_1(R)$ for a ring R, when $\mathcal{A}$ is the category of finitely generated, projective R-modules.*

2.7. **Cartan Homomorphisms.** Ultimately we'd like the K-theory that we have just been defining to bear some relevance to the modules that we met in the first section of these notes. In particular we'd like to deal with the category of finitely generated Λ-modules, dropping the projective condition (note that we could not work simply with the category of Λ-modules, since it is not skeletally small).

We therefore define

$$G_0(R) = K_0(\mathbf{M}(R)),$$

where $\mathbf{M}(R)$ is the category of finitely generated R-modules. It is an abelian subcategory of mod$-R$, the category of R-modules, and is skeletally small.

This is a useful definition, since it turns out that there is a homomorphism $K_0(R) \to G_0(R)$ called the *Cartan homomorphism* for K_0. Thus this homomorphism is a homomorphism from K_0 of the category of finitely generated, projective R-modules, to that of the category of finitely generated R-modules.

Similarly we can define

$$G_1(R) = K_1(\mathbf{M}(R)),$$

and the inclusion of categories $\mathbf{M}(R) \supset \mathbf{P}(R)$ again induces a (Cartan) homomorphism $K_1(R) \to G_1(R)$.

In the case we are interested in, where R is $\Lambda(G)$ as defined in the first section of these notes, the following theorem makes these Cartan homomorphisms very useful. In particular, it is a theorem that the ring $\Lambda(G)$ as defined there, and with the hypothesis that there is no p-torsion, is regular.

Theorem 2.7.1. *For a regular (no left or right zero divisors), Noetherian ring R, the Cartan homomorphisms are both isomorphisms.*

This theorem should be viewed as enabling us to view any statement about $G_0(R)$ and $G_1(R)$ as being interchangeable with one about $K_0(R)$ and $K_1(R)$, given that the ring R is regular and Noetherian.

2.8. **Localization at an Ore Subset.** The reason we have defined all these category theory gadgets and K-theory is that we can apply the following remarkable theorem of Quillen, called the localization theorem.

Theorem (Quillen) 2.8.1. *Let $\mathcal{T}$ be a Serre subcategory of a small abelian category $\mathcal{M}$. Then there is a long exact sequence of K-groups*

$$\ldots K_{i+1}(\mathcal{M}/\mathcal{T}) \to K_i(\mathcal{T}) \to K_i(\mathcal{M}) \to K_i(\mathcal{M}/\mathcal{T}) \to K_{i-1}(\mathcal{T}) \to \ldots \to K_0(\mathcal{M}/\mathcal{T}) \to 0.$$

Note that we have not defined the K-groups K_i for $i \geq 2$. We will not need this part of the sequence and so for us the only relevant part is that which contains the K-groups K_i for $i = 0, 1$.

We will apply this theorem with $\mathcal{M} = \mathbf{M}(R)$, the category of finitely generated Λ-modules, and $\mathcal{T}$ the subcategory of $\mathcal{M}$ consisting of the $M \in \text{Ob } \mathcal{M}$ such that $M_{S^*} = 0$. Here we mean that the localization of M at a certain multiplicative subset, which we will describe below, is zero. This last category is also denoted $\mathbf{M}(\Lambda_{S^*} - \text{tors})$.

The following theorem is important for the application of the localization theorem in this instance.

Theorem 2.8.2. *With the definitions just given, $\mathcal{M}/\mathcal{T}$ is equivalent to the category of finitely generated Λ_{S^*}-modules.*

Again we define what we mean by the localization of Λ at the multiplicative subset S^*, below.

The result of substituting all these categories into the localization theorem is that the following sequence is exact

$$K_1(\Lambda) \longrightarrow K_1(\Lambda_{S^*}) \xrightarrow{\partial} K_0(\Lambda_{S^*} - \text{tors}) \longrightarrow K_0(\Lambda) \longrightarrow K_0(\Lambda_{S^*}).$$

Now to make sense of the foregoing, we define what we mean by the localization of a ring R at a multiplicative subset S. We note that localization in the noncommutative case is delicate. In particular the following two conditions must be met:

i) For any $s \in S$ and $r \in R$, there exists an $s' \in S$ and $r' \in R$ such that $sr' = rs'$; and

ii) If $sr = 0$, then $rs' = 0$ for some $s' \in S$.

In our case, the ring $R = \Lambda(G)$ is regular, and so only (i) will be needed. A multiplicative subset S of R satisfying (i) is called an Ore subset.

