# FROM CLASSICAL TO NON-COMMUTATIVE IWASAWA THEORY AN INTRODUCTION TO THE $GL_2$ MAIN CONJECTURE

OTMAR VENJAKOB

This paper, which is an extended version of my talk 'The $GL_2$ main conjecture for elliptic curves without complex multiplication' given on the 4ECM, aims to give a survey on recent developments in non-commutative Iwasawa theory. It is written mainly for non-experts and does not contain neither proofs nor any new results, but hopefully serves as introduction to the original articles [4, 33]. Also, technical details are sometimes placed into footnotes in order to keep the main text as easily accessible as possible.

## 1. Classical Iwasawa theory

For the motivation of non-commutative Iwasawa theory it might be helpful to first go back to the origin of classical Iwasawa theory starting in some sense with the work of Kummer on cyclotomic fields.

The ideal class group $Cl(K)$ of a number field $K$ measures the failure of unique factorisation into prime elements in its ring of integers $O_K$. It was Kummer who observed that the vanishing of $Cl(\mathbb{Q}(\zeta_p))$, where $\zeta_p$ denotes a primitive $p$th root of unity for a fixed odd prime $p$, implies that the famous equation

$$x^p + y^p = z^p$$

only has trivial solutions in $\mathbb{Z}$.[1] In fact, it is even sufficient that only the $p$-primary part $A_1 := Cl(\mathbb{Q}(\zeta_p))(p)$ of the ideal class group vanishes; in this case $p$ is called *regular*, otherwise *irregular*. Thus, if all prime number would be regular the proof of Fermat's last theorem would have been rather easy. Hence, it was important for Kummer to be able to tell the regular from the irregular primes and he found the following criterion which reveals a mysterious relationship between $A_1$ and certain special values of the complex Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}},$$

*Date*: October 3, 2005.

This survey was written during a stay at Centro de Investigacion en Matematicas (CIMAT), Mexico, as a Heisenberg fellow of the Deutsche Forschungsgemeinschaft (DFG) and I want to thank these institutions for their hospitality and financial support, respectively.

[1] Indeed, after adjoining $\zeta_p$ the right hand side decomposes into the product of pairwise prime elements $x + \zeta_p^i y$, $i = 0, \ldots, p-1$, in $\mathbb{Z}[\zeta_p]$; the ideal class group being zero we can now consider the equation prime by prime showing that $z$ must be the product of $p$ pairwise prime numbers $z_i$ which leads to a contradiction as is easily shown, see [35].

where the Euler product ranges over all prime numbers and converges for $\Re(s) > 1$.

**Theorem 1.1** (Kummer)**.** *$A_1$ is trivial if and only if $p$ does not divide any of the numerators of the values $\zeta(-1), \zeta(-3), \ldots, \zeta(4-p)$.*[2]

For example the first four irregular primes are $37, 59, 67, 103$ and in contrast to the regular ones it is known that there exist infinitely many of them.

Now it was Iwasawas idea to study more general the ($p$-primary) ideal class groups $A_n := Cl(k_n)(p)$ of the fields $k_n = \mathbb{Q}(\mu_{p^n})$ which arise by adjoining the $p^n$th root of unities $\mu_{p^n}$ to $\mathbb{Q}$, both in order to understand better Kummers criterion and to see whether the order of $A_n$ could be at least controlled in view of Fermat's last theorem. Studying the ideal class groups for the whole tower of number fields $k_n$ simultaneously leads naturally to considering the infinite Galois extension $\mathbb{Q}_\infty := \mathbb{Q}(\mu_{p^\infty})$ of $\mathbb{Q}$ whose Galois group $\mathcal{G}$ is given explicitly by the cyclotomic character $\chi : \mathcal{G} \xrightarrow{\cong} \mathbb{Z}_p^\times$, i.e. $\zeta^g = \zeta^{\chi(g)}$ for all $g \,\epsilon\, \mathcal{G}$ and $\zeta \,\epsilon\, \mu_{p^\infty}$. We write $\mathbb{Q}_{cyc}$ for the unique subextension whose Galois group is isomorphic to $\mathbb{Z}_p \cong 1 + p\mathbb{Z}_p \subseteq \mathbb{Z}_p^\times$ and denote the corresponding Galois group by $\Gamma$. We fix a topological generator $\gamma$, say $1+p$, of $\Gamma$. Also we set $\Delta := G(k_1/\mathbb{Q})$ and note that $\mathcal{G} \cong \Gamma \times \Delta$. Iwasawa was not only interested in the size of $A_n$ but also in the finer structure of the ideal class group as Galois module. The natural Galois action on $A_n$ for all $n$ extends naturally to an action of the *Iwasawa algebra* $\Lambda := \Lambda(\mathcal{G})$, i.e. the completed group algebra

$$\mathbb{Z}_p[[\mathcal{G}]] := \varprojlim_n \mathbb{Z}_p[G(k_n/\mathbb{Q})],$$

on the projective limit

$$X := \varprojlim_n A_n.$$

In fact, Iwasawa showed that $X$ is a finitely generated $\Lambda$-torsion module. Since $\Lambda \cong \mathbb{Z}_p[\Delta][[\Gamma]]$ decomposes into a finite product of rings[3] each of which is isomorphic to the power series ring $\mathbb{Z}[[T]]$ in one variable $T = \gamma - 1$ there is a nice structure theory which assigns to any $\Lambda$-torsion module $M$ a *characteristic polynomial* $F_M$ (with coefficients in $\mathbb{Z}_p[\Delta]$), see 3.2 for more details. Neglecting for simplicity the $\mathbb{Z}_p$-torsion part of $M$, $F_M$ can be interpreted as the characteristic polynomial of the endomorphism $T$ acting on the free $\mathbb{Q}_p[\Delta](= \prod_{i=1}^{p-1} \mathbb{Q}_p)$-module $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. This $F_X$ will be used to define the *algebraic* $p$-adic zeta function below.

On the other hand, Kummer had shown mysterious congruences between the values of the modified $\zeta$-function

$$\zeta_{(p)}(s) := (1 - p^{-s})\zeta(s)$$

with the Euler factor at $p$ eliminated, which turn out to be equivalent to the existence of a continuous function $\zeta_{p-adic} : \mathbb{Z}_p \setminus \{1\} \to \mathbb{Q}_p$ such that $\zeta_{p-adic}(1-n) = \zeta_{(p)}(1-n)$ for all $n > 1$. Remember that already Euler knew that for $n > 1$ the values $\zeta(1-n)$ are

[2] Note that $\zeta$ has trivial zeroes at the even negative integers, also the numerator of $\zeta(2-p)$ is never divisible by $p$. The proof of this theorem relies decisively on the analytic class number formula and a decomposition of $A_1$ and the zeta function of $\mathbb{Q}(\zeta_p)$ into eigenspaces and $L$-functions with respect to the powers $\omega^i$ of the Teichmueller character $\omega : G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mu_{p-1}$, respectively.

