Iwasawa theory and generalizations

Kazuya Kato

Abstract. This is an introduction to Iwasawa theory and its generalizations. We discuss some main conjectures and related subjects.

Mathematics Subject Classification (2000). Primary 11R23; Secondary 11G40, 14G10.

Keywords. Iwasawa theory, zeta function.

Zeta values are infinitely attractive objects. They appear in many areas of mathematics, and also in physics. They lead us to the profound mysteries of mathematics.

Iwasawa theory is the best theory at present to understand the arithmetic meaning of zeta values. Classical Iwasawa theory describes the relation between zeta values and ideal class groups. It has been generalized to the study of the relation between zeta values and more general arithmetic objects (rational points and Selmer groups of elliptic curves, Galois representations, Galois cohomology groups, ...). Diagrammatically, we have

$$\begin{array}{ccc} \text{zeta values} & \longleftrightarrow & \text{ideal class groups, Selmer groups, } \ldots. \\ \text{(analytic objects)} & & \text{(arithmetic objects)} \end{array}$$

The mysterious point is that analytic objects and arithmetic objects are connected in spite of the vast distance between their innate natures. Via zeta values, arithmetic, algebra, analysis, geometry intersect. Deep and unexpected problems arise there.

The aim of this paper is to review some results, methods, and problems in Iwasawa theory and its generalizations. The author regrets that he cannot cover many important studies in this field.

The organization of this paper is as follows. In §1, we describe history. In §2, we describe the cyclotomic Iwasawa theory of elliptic curves comparing it with classical Iwasawa theory. In §3, we present non-commutative Iwasawa theory.

The author is very grateful to Professor John Coates for advice.

1. Overview

1.1. Euler. The study of zeta values was started by Euler. In 1735, Euler proved $1 + 1/2^2 + 1/3^2 + 1/4^2 + 1/5^2 + \cdots = \pi^2/6$. He was happy that he solved the

Proceedings of the International Congress
of Mathematicians, Madrid, Spain, 2006

difficult question "what is the sum of the inverses of all squares?" and also that the answer he found (the appearance of π) was surprising.

Riemann's zeta function $\zeta(s)$ is defined as $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ for complex numbers s such that $\Re(s) > 1$, and by analytic continuation, it is extended to the whole complex s-plane as a meromorphic function which is holomorphic at any $s \neq 1$. The above result of Euler says that $\zeta(2) = \pi^2/6$.

Euler proved that $\zeta(4) = \pi^4/90$, $\zeta(6) = \pi^6/945$, and more generally, for any even integer $r \geq 2$, he showed that $\zeta(r)/\pi^r \in \mathbb{Q}$. Euler did not know the theory of analytic continuation, but he had a method to find the correct values of $\zeta(s)$ at integers ≤ 0:

$$\zeta(0) = -1/2, \quad \zeta(r) = 0 \text{ for any even integer } r < 0,$$

$$\zeta(1-r) = 2 \cdot (r-1)! \cdot \zeta(r)/(2\pi i)^r \in \mathbb{Q}^\times \text{ if } r > 0 \text{ is even},$$

$$\zeta(-1) = -1/12, \ \zeta(-3) = 1/120, \ \zeta(-5) = -1/(2^2 \cdot 3^2 \cdot 7),$$

$$\zeta(-7) = 1/(2^4 \cdot 3 \cdot 5), \ \zeta(-9) = -1/(2^2 \cdot 3 \cdot 11), \ \zeta(-11) = 691/(2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13), \ldots.$$

Note that the prime number 691 suddenly appears as the numerator of $\zeta(-11)$.

1.2. Kummer. In the middle of 19th century, Kummer discovered that the special values of the Riemann zeta function have the following remarkable arithmetic properties: (1) a relation with the arithmetic of cyclotomic fields, and (2) a p-adic property. Neither could possibly be imagined from the analytic definition of $\zeta(s)$. These discoveries (1), (2) were the starting point of Iwasawa theory.

(1) *Kummer's criterion.* Let p be a prime number. Then p divides the numerator of $\zeta(r)$ for some negative odd integer r if and only if the class number of $\mathbb{Q}(\zeta_p)$ is divisible by p.

This (1) for example shows that the class number of $\mathbb{Q}(\zeta_{691})$ is divisible by 691 since the numerator of $\zeta(-11)$ is divisible by 691.

Recall that for a number field F (a finite extension of $\mathbb{Q}$) the class number of F is the order of the ideal class group $\mathrm{Cl}(F)$ of F, which is a finite group. We recall that the ideal class group of F is defined to be the quotient of the multiplicative group of non-zero fractional ideals of F divided by the subgroup consisting of principal ideals. It is the most important group in algebraic number theory. Unique factorization into prime elements in F holds if and only if $\mathrm{Cl}(F) = \{1\}$, and the failure of unique factorization in F becomes big (and the arithmetic of F becomes complicated) if the ideal class group of F is big. Kummer tried to prove Fermat's last theorem by studying the arithmetic of cyclotomic fields $\mathbb{Q}(\zeta_p)$ for odd primes p (where we denote by ζ_n a primitive n-th root of 1). The equation $x^p + y^p = z^p$ is rewritten as $\prod_{k=1}^{p}(x+\zeta_p^k y) = z^p$ in the multiplicative form, and hence the theory of multiplicative factorization in $\mathbb{Q}(\zeta_p)$ becomes important. Kummer proved that if the class number of $\mathbb{Q}(\zeta_p)$ is not divisible by p (so that the multiplicative arithmetic of $\mathbb{Q}(\zeta_p)$ becomes sufficiently simple), $x^p + y^p = z^p$ has no non-zero integral solution. This was the

most important result on Fermat's last theorem before the complete proof of Wiles by a different method.

Thus the ideal class group is a "bitter group" which seems to prevent the study of the arithmetic of number fields. But the above criterion (1) of Kummer shows that the ideal class group is in fact a "sweet group" which has a wonderful relation with zeta values.

I add that this study of Kummer was the start of the theory of ideals which became later important in algebraic number theory, algebraic geometry, and many areas of mathematics.

I add also that the final solution of Fermat's last theorem by Wiles [45] also uses the arithmetic of zeta values (generalized Iwasawa theory) of symmetric squares of modular forms.

(2) *Kummer's congruence.* If r is a negative odd integer and $r \not\equiv 1 \bmod (p-1)$, then $\zeta(r) \in \mathbb{Z}_{(p)} = \{m/n \mid (n, p) = 1\}$. If r' is also a negative odd integer and $r' \equiv r \bmod (p-1)$, then $\zeta(r') \equiv \zeta(r) \bmod p$.