In fact, the conditions (i) and (ii) are not just necessary:

Theorem 2.8.3. *There is a* localization *(denoted R_S) of a ring R at a multiplicative subset S, iff the conditions (i) and (ii) above hold. This localization is a ring homomorphism $\phi : R \to R_S$ such that*

i) The image under ϕ of each element of S is invertible in R_S; and

ii) Each element of R_S is of the form $\phi(r) \cdot \phi(s)^{-1}$, for some $r \in R$ and $s \in S$.

We also need to define what we mean by the localization of an R-module M at such a set S. We firstly define an equivalence on the product $M \times S$, by $(m, s) \sim (n, t)$ if there exist $u, v \in R$ such that $su = tv \in S$ and $mu = nv$. Then we define $M_S = (M \times S)/\sim$.

2.9. **A Canonical Ore Subset.** The above results are applied, in practice, to a canonical Ore subset of the ring $\Lambda = \Lambda(G)$. However a further assumption needs to be made.

Assumption: Let G have a normal subgroup H such that $\Gamma = G/H \cong \mathbb{Z}_p$.

This situation is of particular interest to us. For, let E be an elliptic curve over $\mathbb{Q}$ and set $F_\infty = \mathbb{Q}(E(p^\infty))$. By the Weil pairing, $F_\infty \supset \mathbb{Q}(\mu_{p^\infty})$, hence F_∞ contains $\mathbb{Q}^{\text{cyc}}$. Now letting $G = \text{Gal}(F_\infty/\mathbb{Q})$ and $H = \text{Gal}(F_\infty/Q^{\text{cyc}})$, $\Gamma = G/H$ has the required property.

Under this assumption, we can construct a canonical Ore subset as follows.

Definition 2.9.1. *We let S be the set of all $f \in \Lambda(G)$ such that $\Lambda(G)/\Lambda(G)f$ is a finitely generated $\Lambda(H)$-module.*

Theorem 2.9.2. *The set S is a left and right Ore set in $\Lambda(G)$, with no zero divisors.*

The following is helpful in further characterising the set S just defined.

Theorem 2.9.3. *If M is a finitely generated (left or right) $\Lambda(G)$-module, then M is finitely generated over $\Lambda(H)$ iff M is S-torsion.*

Now the perceptive reader will have noticed that in earlier subsections we mentioned an Ore subset S^*. It turns out that by 'saturating' S by p, a more natural theory is obtained, in a sense reducing the theory to modules over $\Lambda(\Gamma)$, which can be identified with $\mathbb{Z}_p[[T]]$. To achieve this slightly more natural version of events, we localize at the set S^*, defined as follows.

Definition 2.9.4. *Let $S^* = \bigcup_{n\geq 0} p^n S$.*

Note that S^* is still a left and right Ore subset of Λ, without zero divisors. We also note that

$$\Lambda(G)_{S^*} = \Lambda(G)_S[1/p].$$

Now we have fully defined the objects that appear in the localization sequence derived above from Quillen's theorem. The important thing now, is that with the definition of S^* just given, one of the categories appearing in the localization sequence has a special meaning.

Definition 2.9.5. *Let $\mathcal{M}_H(G)$ be the category of finitely generated S^*-torsion $\Lambda(G)$-modules.*

Theorem 2.9.6. *The category $\mathcal{M}_H(G)$ is the category of all $\Lambda(G)$-modules such that $M/M(p)$ is finitely generated over $\Lambda(H)$, where $M(p)$ is the largest submodule killed by a power of p. (Note: H is a submodule of $M(p)$.)*

To use the localization sequence to define characteristic elements, we must retain the assumptions we have introduced to date. We note that in particular the assumption that G has no element of order p is automatically satisfied if $p \geq 5$, in the situation we have been considering, involving an elliptic curve over $\mathbb{Q}$. Under all the assumptions, we have:

Theorem 2.9.7. *The following map from the localization sequence which we have built, is surjective:*

$$\partial_G : K_1(\Lambda(G)_{S^*}) \to K_0(\mathcal{M}_H(G)).$$

At last, we can define what we mean by a characteristic element of a finitely generated $\Lambda(G)$-module M.

Definition 2.9.8. *A characteristic element of M is an inverse image under ∂_G, of $[M]$, in $K_0(\mathcal{M}_H(G))$, written ζ_M.*

Finally we mention the following conjecture which will be important for the statement of the main conjecture in the next section.

Conjecture 2.9.9. *Under all the assumptions made thus far,*

$$X(E/F_\infty) = Hom(Sel(E/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p),$$

is an object of the category $\mathcal{M}_H(G)$.