[3] corresponding to the characters $\omega^i$ of $\Delta$.

rational and thus can also be considered as elements of the local field $\mathbb{Q}_p$. Furthermore, Kubota and Leopold showed that $\zeta_{p-adic}$ can be expanded into a $p$-adic power series, thus being $p$-adic analytic. As Iwasawa observed $\zeta_{p-adic}$ can also be interpreted as an element of $Q(\mathcal{G})$, the total ring of fractions of $\Lambda$.[4] First note that every continuous character $\psi : \mathcal{G} \to \mathbb{Z}_p^\times$ extends linearly to a ring homomorphism $\Lambda \to \mathbb{Z}_p$ which we also call $\psi$ by abuse of language. Apart from some bad denominators this map extends also to $Q(\mathcal{G})$. In particular, elements $Z \in Q(\mathcal{G})$ can be considered as functions on certain subsets of the set of continuous characters of $\mathcal{G}$ by setting $Z(\psi) := \psi(Z)$, if the latter is defined.

**Theorem 1.2** (Iwasawa, Kubota, Leopoldt)**.** *There exists a unique element $Z \in Q(\mathcal{G})$ such that*

$$Z(n) := Z(\chi^n) = \zeta_{(p)}(1-n)$$

*for all $k > 1$.*

Note that $Z(n)$ is zero for all odd $n$ due to the trivial zeroes of the Riemann zeta function. Also, by decomposing the cyclotomic character into the product of its projections onto $1 + p\mathbb{Z}_p$ and $\mu_{p-1}$, respectively, one can extend $Z$ to $p$-adic analytic functions $Z_{\omega^i}(s), s \in \mathbb{Z}_p \setminus \{1\}$. [5] Alternatively, $Z$ is determined by an interpolation property with respect to Dirichlet characters instead of powers of the cyclotomic character. In this case the Dirichlet $L$-functions are involved.

In some sense generalizing the analytic class number formula Iwasawa detected a deep relationship between the "$p$-adic families" of ideal class groups $A_n$, namely $X$, on the algebraic side and of special values of $\zeta$, namely $Z$ on the ($p$-adic) analytic side, which he formulated in the following classical

**Main Conjecture (Theorem of Mazur and Wiles)** There is the following equality of ideals in $\Lambda$ :

$$(F_{\mathbb{Z}_p(1)} \cdot Z) = (F_{X^+}).$$

Here $\mathbb{Z}_p(1) := \varprojlim_n \mu_{p^n}$ denotes the Tate-module and, due to the trivial zeroes of $Z$, one only has to consider the $+1$-eigenspace $X^+$ of $X$ with respect to complex conjugation.In particular, the denominator of $Z$ is controlled by $F_{\mathbb{Z}_p(1)}$. More heuristically, the main conjecture should be read as an identity in $Q(\mathcal{G})$

$$Z = \frac{F_{X^+}}{F_{\mathbb{Z}_p(1)}}$$

up to units in $\Lambda$.[6]

[4] $Q(\mathcal{G})$ is isomorphic to the product $\prod_{i=1}^{p-1} Q(\mathbb{Z}_p[[T]])$ of fields of fractions of $\mathbb{Z}_p[[T]]$.

[5] More precisely, the $Z_{\omega^i}$ are the $p$-adic versions of the complex $L$-functions $L(\omega^i, s)$.

[6] This can be read as an alternating product of the characteristic polynomials of the action of $\gamma$ on certain étale cohomology groups with coefficients in $\mathbb{Z}_p(1)$ which identify with the $\Lambda$-modules $\mathbb{Z}_p(1)$ and $X^+$. This is analogous to the function field situation, namely the fact that the zeta function of a curve $C$ over a finite field $\mathbb{F}$, $l \neq p$, can be expressed by means of the Lefschetz fix point formula using the action of the Frobenius endomorphism (instead of $\gamma$) on the étale cohomology of $C$. It was

While this classical theory concerned the multiplicative group $\mathbb{G}_m$ - we adjoined the points of its $p$-primary torsion subgroup to $\mathbb{Q}$ and considered the Galois modules $\mathbb{Z}_p(1)$ and $X^+$ which can be interpreted as Galois cohomology groups with coefficients in $\mathbb{Z}_p(1)$ - we will explain the corresponding theory for an elliptic curve $E$ over $\mathbb{Q}$ in the following sections.

**References:** [35, 22, 21, 8]

## 2. Iwasawa theory of elliptic curves - the philosophy

### 2.1. Arithmetic of elliptic curves.

In order to explain the Iwasawa theory of elliptic curves we first recall basic facts on (the arithmetic of) elliptic curves. To this end let $E$ be an elliptic curve over $\mathbb{Q}$, i.e. a smooth projective curve of genus one with a distinguished $\mathbb{Q}$-rational point (the 0 of the underlying abelian group). Every such $E$ can be realized in $\mathbb{P}^2$ by a (non-unique) Weierstrass equation of the form

$$W : y^2 = x^3 + Ax + B, \quad A, B \,\epsilon\, \mathbb{Z}$$

the distinguished point being the point at infinity.

For every prime $l$ this equation also defines a (not necessarily smooth) curve over the local field $\mathbb{Q}_l$ and the finite field $\mathbb{F}_l$, respectively. One of the basic questions concerning the arithmetic of $E$ is to determine the structure and in particular the size of the group

$$E(K) = \ ?$$

of $K$-rational points of $E$, i.e. the set of solutions of the equation (W) with coordinates in $K$, for $K$ any number field, local field or finite field. Over a number field, e.g. $K = \mathbb{Q}$, there is the famous

**Theorem 2.1** (Mordell-Weil). *The abelian group $E(\mathbb{Q})$ is finitely generated, i.e. it decomposes into*

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tors}},$$

*where $r = rk_{\mathbb{Z}} E(\mathbb{Q})$ is the rank of the Mordell-Weil group or the* algebraic rank *of $E$, while $E(\mathbb{Q})_{\mathrm{tors}}$ is the* finite *torsion subgroup.*

While the possible structures of $E(\mathbb{Q})_{\mathrm{tors}}$ where determined by Mazur, in particular, the order of this group is bounded by 16, it is not known whether the rank can be arbitrarily large when $E/\mathbb{Q}$ varies. The properties of the Mordell-Weil group turn out to be, at least conjecturally, deeply related with $L$-functions, which we are going to recall now. For every prime $l$ we denote by $\widetilde{E}_l$ the reduction of $E$ modulo $l$, i.e. the curve which is given by the reduced equation

$$\widetilde{W} : y^2 = x^3 + \widetilde{A}x + \widetilde{B}, \quad \widetilde{A}, \widetilde{B}, \,\epsilon\, \mathbb{F}_l.$$

this prototype which motivated Iwasawa to find a similar interpretation for the $p$-adic analytic zeta function. The non-trivial contribution of the étale cohomology comes from the jacobian of $C$, which is paralleled by the ideal class group in the number field case. Moreover, the extension from $\mathbb{F}$ to its algebraic closure is achieved by adjoining roots of unity, which corresponds to taking the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