On the other hand, if r is a negative odd integer such that $r \equiv 1 \bmod (p-1)$, p divides the denominator of $\zeta(r)$. Hence the results (1), (2) and the above list of $\zeta(0), \ldots, \zeta(-11)$ already show that the class number of $\mathbb{Q}(\zeta_p)$ is not divisible by p if $p = 3, 5, 7, 11, 13$, and hence $x^p + y^p = z^p$ has no non-zero integral solution for these p according to the result of Kummer. Kummer's congruence was generalized later to congruences modulo higher powers of p.

1.3. Class number formula. The class number formula of Dirichlet and Dedekind proved in the middle of 19th century is also a mysterious relationship between zeta functions and ideal class groups. Let F be a number field, and let $\zeta_F(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$ ($\Re(s) > 1$) be the Dedekind zeta function of F, where $\mathfrak{a}$ ranges over all non-zero ideals of the integer ring O_F of F and $N(\mathfrak{a})$ denotes the norm of $\mathfrak{a}$. Then $\zeta_F(s)$ has a meromorphic analytic continuation to the whole of $\mathbb{C}$ and is holomorphic at $s \neq 1$. If $F = \mathbb{Q}$, then $\zeta_F(s) = \zeta(s)$. The class number formula has the form

$$\lim_{s \to 0} \frac{1}{s^{r_1+r_2-1}} \zeta_F(s) = -\frac{h_F R_F}{w_F}.$$

Here h_F is the class number of F, R_F is the regulator of F (defined by using log of units in O_F), w_F is the number of all roots of 1 in F, r_1 is the number of real places of F, and r_2 is the number of complex places of F.

The class number formula is the first example of many similar formulae, for example, the Iwasawa main conjecture, the Birch and Swinnerton-Dyer conjecture, etc., which all have the form

$$\text{analytic invariant} = \text{arithmetic invariant}.$$

1.4. Iwasawa theory. In the later half of 20th century, studies of mysterious properties of zeta values evolved into a fruitful field of mathematics, Iwasawa theory.

Compared with Kummer's criterion and class number formula, Iwasawa theory is finer in the point that it describes not only the class number, i.e. the order of the ideal class group, but also the action of the Galois group on the ideal class group. In fact, one could even say that the aim of Iwasawa theory is to describe Galois actions on arithmetic objects in terms of zeta values.

For example, as we have seen, by Kummer's criterion, $\zeta(-11) = 691/(\cdots)$ tells that for $p = 691$, the ideal class group of $\mathbb{Q}(\zeta_p)$ contains a subgroup which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. But what does -11 here mean? By Iwasawa theory (this part is due to Ribet [35]), this -11 tells that for $p = 691$, as a module over the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, the ideal class group $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ contains a submodule which is isomorphic to $(\mathbb{Z}/p\mathbb{Z})(-11)$, where for $r \in \mathbb{Z}$, $(\mathbb{Z}/p\mathbb{Z})(r)$ is a one-dimensional representation of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ over $\mathbb{Z}/p\mathbb{Z}$ on which $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ such that $\sigma(\zeta_p) = \zeta_p^c$ ($c \in (\mathbb{Z}/p\mathbb{Z})^\times$) acts as the multiplication by c^r.

The p-adic properties of values of the Riemann zeta function, which first appeared in Kummer's congruence, were summarized by Kubota and Leopoldt [24] as the existence of the p-adic Riemann zeta function which interpolates the zeta values $\zeta(r)$ ($r \in \mathbb{Z}, r \leq 0$) p-adically. Iwasawa showed that the p-adic zeta function was essentially an element of the Iwasawa algebra, and formulated the so-called Iwasawa main conjecture which has (roughly speaking) the form

$$p\text{-adic zeta function} = \text{ideal class group with Galois action.}$$

([20]; see 2.3.1 for the precise statement.) After efforts of Iwasawa, this conjecture was proved by Mazur–Wiles [32].

Wiles [44] exploiting the ideas of Hida, also proved the main conjectures for totally real fields. Moreover Rubin, using ideas of Kolyvagin, proved versions of Iwasawa's main conjecture for abelian extensions of imaginary quadratic fields ([37]). See, for example, [18] for discussions of various aspects of Iwasawa theory.

1.5. Elliptic curves. Recall that an elliptic curve E over a number field F is defined by an equation $y^2 = f(x)$ where $f(x)$ is a cubic polynomial over F without multiple root. The set $E(F) = \{(x, y) \in F \times F \mid y^2 = f(x)\} \cup \{(\infty, \infty)\}$ is endowed with the structure of an abelian group in which (∞, ∞) is the unit element, and the theorem of Mordell–Weil shows that $E(F)$ is finitely generated as an abelian group.

For example, for the elliptic curve $E\colon y^2 = x^3 + 1$ over $\mathbb{Q}$, if $P \in E(\mathbb{Q})$ denotes the point $(2, 3)$, then $2P = P + P = (0, 1)$, $3P = (-1, 0)$, $4P = (0, -1)$, $5P = (2, -3)$, $6P = (\infty, \infty)$, $\mathbb{Z}/6\mathbb{Z} \xrightarrow{\simeq} E(\mathbb{Q})$; $n \mapsto nP$. On the other hand, for the elliptic curve $y^2 = x^3 - 2$, if $P \in E(\mathbb{Q})$ denotes the point $(3, 5)$, then $\mathbb{Z} \xrightarrow{\simeq} E(\mathbb{Q})$; $n \mapsto nP$.

Zeta functions come to this arithmetic world. An elliptic curve E over a number field has its zeta function $L(E, s)$ (called the L-function of E). For $E\colon y^2 = x^3 + 1$ and $E\colon y^2 = x^3 - 2$ over $\mathbb{Q}$, the order of zero of $L(E, s)$ at $s = 1$ is 0 and 1, respectively, and is equal to the rank of $E(\mathbb{Q})$ as a finitely generated abelian group. Birch and Swinnerton-Dyer formulated the following conjecture [4].

Let E be an elliptic curve over a number field F. Then

(1) $\mathrm{ord}_{s=1} L(E, s) = \mathrm{rank}\,(E(F))$.

(2) Let $r = \mathrm{ord}_{s=1} L(E, s)$. Then

$$\lim_{s \to 1} (s-1)^{-r} L(E, s) = \frac{h_E R_E \Omega_E \tau_E}{w_E}$$

where on the right-hand side, h_E is the order of the Tate–Shafarevich group $Ш(E)$ of E (which is an elliptic curve analogue of the ideal class group and is conjectured to be finite), R_E is the discriminant of the height pairing, Ω_E is the period of E, w_E is the square of the order of the torsion part of $E(F)$, and τ_E is "Tamagawa factor" which is a certain local term and is a non-zero rational number.

This is the elliptic curve version of the class number formula.

The first great result on this conjecture was obtained by Coates and Wiles [10]. Their result shows that if E has complex multiplication by an imaginary quadratic field K and if F is $\mathbb{Q}$ or K, then $E(F)$ is finite provided that $L(E, 1) \neq 0$.