In particular, if this conjecture holds, we can define a characteristic element of the dual of Selmer, $X(E/F_\infty)$. This particular characteristic element will play an important part in the main conjecture, just as the characteristic element of a particular module X does, in Iwasawa theory for number fields.

3. The Main Conjecture: p-adic L-functions

Throughout this section we will restrict to an elliptic curve E over $\mathbb{Q}$ with ordinary reduction at p.

Our main task before stating the main conjecture will be to introduce a certain p-adic L-series associated to E.

For a prime number q, let Frob_q be, as usual, the Frobenius automorphism of q in $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)/I_q$, where I_q is the inertia subgroup of q.

Let ρ be any Artin representation of our p-adic Lie group G, realised in a finite dimensional vector space V_ρ over some finite extension K_ρ of $\mathbb{Q}$. (By an Artin representation we mean a representation which factors through some finite quotient of the Galois group G). We can view this field as contained in $\overline{\mathbb{Q}}$, and then as required, view the latter as embedded once and for all into both $\overline{\mathbb{Q}}_p$ and $\mathbb{C}$.

We recall for motivation, the complex Artin L-function:

$$L(\rho, s) = \prod_q \det(1 - \mathrm{Frob}_q^{-1} \cdot q^{-s} | V_\rho^{I_q})^{-1}.$$

It is possible to define a set of local epsilon factors, $e_q(\rho) \in \mathbb{C}^*$, normalized in a particular manner worked out by Deligne. We will not bother to define these factors here and refer advanced readers to Deligne's somewhat technical article.

Now it is possible to define a complex L-function associated with the elliptic curve E, twisted by the representation ρ.

For a prime l distinct from q, consider the Tate module $T_l(E) = \varprojlim E_{l^n}$ and let $V_l(E) = T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, and $H_l^1(E) = \mathrm{Hom}(V_l(E), \mathbb{Q}_l)$.

Now fix a prime λ in K_ρ above l, and let $V_{\rho,\lambda} = V_\rho \otimes_{K_\rho} K_{\rho,\lambda}$, where $K_{\rho,\lambda}$ is the completion of K_ρ at λ.

Now we can define

$$L(E, \rho, s) = \prod_q \det(1 - \mathrm{Frob}_q^{-1} \cdot q^{-s} | (H_l^1(E) \otimes_{\mathbb{Q}_l} V_{\rho,\lambda})^{I_q})^{-1}.$$

Unfortunately the following is still a conjecture.

Conjecture 3.0.10. *$L(E, \rho, s)$ can be continued to $s = 1$ for all Artin characters ρ of G (it converges only for Re $(s) > 3/2$).*

Now fix a global minimal Weierstrass model for E over $\mathbb{Z}$. Let ω be the Nèron differential of this equation. Let γ^+ (γ^- resp.) denote a generator of the subspace of $H_1(E(\mathbb{C}), \mathbb{Z})$ fixed by complex conjugation (resp. on which complex conjugation acts by -1).

Let $\Omega_+(E) = \int_{\gamma^+} \omega$, $\Omega_-(E) = \int_{\gamma^-} \omega$.

Let $d^+(\rho)$, $d^-(\rho)$ be the dimensions of the subspaces of V_ρ on which complex conjugation acts by $+1, -1$ respectively.

With these definitions, the following conjecture, if true, ought to define a p-adic L-function, whose only 'parameter' is the representation ρ.

Conjecture 3.0.11.

$$\frac{L(E, \rho, 1)}{\Omega_+(E)^{d^+(\rho)}\Omega_-(E)^{d^-(\rho)}} \in \overline{\mathbb{Q}},$$

for all Artin representations ρ of G.

Let j_E denote the j-invariant of E. Let R be the set of primes q with $\mathrm{ord}_q(j_E) < 0$.

Let $L_R(E, \rho, s)$ be as for $L(E, \rho, s)$ but with the product only over primes not in R.

Put p^{f_p} equal the p-part of the conductor of ρ.

Since E is ordinary at p,

$$1 - a_pX + pX^2 = (1 - uX)(1 - wX), \quad u \in \mathbb{Z}_p^\times,$$

with $p + 1 - a_p = \#(\tilde{E}_p(\mathbb{F}_p))$, for $\tilde{E}_p$ the reduction of E modulo p.

Now in order to make sense of the following conjecture, we need to understand how an element of $K_1(\Lambda(G)_{S^*})$ can be thought of as a p-adic L-function.We consider such an element as a function defined on Artin representations ρ of G, as follows.