Here we assume that the Weierstrass equation (W) is a (global) minimal model of $E$ over $\mathbb{Z}$, i.e. for all primes $l$ the $l$-part of the integer $\Delta := -16(4A^3+27B^2)$ (*the discriminant*) is minimal with respect to all Weierstrass equations over the $l$-adic integers $\mathbb{Z}_l$ which give rise to the same isomorphism class of elliptic curves. If $\widetilde{E}_l$ is again a smooth curve over $\mathbb{F}_l$, then $E$ is said to have *good* (otherwise *bad*) reduction at $l$. In the previous case the integer $a_l$ is defined by

$$\#\widetilde{E}_l(\mathbb{F}_l) = 1 - a_l + l.$$

Otherwise $\widetilde{E}_l$ has either a node, i.e. *multiplicative* reduction, or a cusp, i.e. *additive* reduction. In the second case we set $a_l = 0$ while in the first case we set $a_l = 1$ if the multiplicative reduction is *split*, i.e. the tangent lines to the node on $\widetilde{E}_l$ have slopes defined over $\mathbb{F}_l$, and $a_l = -1$ if the reduction is *non-split.* Then the complex *Hasse-Weil L-function* of $E$ is defined by the following Euler product

$$L(E/\mathbb{Q}, s) := \prod_l \left(1 - a_l l^{-s} + \epsilon(l) l^{1-2s}\right)^{-1},\ s \,\epsilon\, \mathbb{C},\ \Re(s) > \frac{3}{2},$$

where $\epsilon(l)$ equals by definition 1, if $E$ has good reduction at $l$, and 0 otherwise. By the work of Wiles and Taylor-Wiles it is known that $L(E/\mathbb{Q}, s)$ has an analytic continuation to the entire complex plane. The following conjecture, which is a generalization of the analytic class number formula for number fields, predicts that the *analytic rank* of $E$, i.e. the vanishing order of $L(E/\mathbb{Q}, s)$ at $s = 1$, coincides with the *algebraic rank.* Moreover, the leading coefficient of the Taylor series expansion of the $L$-function at $s = 1$ can be expressed by the most important invariants of $E$ : By Ш$(E/\mathbb{Q})$ we denote the *Tate-Shafarevich group* of $E$, which is conjectured to be finite though this is not known for a single elliptic curve. If $<,>$ denotes the height pairing of $E$ and $P_1, \ldots, P_r$ form some set of generators of $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tor}}$, then the *regulator* of $E$ is defined to be the determinant of the matrix $(< P_i, P_j >)_{i,j}$. Further, if we assume that (W) is a global minimal model of $E$ over $\mathbb{Z}$, then the translation invariant holomorphic differential

$$\omega := \frac{dx}{2y}$$

is called the *Néron Differential* of $E$. The integration of it along a generator $\gamma^+$ of the real part $\pi_1(E(\mathbb{C}), 0)^+ := \pi_1(E(\mathbb{C}), 0)^{G(\mathbb{C}/\mathbb{R})}$ of the fundamental group of the complex manifold $E(\mathbb{C})$ defines the *real period*

$$\Omega_+ = \int_{\gamma^+} \omega$$

of $E$. Similarly, the period $\Omega_-$ is defined via integration along a generator $\gamma_-$ of the $-1$ eigenspace of the fundamental group with respect to the action of complex conjugation. Finally, for any prime $l$ we call *Tamagawa-number* at $l$ the index $c_l = [E(\mathbb{Q}_l) : E^{ns}(\mathbb{Q}_l)]$ of the subgroup $E^{ns}(\mathbb{Q}_l)$ of the group of $\mathbb{Q}_l$-rational points $E(\mathbb{Q}_l)$ consisting of those points whose reduction modulo $l$ is non-singular.

**Conjecture 2.2** ( Birch & Swinnerton-Dyer (BSD) Conjecture)**.**

$$\text{I.} \qquad r := \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q})$$

$$\text{II.} \qquad \lim_{s \to 1} (s-1)^r L(E/\mathbb{Q}, s) = \Omega_+ R_E \frac{\#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2} \prod_l c_l$$

Note that the product over the Tamagawa numbers is actually finite as $C_l = 1$ whenever $E$ has good reduction at $l$.

Thus this conjecture describes a mysterious relationship between the complex analytic $L$-function and the purely algebraically defined Mordell-Weil group. A similar conjecture can be formulated for elliptic curves over arbitrary number fields. The idea of Iwasawa theory is roughly speaking to study this deep connection between the values of (complex) $L$-functions and arithmetic invariants of $E$ for a full tower of number fields simultaneously as we have already seen in section 1.

**References:** [28, 29]

2.2. **The Selmer group of $E$ in towers of number fields.** For technical reasons we make from now on the following

*Assumption:* $p \geq 5$ is a prime such that $E$ has *good ordinary* reduction at $p$, i.e. the order of the group of $p$-division points $\widetilde{E}_p(\overline{\mathbb{F}_p})[p]$ equals $p$.

To study the Mordell-Weil group of $E$ it is often more convenient to go over to the cohomologically defined ($p$-primary) *Selmer group* $Sel(E/K)$ for any finite extension $K/\mathbb{Q}$. Instead of giving the precise definition we just recall that induced by Kummer theory the Selmer group fits into the following short exact sequence, being the bridge between the ($p$-primary) Tate-Shafarevich group and the Mordell-Weill group:

$$\begin{tikzcd} 0 \arrow[r] & E(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \arrow[r] & Sel(E/K) \arrow[r] & \text{Ш}(E/K)(p) \arrow[r] & 0 . \end{tikzcd}$$

Assuming $\#\text{Ш}(E/K)(p) < \infty$, which can be checked - for fixed $p$ - in many cases, it holds for the Pontryagin dual of the Selmer group

$$X(E/K) := Sel(E/K)^{\vee} := \mathrm{Hom}(Sel(E/K), \mathbb{Q}_p/\mathbb{Z}_p),$$

that

$$\mathrm{rk}_{\mathbb{Z}} E(K) = \mathrm{rk}_{\mathbb{Z}_p} X(E/K).$$

Thus, indeed, the Selmer group (or its dual) bears significant arithmetic information of $E$.