The proof of Coates and Wiles is p-adic and was inspired by Iwasawa's generalization of Kummer's ideas. The principle of their method is that if we replace $\zeta(s)$ in Iwasawa theory by $L(E, s)$, then we can obtain a strong result on the relation between $L(E, s)$ and arithmetic.

The conjecture of Birch and Swinnerton-Dyer does not have a p-adic shape at all, but it is often important in mathematics to watch the right-hand side (p-adic world) of

$$\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q} \subset \mathbb{Q}_p,$$

not only the left-hand side (Archimedean world). Zeta functions are able to travel to the p-adic world, and to understand their relation to arithmetic, it is important to study their lifestyles in the p-adic world by the method of Iwasawa theory.

Iwasawa theory of elliptic curves was started by Mazur, and the analogue of the Iwasawa main conjecture for elliptic curves over $\mathbb{Q}$ was formulated by him (see 2.3.2, [29]). This main conjecture is now almost proved as I will explain in § 2.

This main conjecture is for cyclotomic Iwasawa theory of elliptic curves. Iwasawa theory of elliptic curves for anti-cyclotomic abelian extensions of imaginary quadratic fields was developed by Bertolini and Darmon and others (see [3] for example).

Coates has led developments of non-commutative Iwasawa theory of elliptic curves (here the Galois groups are non-commutative). The main conjecture for it was formulated in Venjakob [43] and Coates et al. [8], and this will be explained in §3.

1.6. Generalizations. Iwasawa theory of motives and Iwasawa theory of modular forms are now formulated and studied.

For motives which are of good ordinary reduction at p, main conjectures were formulated by Greenberg [17] and Schneider [40].

The conjectures of the type "$R = T$" concerning Galois deformations ([31]), which are important for the construction of non-commutative class field theory (Langlands program) and for which the work of Wiles [45] was a great contribution, are also regarded as generalizations of Iwasawa's main conjecture.

A very general form of main conjectures in generalized Iwasawa theory is given as equivariant Tamagawa number conjectures (these conjectures grew in Deligne [12], Beilinson [2], Bloch–Kato [5], Fontaine and Perrin-Riou [15], Perrin-Riou [34], Kato [21] for commutative Iwasawa theory of motives, and then in Burns–Flach [7], Huber–Kings [19] for non-commutative Iwasawa theory of motives). In the formulation of equivariant Tamagawa number conjecture, the worlds through which zeta functions travel are extended as $\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q} \subset \mathbb{Q}_p \subset B_{\mathrm{dR}}$, where B_{dR} is the field of p-adic periods defined by Fontaine, which plays the role of complex numbers in p-adic Hodge theory (thus zeta functions now travel through Hodge theory and p-adic Hodge theory). The main conjecture presented in [19] in the previous ICM however did not involve p-adic zeta functions. The main conjecture in [43], [8] explained in § 3 involves p-adic zeta functions. The compatibility of this conjecture with the equivariant Tamagawa number conjecture is shown in [16].

In what follows, for the simplicity of description, we consider only Iwasawa theory for zeta functions associated to number fields and for zeta functions associated to elliptic curves. See [34], [16] etc. for more general motives.

2. Cyclotomic theory

We consider cyclotomic Iwasawa theory of elliptic curves, comparing it with classical Iwasawa theory. When we consider classical theory (resp. theory for elliptic curves), we will say that we are in Case I (resp. Case II). In Case II, assume we are given an elliptic curve E over $\mathbb{Q}$. Let p be a prime number. For simplicity of the description of the theory, we assume $p \neq 2$, and in Case II we assume that E has good ordinary reduction at p.

2.1. Arithmetic side

2.1.1. *Iwasawa algebras.* For a profinite group G, the completed group ring $\mathbb{Z}_p[[G]]$ is defined to be the inverse limit $\varprojlim_U \mathbb{Z}_p[G/U]$ of the usual group rings $\mathbb{Z}_p[G/U]$ where U ranges over all open normal subgroups of G. In the case $G = \mathrm{Gal}(L/F)$ for a Galois extension L of a number field F, the ring $\mathbb{Z}_p[[G]] = \varprojlim_{F'} \mathbb{Z}_p[\mathrm{Gal}(F'/F)]$, where F' ranges over all finite Galois extensions of F contained in L, is often called the Iwasawa algebra.

Let

$$\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_{p^n}), \quad \mathbb{Q}(\zeta_{p^\infty})^+ = \mathbb{Q}(\zeta_{p^\infty}) \cap \mathbb{R},$$

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})^+/\mathbb{Q}) \quad \text{in Case I}, \quad G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \quad \text{in Case II}.$$

Let $\Lambda = \mathbb{Z}_p[[G]]$. Then in Case I (resp. II), Λ is isomorphic to the product of $(p-1)/2$ (resp. $p-1$) copies of the ring $\mathbb{Z}_p[[T]]$ of formal power series in one variable over $\mathbb{Z}_p$.

2.1.2. *Iwasawa modules.* Modules over Iwasawa algebras having arithmetic importance are often called Iwasawa modules, for Iwasawa first studied such modules in his papers. We define an Iwasawa module X over Λ as follows.

First assume that we are in Case I. Let $X = \mathrm{Gal}(M/\mathbb{Q}(\zeta_{p^\infty})^+)$ where M is the largest abelian pro-p extension of $\mathbb{Q}(\zeta_{p^\infty})^+$ in which any prime number different from p is unramified. Then G acts on X via inner automorphisms, and by this action X is regarded as a Λ-module.

This module X can also be expressed in terms of ideal class groups as

$$X \simeq \mathrm{Hom}\,(\varinjlim_n \mathrm{Cl}(\mathbb{Q}(\zeta_{p^n}))^-, (\mathbb{Q}_p/\mathbb{Z}_p)(1)).$$

Here $\mathrm{Cl}(\mathbb{Q}(\zeta_{p^n}))^-$ is the part of $\mathrm{Cl}(\mathbb{Q}(\zeta_{p^n}))$ on which the complex conjugate acts as -1, and $(\mathbb{Q}_p/\mathbb{Z}_p)(1)$ denotes the group of all roots of 1 of p-power orders. This isomorphism is deduced from Kummer theory. It preserves Galois actions (on the right-hand side, an element σ of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ acts as $h \mapsto \sigma \circ h \circ \sigma^{-1}$). By this isomorphism and by the finiteness of the ideal class groups, we can show that X is a finitely generated torsion Λ-module ("torsion" means that each element of X is killed by some non zero-divisor in Λ).