Firstly we note that the representation ρ gives us a map from $\mathbb{Z}_p[G/U]$, for any finite quotient G/U of G, to an $n \times n$ matrix over various extension fields of $\mathbb{Q}_p$. So that we don't have to work over fields that vary depending on ρ we can simply embed into $\mathbb{C}_p$, the completion of an algebraic closure of $\mathbb{Q}_p$.

Next we note that such representations are coherent, giving a map from Λ to $n \times n$ matrices over $\mathbb{C}_p$. This map extends to $\Lambda(G)_{S^*}$. Now we take K_1 of this map. We then make use of the fact that the K_1-group of a matrix ring over $\mathbb{C}_p$ is naturally isomorphic to K_1 of $\mathbb{C}_p$ itself, which is in fact naturally isomorphic to the units of $\mathbb{C}_p$.

Thus in reality we have a map for each element of $K_1(\Lambda(G)_{S^*})$ to the units of $\mathbb{C}_p$ depending only only the representation ρ. This map can be thought of as a p-adic L-function.

Conjecture 3.0.12. *Assuming $p \geq 5$ and E has good ordinary reduction at p, then there exists an $\mathcal{L}_E$ in $K_1(\Lambda(G)_{S^*})$ such that for all Artin representations ρ of G, $\mathcal{L}_E(\rho) \neq \infty$ and*

$$\mathcal{L}_E(\rho) = \frac{L_R(E, \rho, 1)}{\Omega_+(E)^{d^+(\rho)}\Omega_-(E)^{d^-(\rho)}} \cdot e_p(\rho) \cdot Q \cdot u^{-f_p},$$

where

$$Q = \frac{det(1 - Frob_q^{-1} \cdot u^{-1} | V_{\hat{\rho}}^{I_q})}{det(1 - Frob_q^{-1} \cdot w^{-1} | V_\rho^{I_q})},$$

and $\hat{\rho}$ is the contragredient representation:

$$\hat{\rho}(g) = {}^t\rho(g^{-1}).$$

At last we come to our goal - the main conjecture of GL_2 Iwasawa theory.

Conjecture (Main Conjecture) 3.0.13. *Assume $p \geq 5$ and E has good ordinary reduction at p. Assume $X(E/F_\infty)$ belongs to $\mathfrak{M}_H(G)$ as conjectured earlier. Then given that the previous conjecture holds, the p-adic L-function $\mathcal{L}_E$ in $K_1(\Lambda(G)_{S^*})$ is a characteristic element of $X(E/F_\infty)$.*

References

[1] Björk, J.-E. *Rings of differential operators.* North-Holland Mathematical Library, 21. North-Holland Publishing Co., Amsterdam-New York, 1979.

[2] Coates, J.; Fukaya, T.; Kato, K.; Sujatha, R.; Venjakob, O. *The GL_2 main conjecture for elliptic curves without complex multiplication.* Preprint

[3] Coates, J.; Schneider, P.; Sujatha, R. *Modules over Iwasawa algebras.* J. Inst. Math. Jussieu 2 (2003), no. 1, 73–108.

[4] Greenberg, Ralph *Iwasawa theory—past and present.* Class field theory—its centenary and prospect (Tokyo, 1998), 335–385, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001.

[5] Greenberg, Ralph *Introduction to Iwasawa theory for elliptic curves.* Arithmetic algebraic geometry (Park City, UT, 1999), 407–464, IAS/Park City Math. Ser., 9, Amer. Math. Soc., Providence, RI, 2001.

[6] Venjakob, Otmar *On the Iwasawa theory of p-adic Lie extensions.* Compositio Math. 138 (2003), no. 1, 1–54.

[7] Venjakob, Otmar *A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory. With an appendix by Denis Vogel.* J. Reine Angew. Math. 559 (2003), 153–191.

[8] Venjakob, Otmar *On the structure theory of the Iwasawa algebra of a p-adic Lie group.* J. Eur. Math. Soc. (JEMS) 4 (2002), no. 3, 271–311.

[9] Ochi, Yoshihiro; Venjakob, Otmar *On the structure of Selmer groups over p-adic Lie extensions.* J. Algebraic Geom. 11 (2002), no. 3, 547–580.

[10] Yager, Rodney I. *On two variable p-adic L-functions.* Ann. of Math. (2) 115 (1982), no. 2, 411–449.

E-mail address: `wbhart@math.leidenuniv.nl`