Now we introduce a canonical tower of number fields associated with $E$. By $E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$ we denote the $p^n$-division points of $E$ over a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. The action of the absolute Galois group $G_{\mathbb{Q}}$ on this group induces, after choosing a basis, the representation

$$\rho_{p^n} : G_{\mathbb{Q}} \longrightarrow Aut(E[p^n]) \cong GL_2(\mathbb{Z}/p^n\mathbb{Z}).$$

We define $K_n := \mathbb{Q}(E[p^n]), 0 \leq n < \infty$, to be the maximal subfield of $\overline{\mathbb{Q}}$ fixed under the kernel of $\rho_{p^n}$. Then $K_\infty := \bigcup_{n \geq 0} K_n$ is nothing else then the fixed field under the kernel of the representation

$$\rho_{p^\infty} : G_{\mathbb{Q}} \longrightarrow Aut_{\mathbb{Z}_p}(T_pE) \cong GL_2(\mathbb{Z}_p)$$

of $G_{\mathbb{Q}}$ on the Tate module

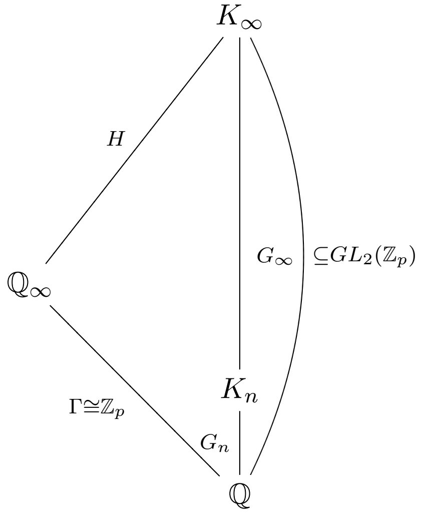
$$T_pE := \varprojlim_n E[p^n],$$

where the inverse limit is formed with respect to the multiplication by $p$ maps. In particular, $K_\infty$ is a Galois extension of $\mathbb{Q}$ with Galois group $G := G(K_\infty/\mathbb{Q})$ isomorphic to a closed subgroup of $GL_2(\mathbb{Z}_p)$. Thus $G$ is a $p$-adic Lie group. We want to stress that the $L$-function of $E$ only depends on the Galois representation $\rho_{p^\infty}$, thus the tower of number fields $\{K_n\}_n$ is most natural in order to study the arithmetic of $E$, in particular, to investigate properties of its $L$-function.

Note that due to the Weil pairing $\det \circ \rho$ is isomorphic to the cyclotomic character $\chi : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_p^\times$ which describes the action of $G_{\mathbb{Q}}$ on the $p$-power roots of unity $\mu_{p^\infty} : g\zeta = \zeta^{\chi(g)}$ for all $g \,\epsilon\, G_{\mathbb{Q}}$ and $\zeta \,\epsilon\, \mu_{p^\infty}$. Thus $K_\infty$ contains the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$. We write $H$ for the Galois group $G(K_\infty/\mathbb{Q}_\infty)$ and obtain the diagram sidewards.
As before the *Iwasawa algebra* of $G$

$$\Lambda(G) = \varprojlim_n \mathbb{Z}_p[G_n]$$

is the inverse limes of the group algebras $\mathbb{Z}_p[G_n]$ of $G_n$ with coefficients in $\mathbb{Z}_p$. It is a compact, regular Noetherian ring. In contrast to the classical Iwasawa algebra $\Lambda(\Gamma)$ of $\Gamma$ it is *not commutative in general.*



Now, for every $n \geq 1$, the Galois action makes $X(E/K_n) := Sel(E/K_n)^\vee$ into a compact $\mathbb{Z}_p[G_n]$-module. To study, on the algebraic side, all these Selmer groups simultaneously for the whole tower of number fields means to go over to the inverse limit

$$X := X(E/K_\infty) := \varprojlim_n Sel(E/K_n)^\vee,$$

which turns out to be a finitely generated $\Lambda(G)$-module, conjecturally even a *torsion* $\Lambda(G)$-module. Roughly one should think of it as the family of all the Mordell-Weil groups $E(K_n)$ (and Tate-Shafarevich groups $Ш(E/K_n)(p)$). The analytic counterpart of this family will be discussed in the next subsection.

**References:** [2, 5, 23, 24, 13]

2.3. **Twisted $L$-functions.** For every $n \geq 0$, let $\mathrm{Irr}(G_n)$ denote the set of isomorphism classes of (absolutely) irreducible representations of $G_n$, realized over an appropriate number field embedded into $\mathbb{C}$ or over a local field contained in $\overline{\mathbb{Q}_l}$ (depending on $n$). Via the canonical projection $G \twoheadrightarrow G_n$ they are also considered as representations of $G$, to which we shall refer as *Artin representation.* Let $R$ be the finite set of primes of $\mathbb{Q}$ containing $p$ and all primes $l$ at which $E$ has bad reduction.

On the analytic side one is searching for a function $\mathcal{L}_E$, the *$p$-adic analytic $L$-function of $E$* , on the set $\bigcup_n \mathrm{Irr}(G_n)$ which assigns to $\rho$ the value at $s = 1$ of the complex $L$-function $L(E, \rho, s)$ of $E$ twisted by $\rho$ or rather its modified version $L_R(E, \rho, s)$ with the Euler factors at primes in $R$ eliminated. [7] [8]

Heuristically, summarizing the (generalized) BSD conjecture over all the fields $K_n$ leads directly to the Iwasawa Main Conjecture of $E$[9]. Since the (modified) $L$-function $L_R(E/K_n, s)$ of $E$ over $K_n$ (similarly defined as over $\mathbb{Q}$ and without the Euler factors in $R$) decomposes into the product of twisted $L$-functions (with multiplicities), the idea is that on the analytic side of the picture the family of special values at $s = 1$ of $L_R(E, \rho, s)$ can be interpolated $p$-adically, which should lead to the *$p$-adic analytic $L$-function.* On the other hand on the algebraic side there should be some procedure to assign to the $\Lambda(G)$-module $X = X(E/K_\infty)$ (as for any torsion $\Lambda(G)$-module) some *characteristic element* $F_X$ bearing hopefully many arithmetic information of $E$. The (heuristic) comparison of the algebraic and analytic aspect when going over to towers of number fields are illustrated in the following diagram

[7] we restrict to those primes not lying in $R$, because the corresponding factors at primes in $R$ usually do not behave well $p$-adically and thus have to be eliminated from the usual definition of the $L$-function in order to expect a $p$-adic $L$-function in whatever sense.