2.1.3. Next assume that we are in Case II. For a number field K, we have an exact sequence

$$0 \to E(K) \otimes \mathbb{Q}/\mathbb{Z} \to \mathrm{Sel}(E/K) \to Ш(E/K) \to 0.$$

Here $\mathrm{Sel}(E/K)$ is the Selmer group of E over K which is a certain subgroup of the Galois cohomology group $H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})_{\mathrm{tor}})$, where $\overline{K}$ is the algebraic closure of K (= the algebraic closure of $\mathbb{Q}$) and $E(\overline{K})_{\mathrm{tor}}$ denotes the torsion part of $E(\overline{K})$. It is conjectured that the Tate–Shafarevich group $Ш(E/K)$ is always finite.

Define

$$X = \mathrm{Hom}\,(\varinjlim_n \mathrm{Sel}(E/\mathbb{Q}(\zeta_{p^n})), \mathbb{Q}_p/\mathbb{Z}_p).$$

Then X is regarded as a Λ-module via the natural action of G on it. It is a finitely generated Λ-module. Mazur conjectured that it is a torsion Λ-module, and this was proved in [22] (the case with complex multiplication is due to Rubin).

2.1.4. *Characteristic ideals.* For a finite abelian group (for example, for the ideal class group), the most important invariant is its order. For an Iwasawa module like X, the most important invariant is its characteristic ideal.

Recall that a finite abelian group M is isomorphic to a finite direct sum $\bigoplus_{i=1}^n \mathbb{Z}/(a_i)$ for non-zero integers $a_1, \ldots, a_n$, and the order $\sharp(M)$ of M is characterized by the equality $(\sharp(M)) = \left(\prod_{i=1}^n a_i\right)$ of ideals of $\mathbb{Z}$.

Now let R be a commutative ring which is isomorphic to a finite product of copies of $\mathbb{Z}_p[[T]]$, and let M be a finitely generated torsion R-module. Then there

are non zero-divisors $a_1, \dots, a_n$ of R and an injective homomorphism of R-modules $h\colon \bigoplus_{i=1}^n R/(a_i) \to M$ with finite cokernel. Define the characteristic ideal $\mathrm{Char}(M)$ of M as the principal ideal $\left(\prod_{i=1}^n a_i\right)$ of R. Then $\mathrm{Char}(M)$ is independent of the choices of $a_1, \dots, a_n$ and h as above.

2.2. Zeta side

2.2.1. Assume that we are in Case I. We review the p-adic Riemann zeta function.

Let $\kappa\colon \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \xrightarrow{\simeq} \mathbb{Z}_p^\times$ be the cyclotomic character, which is an isomorphism characterized by $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\kappa(\sigma)}$ ($\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$, $n \geq 1$). For an even integer r, the homomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \to \mathbb{Z}_p^\times;\ \sigma \mapsto \kappa(\sigma)^r$ factors through G, and we denote the induced homomorphism $G \to \mathbb{Z}_p^\times$ by κ^r.

For a commutative ring R, the total quotient ring is defined by

$$Q(R) = \left\{\tfrac{a}{b} \mid a, b \in R, b \text{ is a non zero-divisor}\right\}.$$

If R is an integral domain, $Q(R)$ is the field of fractions of R.

The p-adic Riemann zeta function ξ is the unique element of $Q(\Lambda)$ satisfying the following conditions (1) and (2):

(1) $(1-\sigma)\xi \in \Lambda$ for any $\sigma \in G$.

(2) For any even integer $r > 0$, the ring homomorphism $\Lambda \to \mathbb{Z}_p$ induced by $\kappa^r\colon G \to \mathbb{Z}_p^\times$ sends $(1-\sigma)\xi$ for $\sigma \in G$ to $(1-\kappa^r(\sigma))(1-p^{r-1})\zeta(1-r)$.

2.2.2. *Comparison with complex analysis.* The Riemann zeta function lives on the complex plane, but the p-adic Riemann zeta function lives in Galois theory. Though the complex plane and Galois theory are very much different, zeta can fly between these different worlds.

The ring Λ is the p-adic analogue of the ring A of all holomorphic functions on the complex plane. The total quotient ring $Q(\Lambda)$ is the p-adic analogue of the field $Q(A)$ of all meromorphic functions on the complex plane.

The p-adic Riemann zeta function $\xi \in Q(\Lambda)$ is the p-adic analogue of $\zeta(1-s) \in Q(A)$. For an even integer r, the ring homomorphism $\Lambda \to \mathbb{Z}_p;\ \sigma \mapsto \kappa^r(\sigma)$ ($\sigma \in G$) is the p-adic analogue of the ring homomorphism $A \to \mathbb{C};\ f \mapsto f(r)$. Let

$$I(A) = \{f \in A \mid f(0) = 0\}, \quad I(\Lambda) = \mathrm{Ker}\,(\Lambda \to \mathbb{Z}_p;\ \sigma \mapsto 1\ (\sigma \in G)).$$

Then $I(\Lambda)$ is a principal prime ideal of Λ and is generated by $1-\sigma$ for all $\sigma \in G$. The fact $I(\Lambda)\xi \subset \Lambda$ (2.2.1, (1)) is the p-adic analogue of the fact that $I(A)\zeta(1-s) \subset A$.

The understanding of the ideal $I(A)\zeta(1-s) = (s\zeta(1-s))$ of A is equivalent to the understanding of zeros of $\zeta(s)$ counting multiplicity. Riemann's hypothesis is a beautiful statement about zeros of $\zeta(s)$, but it is not yet proved. On the other hand, for the p-adic side, there is also a beautiful statement about the ideal $I(\Lambda)\xi$ of Λ. It is Iwasawa's main conjecture introduced in 2.3.1 below, which was proved by Mazur–Wiles [32].

2.2.3. Assume that we are in Case II. The complex L-function $L(E, s)$ of E is defined as the Euler product $L(E, s) = \prod_\ell P_\ell(\ell^{-s})^{-1}$ for $\Re(s) > 3/2$, where ℓ ranges over all prime numbers and $P_\ell(T)$ is a polynomial described as follows. If E has good reduction at ℓ, $P_\ell(T) = 1 - a_\ell T + \ell T^2$ with $a_\ell = 1 + \ell - \sharp(E(\mathbb{F}_\ell))$. If E has bad reduction at ℓ, $P_\ell(T)$ is either $1 - T$, or $1 + T$, or 1. We can write $L(E, s)$ in the form of a Dirichlet series $\sum_{n=1}^\infty a_n n^{-s}$.

By the solution of the Shimura–Taniyama conjecture by Wiles, Breuil, Conrad, Diamond, Taylor [6], $\sum_{n=1}^\infty a_n q^n$ is the q-expansion of a cusp form of weight 2. From this we can deduce that the L-function of E twisted by a Dirichlet character χ defined as $L(E, s, \chi) = \sum_{n=1}^\infty a_n \chi(n) n^{-s}$ has an analytic continuation to the whole of $\mathbb{C}$ as a holomorphic function.