[8] For the interested reader we recall the definition of $L_R(E, \rho, s)$. Again it is defined as an Euler product, which converges only for $\Re(s) > \frac{3}{2}$,

$$L_R(E, \rho, s) := \prod_{q \notin R} P_q(E, \rho, q^{-s})^{-1}, \quad s \in \mathbb{C},$$

where the $P_q(E, \rho, T)$ are polynomials to be defined below. The only thing known about its analytic continuation at present is that it has a meromorphic continuation when $\rho$ factors through a soluble extension of $\mathbb{Q}$. We will assume the analytic continuation of $L(E, \rho, s)$ to $s = 1$ for all Artin characters $\rho$ of $G$ in what follows. If $q$ is any prime number we write $\mathrm{Frob}_q$ for the Frobenius automorphism of $q$ in $G(\overline{\mathbb{Q}_q}/\mathbb{Q}_q)/I_q$, where, as usual, $I_q$ denotes the inertia subgroup. Assume now that $\rho \in \mathrm{Irr}(G_n)$ is realized on a vector space $V_\rho$ over a number field $K$ of dimension $n_\rho$. For a fixed place $\lambda$ of $K$ lying above $l \neq q$ we denote by $K_\lambda$ the completion of $K$ with respect to $\lambda$ and we set

$$V_{\rho,\lambda} = V_\rho \otimes_K K_\lambda.$$

Also we consider the $l$-adic Tate module $V_l E := H_1(E(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}_l \cong T_l E \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ and set

$$H_l^1(E) := \mathrm{Hom}(V_l E, \mathbb{Q}_l).$$

Finally we put for any prime $l$ different from $q$

$$P_q(E, \rho, T) := \det(1 - \mathrm{Frob}_q^{-1}.T | (H_l^1(E) \otimes_{\mathbb{Q}_l} V_{\rho,\lambda})^{I_q}).$$

It can be shown that for $\rho$ the trivial representation the local $L$-function $P_q(E, p^{-s}) := P_q(E, \rho, p^{-s})$ coincides with the Euler factor at $q$ of the Hasse-Weil $L$-function of $E$. In particular, the integers $a_q$ are just the traces of $\mathrm{Frob}_q$ acting on the maximal unramified quotient $(V_l E)_{I_q}$ of the Tate module.

[9] In fact this can be made precise in the context of the Equivariant Tamagawa Number Conjecture (ETNC), a natural generalisation of the BSD conjecture, see [11], also [1, 16].

| **algebraic** | **analytic** |
|---|---|
| $X(E/K_n)$<br>as $G_n$-module | $L_R(E/K_n) = \prod_{\mathrm{Irr}(G_n)} L_R(E,\rho,s)^{n_\rho}$ |
| **$p$-adic families** | |
| $X(E/K_\infty)$ | $(L_R(E,\rho,1))_{\rho\ \epsilon\ \mathrm{Irr}(G_n),n<\infty}$ |
| **$p$-adic $L$-functions** | |
| $F_E := F_X$<br>characteristic element | $\mathcal{L}_E$<br>analytic $p$-adic $L$-function |

This comparison culminates in the

**Main Conjecture:** $F_E \equiv \mathcal{L}_E,$

which says that the characteristic element of $E$ and the $p$-adic analytic $L$-functions (if they exist at all) are essentially the same, in a sense we have to make precise later. If such a relation should hold it must be a very deep relationship since it connects two totally different aspects of $E$ living in completely different worlds and in some sense ”explaining” the mysterious BSD-conjecture.

We conclude this section by illustrating the analogy between the $\mathbb{G}_m$- and the $E$-case:

| $\mathbb{G}_m$ | $E$ |
|---|---|
| $\zeta(s)$ | $L(E,s)$ |
| $\mathbb{Q}(\mu_{p^\infty})$ | $\mathbb{Q}(E[p^\infty])$ |
| $Cl(k_n)$ | $E(K_n)$ |
| $X^+$ | $X(E/K_\infty)$ |
| $\zeta_{p-adic}$ | $\mathcal{L}_E$ |

## 3. Iwasawa theory of elliptic curves - recent developments

3.1. **What is new?** Before we try to describe different approaches to make the philosophy explained above precise we would like to mention that we have to distinguish two totally different cases. Consider the following explicit elliptic curves

$$E_1 : y^2 = x^3 - x$$

and

$$E_2 : y^2 + y = x^3 - x^2.$$

At a first glance who would expect an essentially difference between them? But while the first one has a ”big” ring of endomorphisms - one can show that $\mathrm{End}(E_1) \cong \mathbb{Z}[i] \neq \mathbb{Z}$, i.e. $E$ admits complex multiplication (CM) - the second one only has the endomorphisms arising from multiplication with integers: $\mathrm{End}(E_2) \cong \mathbb{Z}$, i.e. $E$ does *not* admit complex multiplication.

Now it follows that in the *CM-case,* the group $G$ has the form

$$G \cong {\mathbb{Z}_p}^2 \times \text{finite abelian group},$$

in particular it is *abelian.* This commutative theory is rather well known, the 2-*variable main conjecture*[10] is a Theorem of Rubin [25] in many cases, see also at the end of 3.5.

Thus we want to concentrate on the second, the $GL_2$-*case.* By a deep result of Serre [27] now $G$ is of the form

$$G \subseteq_o GL_2(\mathbb{Z}_p) \quad \text{open subgroup},$$

in particular it is *not abelian.*

In this case it was not even known how to formulate a $GL_2$ *main conjecture* and it is this case were the substantial progress we want to describe in these notes has been achieved recently. This development concerns unfortunately only the algebraic side of the picture drawn above, in particular, the *existence of characteristic elements* has been established, while the $p$-adic analytic part will be purely conjectural.

We also should mention that there is a well-developed (commutative) Iwasawa theory of elliptic curves over the $\mathbb{Q}_\infty$, [19, 12, 20]We refer to the corresponding main conjecture as 1-*variable main conjecture.* For CM-elliptic curves this is consequence of the 2-variable main conjecture. In the non-CM case there are partial results by Kato [17] and recent results by Urban and Skinner [**?**], which together prove the latter main conjecture in several cases.

3.2. **Structure Theory.** In this section let $G$ be any compact $p$-adic Lie group without element of order $p$ ($G$ can always be realized as an closed subgroup of $GL_n(\mathbb{Z}_p)$ for some $n$).

In order to define the characteristic element of a $\Lambda(G)$-module it is tempting to imitate the approach of classical Iwasawa theory, i.e. the case where

$$G \cong {\mathbb{Z}_p}^n$$

and thus there is an isomorphism $\Lambda = \Lambda(G) \cong \mathbb{Z}_p[[X_1, \ldots, X_n]]$ for any choice of a minimal system of topological generators $\gamma_1, \ldots, \gamma_n$ of $G$ by the identities $X_i = \gamma_i - 1$. In particular, $\Lambda(G)$ is a complete, regular local ring of dimension $n+1$. In the case $n = 1$ it was Iwasawa himself - and more generally for integrally closed (commutative) domains Serre - who established a structure theorem, similar to that concerning modules over principal ideal domains: Every finitely generated $\Lambda(G)$-torsion module $M$ is up to pseudo-null modules a direct product of cyclic modules

$$M \sim \prod_i \Lambda/\Lambda f_i^{n_i},$$

[10] Since $G$ has dimension 2 as $p$-adic Lie group the $p$-adic $L$-function is a power series in two variables.

where $n_i$ are uniquely defined integers and $f_i$ are irreducible elements of $\Lambda(G)$, unique up to units. The pseudo-null[11] modules have to be considered as small - in fact, for $n = 1$ they are precisely the class of all finite modules - and the idea is that they do not contribute essential information in the arithmetic applications. Now one defines the characteristic element using the above invariants attached to $M$

$$F_M := \prod f_i^{n_i}.$$

Returning to the general case, i.e. to a not necessarily commutative group $G$, the concept of *pseudo-null* modules was developped in the authors thesis [30, 31, 34] by cohomological methods establishing the fundamental fact that $\Lambda(G)$ is an Auslander regular ring, for details see (loc. cit.). Then Coates, Schneider and Sujatha went on establishing a structure theorem in this non-commutative setting almost totally parallel to the above mentioned theory.

**Theorem 3.1** (Coates, Schneider, Sujatha)**.** *For every torsion $\Lambda$-module $M$ there exist left ideals $L_1, \ldots, L_r$ such that, up to pseudo-null modules, $M$ decomposes into a product of cyclic modules*

$$M \sim \prod_{i=1}^{r} \Lambda/L_i.$$

For details and the mild technical further assumption on $G$ needed in this theorem, see [7] and [3]. Unfortunately, it turned out that the $G$-Euler characteristic, an important arithmetic invariant if e.g. applied to the Selmer group and which will be defined later, is not invariant under pseudo-isomorphisms[12]. Moreover, the ideals $L_i$ occurring above need not be principal in general (see [32, appendix] for a counterexample). Thus, at moment, the theorem cannot be used to attach an characteristic element to $M$ and it is still not clear which role this astonishing structure result will play in non-commutative Iwasawa theory. In order to circumvent this dilemma we are going to apply techniques from algebraic $K$-theory and localisation of (possibly non-commutative) rings.

**References:** [7, 6, 22, 15, 14, 32, 26]

3.3. **Localisation of Iwasawa algebras and characteristic elements.** The following theory stems from joint work of Coates, Fukaya, Kato and Sujatha with the author [4] and makes heavily use of the following

*Assumption:* There exists a normal closed subgroup $H \trianglelefteq G$ such that the quotient $\Gamma := G/H$ is isomorphic to $\mathbb{Z}_p$.

Recall that it is satisfied in our application because $K_\infty$ contains the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_{cyc}$ of $\mathbb{Q}$.

In this situation we are able to define a multiplicatively closed subset $\mathcal{T}$[13] consisting of non-zerodivisors of $\Lambda := \Lambda(G)$ hoping that one can localize $\Lambda$ with respect to it.

[11] A finitely generated $\Lambda(G)$-module $M$ is *pseudo-null* if its support has codimension at least 2 in the spectrum of $\Lambda(G)$.

[12] A homomorphism of modules whose kernel and cokernel are pseudo-null

[13] First define $\mathcal{T}' := \{\lambda \in \Lambda | \Lambda/\Lambda\lambda$ finitely generated over $\Lambda(H)\}$ and then saturate it with the powers of $p$, i.e. $\mathcal{T} := \bigcup_{i \geq 0} p^i \mathcal{T}' \subseteq \Lambda$.

While this is always possible for commutative rings this is a quite subtle issue for *non-commutative* rings: one has to check that $\mathcal{T}$ satisfies the Ore-condition, which means roughly speaking that every right fraction with denominator in $\mathcal{T}$ can also be written as left fraction, and vice-versa. If the localisation with respect to $\mathcal{T}$ exists, it should be related - by construction - to the following subcategory of the category of $\Lambda$-torsion modules:

$\mathfrak{M}_H(G)$ category of $\Lambda$-modules $M$ such that modulo $\mathbb{Z}_p$-torsion $M$ is finitely generated over $\Lambda(H) \subseteq \Lambda(G)$.

Thus, from a technical point of view the following theorem is the key result of our construction:

**Theorem 3.2.** *The localization $\Lambda_{\mathcal{T}}$ of $\Lambda$ with respect to $\mathcal{T}$ exists and there is a surjective map arising from $K$-theory*[14]

$$\partial : (\Lambda_{\mathcal{T}})^{\times} \twoheadrightarrow K_0(\mathfrak{M}_H(G))$$

*from the group of units $(\Lambda_{\mathcal{T}})^{\times}$ of $\Lambda_{\mathcal{T}}$ to the Grothendieck group $K_0(\mathfrak{M}_H(G))$ of $\mathfrak{M}_H(G)$.*

This leads directly to the following

**Definition 3.3.** Any $F_M \,\epsilon\, (\Lambda_{\mathcal{T}})^{\times}$ with $\partial[F_M] = [M]$ is called *characteristic element* of $M \,\epsilon\, \mathfrak{M}_H(G)$.

In order to show that this is not just a sophisticated but useless definition we state some basic properties of our construction. In particular, $F_M$ behaves well with Euler characteristics.

### Properties

(i) Any $f \,\epsilon\, (\Lambda_{\mathcal{T}})^{\times}$ can be interpreted as a map on the isomorphism classes of (continuous) representations $\rho : G \to Gl_n(\mathcal{O}_K)$, where $O_K$ runs through the ring of integers of finite extensions $K$ of $\mathbb{Q}_p$ :

$$\rho \mapsto f(\rho) \,\epsilon\, K \cup \{\infty\} \subseteq \overline{\mathbb{Q}_p} \cup \{\infty\}.$$

(ii) The evaluation of $F_M$ at $\rho$ gives the generalized $G$-Euler characteristic[15] $\chi(G, M(\rho))$

$$|F_M(\rho)|_p^{-[K:\mathbb{Q}_p]} = \chi(G, M(\rho))$$

[14] There is an exact localization sequence

$$\begin{tikzcd}
\Lambda^{\times} \arrow[d, two heads] & (\Lambda_{\mathcal{T}})^{\times} \arrow[d, two heads] & & \\
K_1(\Lambda) \arrow[r] & K_1(\Lambda_{\mathcal{T}}) \arrow[r, "\partial"] & K_0(\mathfrak{M}_H(G)) \arrow[r] & 0,
\end{tikzcd}$$

where the surjectivity claims need little arguments, see [4, §4].

[15] Note that with $M$ also every twist $M(\rho) := M \otimes_{\mathbb{Z}_p} \mathcal{O}_K^n$ (with diagonal $G$-action, via $\rho$ on the right factor) belongs to $\mathfrak{M}_H(G)$. By definition, $\chi(G, M(\rho)) := \prod_{i \geq 0} \left(\#\mathrm{H}_i(G, M(\widehat{\rho}))\right)^{(-1)^i}$, if all groups are finite and where $\widehat{\rho}$ denotes the contragredient representation of $\rho$.

if the Euler-characteristic is defined. Here the $p$-adic valuation is normalized as usual by $|p|_p = \frac{1}{p}$.