The p-adic L-function $L_p(E)$ of E is defined in $\Lambda[1/p]$. A difference with the case of the Riemann zeta function is that $L(E, r) = 0$ for all $r \in \mathbb{Z}_{\leq 0}$ and these values are not useful for the p-adic interpolation. The element $L_p(E)$ in $\Lambda[1/p]$ is characterized in the following way:

For any $n \geq 1$ and any Dirichlet character $\chi : (\mathbb{Z}/p^n\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$, the ring homomorphism $\Lambda \to \overline{\mathbb{Q}}_p$ induced by $G \to \overline{\mathbb{Q}}_p^\times$; $\sigma \mapsto \chi(\sigma)$ sends $L_p(E)$ to $L(E, 1, \chi)/((\text{period}) \times (\text{local term}))$. Here we regard χ as a character of G via the cyclotomic character. For the definitions of (period) and (local term) see [30], for example.

2.3. Main conjecture

2.3.1. In Case I, the Iwasawa main conjecture proved by Mazur–Wiles is stated as

$$I(\Lambda)\xi = \mathrm{Char}(X).$$

Here $I(\Lambda)$ denotes $\mathrm{Ker}\,(\Lambda \to \mathbb{Z}_p; \sigma \mapsto 1\ (\sigma \in G))$ as in 2.2.2.

2.3.2. In Case II, the main conjecture formulated by Mazur is stated as

$$\Lambda L_p(E) = \mathrm{Char}(X).$$

(We recall that in Case II we assume that p is a good ordinary prime for E.)

2.3.3. The above conjecture of Mazur is now almost proved.

(1) Rubin [37]. If E has complex multiplication, then the conjecture is true.

(2) [22]. Assume E has no complex multiplication. Then there is $n \geq 0$ such that $\mathrm{Char}(X)$ divides $\Lambda p^n L_p(E)$. This n can be taken to be 0 under some mild assumptions. (Here "I divides J" means $J \subset I$.)

(3) Skinner and Urban [41]. Here to my present knowledge, the existence of some Galois representations associated to some automorphic forms on $U(2, 2)$ is

needed for the following result (but it seems that this existence will soon be proven).

$$\Lambda L_p(E) \text{ divides } \mathrm{Char}(X) \text{ under some mild assumptions.}$$

Ideas of the proofs of these results are sketched in the subsections 2.4 and 2.5.

2.3.4. We give some remarks on what is known about the Birch and Swinnerton-Dyer conjecture.

(1) In [25], Kolyvagin proved the following result.

If $\mathrm{ord}_{s=1} L(E, s) \leq 1$, then $\mathrm{ord}_{s=1} L(E, s) = \mathrm{rank}\,(E(\mathbb{Q}))$ and $Ш(E)$ is finite.

(2) If $L(E, 1) \neq 0$, we can deduce from the main conjecture 2.3.2 that the ratio of the left side and the right side in part (2) of the Birch Swinnerton-Dyer conjecture stated in §1.5 is a rational number which is a p-adic unit.

(3) There is a p-adic analogue of the Birch and Swinnerton-Dyer conjecture ([30]) which states that

$$\mathrm{ord}_{s=1} L_p(E) = \mathrm{rank}\,(E(\mathbb{Q})).$$

Here $\mathrm{ord}_{s=1} L_p(E)$ is the order (valuation) of the image of $L_p(E)$ in the local ring of Λ at the prime ideal $I(\Lambda) = \mathrm{Ker}\,(\Lambda \to \mathbb{Z}_p; \sigma \mapsto 1)$, which is a discrete valuation ring.

From the above result 2.3.3 (2), we can obtain that

$$\mathrm{rank}\,(E(\mathbb{Q})) \leq \mathrm{ord}_{s=1} L_p(E).$$

However for the original Birch and Swinnerton-Dyer conjecture, we do not have such general inequality, for the relation of $\mathrm{ord}_{s=1} L(E, s)$ and $\mathrm{ord}_{s=1} L_p(E)$ are not yet determined (although they are conjectured to be equal). At present, we cannot extend the above result (1) of Kolyvagin to the rank ≥ 2 case.[1]

2.3.5. It seems that zeta functions contain information about the structure of Iwasawa modules which is finer than the characteristic ideals.

For example, assume that X is either $\Lambda/(ab)$ or $\Lambda/(a) \oplus \Lambda/(b)$ for some $a, b \in \Lambda$. Since the characteristic ideals of both cases are (ab), we may think that p-adic zeta functions cannot tell which is the case. But in [28], Kurihara states the following with a sketch of the proof: In Case I, if we consider not only the single p-adic zeta function $\xi \in Q(\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})^+/\mathbb{Q})]])$ but also the p-adic zeta functions in $Q(\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\zeta_{Np^\infty})^+/\mathbb{Q})]])$ for all N which p-adically interpolate values of various Dirichlet L-functions, then these p-adic zeta functions can tell which is the case.

[1] *Added in the proof.* Skinner and Urban have obtained results for the rank ≥ 2 case. See their article in Volume II of the Proceedings of this ICM.

For a commutative ring R and for an R-module M of finite presentation, the r-th Fitting ideal of M is defined as follows. Take a presentation of M as the cokernel of an R-homomorphism $f\colon R^m \to R^n$. Then the r-th Fitting ideal of M is the ideal of R generated by the determinants of all $(n-r, n-r)$-minors of the matrix f. This is independent of the presentation of M. For example, the 0-th and the 1-st Fitting ideals of the Λ-module $\Lambda/(ab)$ are (ab) and Λ, respectively, whereas the 0-th and the 1-st Fitting ideals of $\Lambda/(a) \oplus \Lambda/(b)$ are (ab) and (a, b), respectively.

Kurihara [28] shows that for any $r \geq 0$, the r-th Fitting ideal of X is determined by the p-adic zeta functions in $Q(\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\zeta_{Np^\infty})^+/\mathbb{Q})]])$ for varying N (his result is more general and can treat totally real fields). Partial results are proved in [26] and [27].

2.4. The modular form method. There are two proofs of the Iwasawa main conjecture for cyclotomic fields. One is the original proof of Mazur–Wiles using modular forms. The other is the proof of Rubin given later based on the method of Euler systems of Kolyvagin (see [38] for example). These two methods in Case I are both extended to Case II: The proofs of the results (1), (2) of 2.3.3 are by the Euler system methods, and the proof of the result (3) is an extension of the method of Mazur–Wiles (we will call a method of this type a modular form method).

In this subsection (resp. the next subsection), I sketch the ideas of the modular form method (resp. Euler system method).

By their natures, the modular form method is used to prove the divisibility, "the p-adic zeta function divides the characteristic ideal of the Iwasawa module", and the Euler system method is used to prove the converse divisibility. In Case 1, by the help of the class number formula, any one divisibility implies the converse divisibility.

2.4.1. Riemann's zeta function is regarded as the zeta function of a modular form of GL_1. The method of Mazur–Wiles in Case I is to use modular forms of the bigger algebraic group GL_2 to prove the main conjecture for a modular form of GL_1. The zeta function of an elliptic curve over $\mathbb{Q}$ is the zeta function of a modular form of GL_2. The method of Skinner–Urban in Case II is to use modular forms of the bigger algebraic group $U(2, 2)$ to prove the main conjecture for a modular form of GL_2.

2.4.2. There are three key points (a)–(c) about the method of Mazur–Wiles.

(a) Riemann zeta values appear as constant terms of Eisenstein series.

In fact, for k even ≥ 4, the Eisenstein series E_k of weight k has the q-expansion

$$E_k = \zeta(1-k)/2 + \textstyle\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Here $\sigma_m(n)$ denotes the sum of d^m for all divisors d of n.

(b) An eigen cusp form produces a two-dimensional irreducible p-adic representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

This is the theory of Eichler–Shimura and Deligne. In Langlands program, we expect that Galois representations arise from modular forms of various algebraic groups.

(c) The ideal class group is related to extensions of Galois representations with finite coefficients.

For example, for $r \in \mathbb{Z}$, there exists a non-trivial extension $0 \to \mathbb{Z}/p\mathbb{Z}(r) \to ? \to \mathbb{Z}/p\mathbb{Z} \to 0$ of representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ over $\mathbb{Z}/p\mathbb{Z}$ which splits as a representation of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ and is unramified outside p if and only if the Galois module $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ contains $(\mathbb{Z}/p\mathbb{Z})(r)$. (This can be proved by class field theory.)

2.4.3. To see how we can relate Riemann zeta values to the minus parts of ideal class groups by this method, we discuss simply how we can prove the "if part", due to Ribet [35], of the following theorem of Herbrand–Ribet: For $k \geq 2$ even, the Galois module $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ contains $(\mathbb{Z}/p\mathbb{Z})(1-k)$ if and only if p divides the numerator of $\zeta(1-k)$. In fact, this work of Ribet was a great hint for Mazur and Wiles in their work [32]. The proof goes in the following way.

We may and do assume that $4 \leq k \leq p-3$ and $k \not\equiv 0 \bmod (p-1)$. If p divides $\zeta(1-k)$, by 2.4.2 (a), $E_k \bmod p$ has no constant term. This shows that $E_k \equiv f \bmod p$ for some eigen cusp form f. For example, 691 divides $\zeta(-11)$ and $E_{12} \equiv \Delta \bmod 691$ where Δ is the eigen cusp form $q\prod_{n=1}^{\infty}(1-q^n)^{24}$. (This is Ramanujan's congruence.)

The congruence $f \cong E_k \bmod p$ tells that, by taking mod p of the 2-dimensional p-adic representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ associated to f (2.4.2 (b)), we can obtain a 2-dimensional representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ over $\mathbb{Z}/p\mathbb{Z}$ which is a non-trivial extension of the form $0 \to (\mathbb{Z}/p\mathbb{Z})(1-k) \to ? \to \mathbb{Z}/p\mathbb{Z} \to 0$ having the properties in 2.4.2 (c).

Hence by 2.4.2 (c) above we have $(\mathbb{Z}/p\mathbb{Z})(1-k) \subset \mathrm{Cl}(\mathbb{Q}(\zeta_p))$ as Galois modules.

2.4.4. Skinner and Urban extended this approach to Case II. In place of 2.4.2 (a), the zeta values $L(E, 1, \chi)$ appear in the constant terms of the Eisenstein series of $U(2,2)$. In place of 2.4.2 (b), Galois representations associated to modular forms of $U(2,2)$ are used. In place of 2.4.2 (c), by the definition of Selmer group, an element of the Selmer group $\mathrm{Sel}(E/K)$ of order n corresponds to an extension $0 \to \mathrm{Ker}(n\colon E(\overline{K}) \to E(\overline{K})) \to ? \to \mathbb{Z}/n\mathbb{Z} \to 0$ of representations of $\mathrm{Gal}(\overline{K}/K)$ over $\mathbb{Z}/n\mathbb{Z}$.

2.5. The Euler system method

2.5.1. It seems that zeta functions appear in this world showing three different shapes. First, they appear in the complex analytic world as complex analytic zeta functions, and are defined usually as Euler products. Secondly, they appear in the p-adic world as p-adic zeta functions. Now thirdly, they appear in the arithmetic world, as "arithmetic incarnations of zeta" such as cyclotomic units, elliptic units, Heegner points, and Beilinson elements. These incarnations are arithmetic objects which are related to zeta values in many ways. They form a family which has the property of being an

Euler system ([38]). I do not discuss the property of being an Euler system, but it is an arithmetic reflection of the fact that these incarnations are related to special values of Euler products.

For example, we call $1-\alpha$ (α a root of 1, $\alpha \neq 1$) a cyclotomic unit. The logarithms of cyclotomic units are related to complex zeta values as

$$\sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times} \chi(a)\log(|1-\zeta_N^a|) = -2L'(0,\chi)$$

for any even Dirichlet character χ, where $\zeta_N = \exp(2\pi i/N)$.

Furthermore, as was discovered by Kummer and Iwasawa, cyclotomic units are related p-adically to zeta values $\zeta(r)$ for $r \in \mathbb{Z}$, $r \leq 0$, and furthermore produce the p-adic Riemann zeta function in a certain p-adic way.

Because the arithmetic incarnations of zeta are arithmetic in nature, they can play an important role in the study of arithmetic properties of zeta values. Cyclotomic units are important in classical Iwasawa theory, elliptic units in Iwasawa theory of imaginary quadratic fields and in Iwasawa theory of elliptic curves with complex multiplication (as in [10], [37]), Heegner points in anti-cyclotomic Iwasawa theory of elliptic curves (as in [25], [3]), and Beilinson elements in cyclotomic Iwasawa theory of elliptic curves.

2.5.2. The results 2.3.3 (1), (2) were obtained by using elliptic units and Beilinson elements, respectively. The methods are similar to the second proof of Iwasawa's main conjecture given by Rubin using cyclotomic units.

In these methods, the key points are that (a) these incarnations of zeta are related p-adically to p-adic zeta functions, and that (b) they form Euler systems.

I will explain the methods in Case I first, and then tell about Case II.