For more details and proofs, see [4, § 3],[33, §8].

3.4. **Numerical Example.** Consider the two elliptic curves

$$\begin{aligned} E = X_1(11) \quad &: \quad y^2 + y = x^3 - x^2, \\ A \quad &: \quad y^2 + y = x^3 - x^2 - 7820x - 263580 \end{aligned}$$

and let $p = 5$. One can show that $X \epsilon \mathfrak{M}_H(G)$, i.e. that $F_X$ exists. Now $G = G(\mathbb{Q}(E(5))/\mathbb{Q})$ has 2 irreducible Artin Representations of degree 4 :

$$\rho_i = \mathrm{Ind}\chi_i : G \to GL_4(\mathbb{Z}_5),$$

which are in fact induced by the characters $\chi_i$, $i = 1, 2$, corresponing to the cyclic extensions of degree 5 as indicated in the following diagram

$$\begin{tikzcd}
\mathbb{Q}(E[5]) \arrow[dr, dash, "\chi_1"'] & & \mathbb{Q}(A[5]) \arrow[dl, dash, "\chi_2"] \\
& \mathbb{Q}(\mu_5) \arrow[d, dash] & \\
& \mathbb{Q} &
\end{tikzcd}$$

Calculations show that $\chi(G, X(\rho_i))$ equals $5^3$ and 5 for $i = 1$ and $i = 2$, respectively. Thus

$$F_X(\rho_1) \sim 5^3, \;\; F_X(\rho_2) \sim 5$$

up to $\mathbb{Z}_5^\times$.

3.5. **Analytic $p$-adic $L$-function and the $GL_2$-main conjecture.** In contrast to the algebraic theory above the following analytic part is purely conjectural. First of all we have Delignes [9]

**Period - Conjecture:** $$\frac{L_R(E, \rho, 1)}{\Omega(E, \rho)} \epsilon \bar{\mathbb{Q}}$$

for a suitable period $\Omega(E, \rho) \epsilon \mathbb{C}$, which permits to consider $\frac{L_R(E,\rho,1)}{\Omega(E,\rho)}$ as value in $\bar{\mathbb{Q}}_p$, i.e. in the same target where the elements of $(\Lambda(G)_\mathcal{T})^\times$ interpreted as functions take their values. In analogy with classical Iwasawa theory we call such an element which interpolates these values *$p$-adic analytic $L$-function* though one could criticize that there is no $p$-adic analysis involved at present.

**Conjecture 3.4** (Existence of analytic $p$-adic $L$-function)**.** *Let $p \geq 5$ and assume that $E$ has good ordinary reduction at $p$. Then there exists*

$$\mathcal{L}_E \; \epsilon \; (\Lambda(G)_\mathcal{T})^\times,$$

*such that for all Artin representations $\rho$ of $G$ one has $\mathcal{L}_E(\rho) \neq \infty$ and*

$$\mathcal{L}_E(\rho) \sim \frac{L_R(E,\rho,1)}{\Omega(E,\rho)}$$

*up to some modifications of the Euler factor at $p$.*

The precise formula[16] describing the interpolation property can be deduced from Fukaya and Kato's version[17] of the Equivariant Tamagawa Number Conjecture (ETNC) together with their $\epsilon$-conjecture and thus follows a precise recipe whose explanation is unfortunately out of the scope of this article. In particular, the following version of a non-commutative Iwasawa main conjecture is compatible with the ETNC corresponding to our tower $K_n$ of number fields:

**Conjecture 3.5** (Main Conjecture). *Assume that $p \geq 5$, $E$ has good ordinary reduction at $p$, and $X(E/K_\infty)$ belongs to $\mathfrak{M}_H(G)$. Granted the existence of the $p$-adic $L$-function, $\mathcal{L}_E$ is a characteristic element of $X(E/K_\infty)$ :*

$$\partial[\mathcal{L}_E] = [X(E/K_\infty)].$$

Before we discuss evidence for this conjectures we would like to comment on some of its implications. Assuming the existence of $\mathcal{L}_E$, one can show

(i) that the $GL_2$-main conjecture implies the 1-variable main conjecture (over $\mathbb{Q}_{cyc}$).

(ii) that, assuming also the $GL_2$-main conjecture, it holds

$$\chi(G, X(\rho)) \text{ finite } \Leftrightarrow L_R(E,\rho,1) \neq 0.$$

In this case one has with $m_\rho := [K : \mathbb{Q}_p]$ :

$$\chi(G, X(\rho)) = |\mathcal{L}_E(\rho)|_p^{-m_\rho}.$$

(iii) that, if $L(E,1) \neq 0$, by results of Kolyvagin the groups $E(\mathbb{Q})$ and $\text{Ш}(E/\mathbb{Q})$ are finite and the $p$-part of the BSD conjecture (II.) holds:

$$\frac{L(E/\mathbb{Q},1)}{\Omega_+} \sim_p \frac{\#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q}))^2} \prod_l c_l$$

up to $\mathbb{Z}_p^\times$.

[16] Since $E$ is ordinary at $p$, we have $P_p(E,1,T) = 1 - a_pT + pT^2 = (1-uT)(1-wT)$ with $u \,\epsilon\, \mathbb{Z}_p^\times$. We put $p^{f_\rho} = p$-part of conductor of $\rho$, and denote by $e_p(\rho)$ the local $\varepsilon$-factor of $\rho$ at $p$. Finally we set $P_p(\rho,T) := \det(1 - \mathrm{Frob}_q^{-1}.T|V_\rho^{I_p})$. Then the interpolation formula is

$$\mathcal{L}_E(\rho) = \frac{L_R(E,\rho,1)}{\Omega(E,\rho)} \cdot e_p(\rho) \cdot \frac{P_p(\hat{\rho},u^{-1})}{P_p(\rho,w^{-1})} \cdot u^{-f_\rho},$$

where $\Omega(E,\rho) = \Omega_+(E)^{d^+(\rho)}\Omega_-(E)^{d^-(\rho)}$ while $d^+(\rho)$ and $d^-(\rho)$ denote the dimension of the subspace of $V_\rho$ on which complex conjugation acts by $+1$ and $-1$, respectively (see [4, 5.7]).

[17] The original ETNC was formulated by Burns and Flach [1] inspired by [18]. A different version of an Iwasawa main conjecture (without $p$-adic $L$-functions) was discussed by Huber and Kings [16]

We conclude this survey by giving some evidence for Main Conjecture:

In the *CM-case* the existence of $\mathcal{L}_E$ follows from the existence of the 2-variable $p$-adic $L$-function (Manin-Vishik [], Katz [**?**], Yager [36]). If $X \epsilon \mathfrak{M}_H(G)$, then the main conjecture follows from the 2-variable main conjecture (Rubin,Yager).