2.5.3. As is well known in classical Iwasawa theory thanks to deep works of Iwasawa, the Iwasawa main conjecture introduced in 2.3.1 is equivalent to

$$\mathrm{Char}(U/\Lambda z) = \mathrm{Char}(C^+).$$

Here U (resp. C^+) is the projective limit of

$$(\mathbb{Z}[\zeta_{p^n}, 1/p]^+)^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad (\text{resp. } \mathrm{Cl}(\mathbb{Q}(\zeta_{p^n})^+)(p))$$

with respect to norm maps ((p) denotes the p-primary part), and $z \in U$ is the system of cyclotomic units $((1-\zeta_{p^n})(1-\zeta_{p^n}^{-1}))_n$. To rewrite Iwasawa's main conjecture 2.3.1 in this form, we replace the p-adic zeta function in the conjecture 2.3.1 by z using the strong relation (2.5.2 (a)) between them, and replace X by C^+ using the fact that C^+ is a quotient Λ-module of X by class field theory. Note that in this rewritten form of Iwasawa's main conjecture, since the p-adic zeta function was replaced by the arithmetic incarnation, both sides became arithmetic sides.

We can prove that $\mathrm{Char}(C^+)$ divides $\mathrm{Char}(U/\Lambda z)$ by the method of Euler system (Kolyvagin's idea [25]; Thaine [42] had partially a similar idea) using the Euler system

property of cyclotomic units (2.5.2 (b)). The method here is simply speaking as in 2.5.4 below. This divisibility implies the divisibility $\mathrm{Char}(X) \mid I(\Lambda)\xi$ and gives the proof of Iwasawa's main conjecture.

2.5.4. The proof of $\mathrm{Char}(C^+) \mid \mathrm{Char}(U/\Lambda z)$ by the Euler system method is sketched roughly as follows.

Let $h\colon \bigoplus_{i=1}^n \Lambda/(a_i) \to C^+$ be an injective Λ-homomorphism with finite cokernel. The Λ-module U is isomorphic to Λ, and hence $U/\Lambda z \simeq \Lambda/(\mu)$ for some $\mu \in \Lambda$. Our task is to prove that $\prod_{i=1}^n a_i$ divides μ. For $1 \leq i \leq n$, denote the standard i-th generator in $\bigoplus_{i=1}^n \Lambda/(a_i)$ by e_i. Then by modifying cyclotomic units using their Euler system property, for each $m \geq 1$, we can construct a non-zero element α of $\mathbb{Q}(\zeta_{p^m})^+$ such that there is a non-zero fractional ideal of $\mathbb{Q}(\zeta_{p^m})^+$ whose class coincides with the image of $h(e_1)$ and which is sent by the action of μ to the principal ideal (α). This shows that μ kills $h(\Lambda e_1)$, and hence $a_1 \mid \mu$. Put $\mu = \mu_1 a_1$ with $\mu_1 \in \Lambda$. By a similar method, we can show that μ_1 kills $h(\Lambda e_1 \oplus \Lambda e_2)/h(\Lambda e_1)$. Hence $a_2 \mid \mu_1$. Put $\mu_1 = \mu_2 a_2$ with $\mu_2 \in \Lambda$. Then we can show that μ_2 kills $h(\Lambda e_1 \oplus \Lambda e_2 \oplus \Lambda e_3)/h(\Lambda e_1 \oplus \Lambda e_2)$. By repeating this, we have $\mu = \mu_n \prod_{i=1}^n a_i$ with $\mu_n \in \Lambda$.

For the precise description of the method see [38].

2.5.5. In Case II we can use similar methods to prove that X is Λ-torsion and to prove 2.3.3 (1), (2). I describe rough ideas about 2.3.3 (2).

Beilinson elements are defined in [2] as elements of K_2 of modular curves (K_2 is a group which appears in algebraic K-theory). Via the Weil parametrization of an elliptic curve E over $\mathbb{Q}$, and via the Archimedean regulator maps of K_2 (analogues of logarithms for the multiplicative group), they are related to $L'(E, 0, \chi)$. Furthermore, we can prove that they are related p-adically to the values $L(E, 1, \chi)$ and to the p-adic zeta function $L_p(E)$.

In Case I, the Λ-module U (resp. C^+) is isomorphic to the inverse limit of the étale cohomology groups $H^i(\mathbb{Z}[\zeta_{p^n}, 1/p]^+, \mathbb{Z}_p(1))$ with $i = 1$ (resp. $i = 2$). In Case II, in place of U (resp. C^+), we use the inverse limit $\mathfrak{H}^i$ of the étale cohomology groups $H^i(\mathbb{Z}[\zeta_{p^n}, 1/pN], T_pE)$ with $i = 1$ (resp. $i = 2$), where N is the conductor of E and T_pE is the p-adic Tate module of E. By using the strong relation of Beilinson elements and $L_p(E)$ (2.5.2 (a)), we can show that the fact "X is Λ-torsion and $\mathrm{Char}(X) \mid \Lambda L_p(E)$" is equivalent to the fact that "$\mathfrak{H}^1/\Lambda z$ and $\mathfrak{H}^2$ are Λ-torsion and $\mathrm{Char}(\mathfrak{H}^2) \mid \mathrm{Char}(\mathfrak{H}^1/\Lambda z)$" where $z \in \mathfrak{H}^1$ is an element which comes from Beilinson elements. In the case E has no complex multiplication, the last fact is proved by arguments similar to 2.5.4 using the Euler system property of Beilinson elements (2.5.2 (b)). (In this method, we make also a heavy use of the result by Rohrlich that $L_p(E)$ is a non zero-divisor of $\Lambda[1/p]$.)

2.5.6. We expect that the Euler system method works for any motives. However, a big difficulty is that at present we can find only few arithmetic incarnations of zeta, though we have found a lot of zeta functions.

3. Non-commutative Iwasawa theory

For an elliptic curve E over a number field F without complex multiplication, the field obtained by adjoining all p^n-torsion points of E to F for all n is a Galois extension of F whose Galois group is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ of finite index (by a theorem of Serre) and hence is highly non-commutative. It is natural to look for a non-commutative Iwasawa theory for E.

In this section, I introduce the ideas in the papers [43] and [8] on non-commutative Iwasawa theory, and discuss related problems.

In this section, we consider two cases I, II. In Case I, we consider non-commutative Iwasawa theory of totally real fields. In Case II, we consider non-commutative Iwasawa theory of elliptic curves.

Fix a prime number p and assume $p \neq 2$ for simplicity. Both in the cases I, II, let F be a number field, and let F_∞ be a Galois extension of F satisfying the following conditions (i)–(iii).

(i) The Galois group $G = \mathrm{Gal}(F_\infty/F)$ is a p-adic Lie group.

(ii) There are only finitely many primes of F which ramify in F_∞.

(iii) F_∞ contains the cyclotomic $\mathbb{Z}_p$-extension F^{cyc} of F.

In Case I, we assume further that F_∞ is totally real, and that F_∞ contains $F(\zeta_{p^\infty})^+$.

In Case II, we assume that we are given an elliptic curve E over F which is of good ordinary reduction at any prime of F lying over p.