In the $GL_2$*-case* almost nothing is known! There is only weak numerical evidence by calculations of T. and V. Dokchitser [10]. Let $E = X_1(11)$, $p = 5$, and $\rho_i$, $i = 1, 2$, be the two unique irreducible Artin representations of degree 4 as before. Then they verify that the relation

$$\chi(G, X(\rho_i)) = |\mathcal{L}_E(\rho_i)|_p^{-1}, \quad i = 1, 2$$

holds as is predicted by the main conjecture, see above. Here $\mathcal{L}_E(\rho_i)$ denotes the term describing the interpolation property of $\mathcal{L}_E$ if the $p$-adic $L$-function should exist.

## References

1. D. Burns and M. Flach, *Tamagawa numbers for motives with (non-commutative) coefficients*, Doc. Math. **6** (2001), 501–570 (electronic). 9, 17
2. J. Coates, *Fragments of the $GL_2$ Iwasawa theory of elliptic curves without complex multiplication.*, Arithmetic theory of elliptic curves. Lectures given at the 3rd session of the Centro Internazionale Matematico Estivo (CIME), Cetraro, Italy, July 12-19, 1997., LNM, vol. 1716, Springer, 1999, pp. 1–50. 2.2
3. ______, *Iwasawa algebras and arithmetic*, Astérisque (2003), no. 290, Exp. No. 896, vii, 37–52. 3.2
4. J. Coates, T. Fukaya, K. Kato, R. Sujatha, and O. Venjakob, *The $GL_2$ main conjecture for elliptic curves without complex multiplication*, preprint (2004). (document), 3.3, 14, 3.3, 16
5. J. Coates and S. Howson, *Euler characteristics and elliptic curves II*, J. Math. Soc. Japan **53** (2001), 175–235. 2.2
6. J. Coates, P. Schneider, and R. Sujatha, *Links between cyclotomic and $GL_2$ Iwasawa theory*, to appear in Doc. Math. 3.2
7. ______, *Modules over Iwasawa algebras*, J. Inst. Math. Jussieu **2** (2003), no. 1, 73–108. 3.2
8. Pierre Colmez, *Fonctions L p-adiques*, Astérisque (2000), no. 266, Exp. No. 851, 3, 21–58. 1
9. P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, Automorphic forms, representations and $L$-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 313–346. 3.5
10. T. Dokchitser and V. Dokchitser, in preparation, no. 2004. 3.5
11. T. Fukaya and K. Kato, *A formulation of conjectures on p-adic zeta functions in non-commutative Iwasawa theory*, preprint (2003). 9
12. R. Greenberg, *Iwasawa theory for elliptic curves.*, Arithmetic theory of elliptic curves. Lectures given at the 3rd session of the Centro Internazionale Matematico Estivo (CIME), Cetraro, Italy, July 12-19, 1997., LNM, vol. 1716, Springer, 1999, pp. 51–144. 3.1
13. Y. Hachimori and O. Venjakob, *Completely faithful Selmer groups over Kummer extensions*, Documenta Math. **Extra Volume: Kazuya Kato's Fiftieth Birthday** (2003), 443–478. 2.2
14. S. Howson, *Euler characteristics as invariants of Iwasawa modules*, Proc. London Math. Soc. (3) **85** (2002), no. 3, 634–658. 3.2
15. ______, *Structure of central torsion Iwasawa modules*, Bull. Soc. Math. France **130** (2002), no. 4, 507–535. 3.2

16. A. Huber and G. Kings, *Equivariant Bloch-Kato conjecture and non-abelian Iwasawa main conjecture*, Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002) (Beijing), Higher Ed. Press, 2002, pp. 149–162. 9, 17
17. K. Kato, *Hodge Theory and Values of Zeta Functions of Modular Forms*, appears in: Astérisque. 3.1
18. ______, *Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via $B_{\mathrm{dR}}$. I*, Arithmetic algebraic geometry (Trento, 1991), Lecture Notes in Math., vol. 1553, Springer, Berlin, 1993, pp. 50–163. 17
19. B. Mazur, *Rational points of Abelian varieties with values in towers of number fields.*, Invent. Math. **18** (1972), 183–266. 3.1
20. B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61. 3.1
21. B. Mazur and A. Wiles, *Class fields of Abelian extensions of $\mathbb{Q}$.*, Invent. Math. **76** (1984), 179–330. 1
22. J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundlehren der mathematischen Wissenschaften, vol. 323, Springer, 2000. 1, 3.2
23. Y. Ochi and O. Venjakob, *On the structure of Selmer groups over p-adic Lie extensions*, J. Algebraic Geom. **11** (2002), no. 3, 547–580. 2.2
24. ______, *On the ranks of Iwasawa modules over p-adic Lie extensions*, Math. Proc. Cambridge Philos. Soc. **135** (2003), 25–43. 2.2
25. K. Rubin, *On the main conjecture of Iwasawa theory for imaginary quadratic fields.*, Invent. Math. **93** (1988), no. 3, 701–713. 3.1
26. P. Schneider and O. Venjakob, *On the dimension theory of skew power series rings*, preprint (2004). 3.2
27. J.-P. Serre, *Proprietes galoisiennes des points d'ordre fini des courbes elliptiques. (Galois properties of points of finite order of elliptic curves).*, Invent. Math. **15** (1972), 259–331. 3.1
28. Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 199? 2.1
29. John T. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206. 2.1
30. O. Venjakob, *Iwasawa theory of p-adic Lie extensions.*, Ph.D. thesis, Heidelberg: Univ. Heidelberg, Naturwissenschaftlich-Mathematische Gesamtfakultät, 112 p. , 2000. 3.2
31. ______, *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. 3.2
32. ______, *A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory*, J. reine angew. Math. **559** (2003), 153–191. 3.2
33. ______, *Characteristic Elements in Noncommutative Iwasawa Theory*, Habilitationsschrift eingereicht bei der Fakultät für Mathematik und Informatik der Ruprecht-Karls-Universität Heidelberg (2003). (document), 3.3
34. ______, *Iwasawa Theory of p-adic Lie Extensions*, Compos. Math. **138** (2003), no. 1, 1–54. 3.2
35. L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. 1, 1
36. R. I. Yager, *On two variable p-adic L-functions.*, Ann. Math., II. Ser. **115** (1982), 411–449. 3.5

Universität Heidelberg, Mathematisches Institut, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany.

*E-mail address*: otmar@mathi.uni-heidelberg.de

*URL*: http://www.mathi.uni-heidelberg.de/~otmar/