Let $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}}) \subset G$, so that H is a closed normal subgroup of G with $G/H \simeq \mathbb{Z}_p$. In Case I, fix a finite set Σ of primes of F which contain all primes of F lying over p and all primes of F which ramify in F_∞.

3.1. Arithmetic side

3.1.1. Let $\Lambda = \mathbb{Z}_p[[G]]$. By a Λ-module, we mean a left Λ-module. We define a Λ-module X as follows.

In Case I, let $X = \mathrm{Gal}(M/F_\infty)$ where M is the largest abelian pro-p extension of F_∞ which is unramified outside Σ.

In Case II, let $X = \mathrm{Hom}\,(\varinjlim_{F'} \mathrm{Sel}(E/F'), \mathbb{Q}_p/\mathbb{Z}_p)$ where F' ranges over all finite Galois extensions of F contained in F_∞.

Then in both cases X is a finitely generated Λ-module.

3.1.2. In Case I, X is a torsion Λ-module (that is, each element of X is killed by some non zero-divisor of Λ). In Case II, a natural conjecture is that X is Λ-torsion.

More precisely:

Conjecture 3.1.3. In Case I, X is finitely generated as a $\mathbb{Z}_p[[H]]$-module.

Conjecture 3.1.4. ([8] 5.1.) In Case II, $X/X(p)$ is finitely generated as a $\mathbb{Z}_p[[H]]$-module, where $X(p)$ denotes the part of X killed by some power of p.

Let F' be a finite extension of F contained in F_∞ such that F_∞/F' is a pro-p extension. In Case I, 3.1.3 is true if the μ-invariant of the cyclotomic $\mathbb{Z}_p$-extension of F' is zero (it is conjectured by Iwasawa that the μ-invariant of the cyclotomic $\mathbb{Z}_p$-extension of any number field is zero). In Case II, 3.1.4 is true if E is isogenous over F' to an elliptic curve E' such that the μ-invariant of E' for the cyclotomic $\mathbb{Z}_p$-extension of F' is zero.

3.2. Zeta side

3.2.1. Where do the p-adic zeta functions in non-commutative Iwasawa theory live? Non-commutative rings are not good places to live for complex zeta functions defined as Euler products, for the meaning of Euler product becomes unclear by the non-commutativity of the product. Though p-adic zeta functions are not Euler products, this gives us the impression that any p-adic zeta function cannot live in the non-commutative Λ.

However, for a non-commutative ring R, the non-commutativity of the product in $R^\times$ vanishes under the canonical homomorphism $R^\times \to K_1(R)$.

3.2.2. Recall that for a ring R, $K_1(R)$ is defined to be the abelian group

$$\mathrm{GL}(R)/[\mathrm{GL}(R), \mathrm{GL}(R)],$$

where $\mathrm{GL}(R) = \bigcup_n \mathrm{GL}_n(R)$ in which $\mathrm{GL}_n(R)$ is embedded in $\mathrm{GL}_{n+1}(R)$ by $T \mapsto \left(\begin{smallmatrix} T & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

3.2.3. As is explained below, in Case I (resp. Case II) we expect that the p-adic zeta function lives in K_1 of a certain localization of Λ (resp. of $\bar{\Lambda} = O[[G]]$ where O is the completion of the valuation ring of the maximal unramified extension of $\mathbb{Q}_p$) defined as follows. (Note that the theory of localizations of non-commutative rings is not so simple as that for commutative rings.) Define

$$S = \{s \in \Lambda \mid \Lambda/\Lambda s \text{ is a finitely generated } \mathbb{Z}_p[[H]]\text{-module}\}, \quad S^* = \bigcup_{n\geq 0} p^n S.$$

Then S and S^* are multiplicative subsets of Λ, consisting of left and right non zero-divisors and satisfying the left and right Ore conditions ([33]) in the localization theory of non-commutative rings. Hence we have rings $\Lambda_S = S^{-1}\Lambda = \Lambda S^{-1}$ by inverting elements of S, and also $\Lambda_{S^*} = \Lambda_S[1/p]$. In the case that H is finite and G is commutative, $\Lambda_{S^*} = Q(\Lambda)$.

Let $\mathfrak{N}_H(G)$ (resp. $\mathfrak{M}_H(G)$) be the category of finitely generated Λ-modules M such that M (resp. $M/M(p)$) is finitely generated as a $\mathbb{Z}_p[[H]]$-module. For a finitely generated Λ-module M, M is S-torsion if and only if it belongs to $\mathfrak{N}_H(G)$, and it is S^*-torsion if and only if it belongs to $\mathfrak{M}_H(G)$.

We have similarly multiplicative subsets $\bar{S}$ and $\bar{S}^* = \bigcup_{n\geq 0} \bar{S}p^n$ of $\bar{\Lambda}$ and localizations $\bar{\Lambda}_{\bar{S}}$, $\bar{\Lambda}_{\bar{S}^*}$.

3.2.4. We expect that the p-adic zeta function in non-commutative Iwasawa theory is characterized by the relation of its special values with complex zeta values. For an element f of $K_1(\Lambda_{S^*})$ and for a continuous representation $\rho\colon G \to \mathrm{GL}_n(\mathbb{C}_p)$ where $\mathbb{C}_p$ is the completion of the algebraic closure of $\mathbb{Q}_p$, the value $f(\rho) \in \mathbb{C}_p \cup \{\infty\}$ is defined in [8]. I do not give here the precise general definition, but a basic fact is that if f is the image of an element a of $\Lambda \cap (\Lambda_{S^*})^\times$, the value of f at ρ is equal to $\det(\rho(a))$, where $\rho(a)$ denotes the image of a under the ring homomorphism $\Lambda \to M_n(\mathbb{C}_p)$ induced by ρ.

We can define similarly the value $f(\rho) \in \mathbb{C}_p \cup \{\infty\}$ of an element f of $K_1(\bar{\Lambda}_{\bar{S}^*})$ at a continuous representation $\rho\colon G \to \mathrm{GL}_n(\mathbb{C}_p)$.

Now we state our conjecture for the existence of the p-adic zeta function in non-commutative Iwasawa theory.

Conjecture 3.2.5. (1) In Case I, there is an element $L_p(F_\infty/F) \in K_1(\Lambda_S)$ (called the p-adic zeta function for the extension F_∞/F) having the following property.

For any even integer $r \geq 1$ and any representation ρ of G which factors through a finite quotient Galois group, the value of $L_p(F_\infty/F)$ at the representation $\rho\kappa^r$ of G is the value $L_\Sigma(1-r, \rho)$ of the Artin L-function $L_\Sigma(s, \rho)$. (The subscript Σ means that the Euler factors at primes in Σ are removed from the Euler product.)

(2) In Case II, there is an element $L_p(E, F_\infty/F) \in K_1(\bar{\Lambda}_{\bar{S}^*})$ (called the p-adic zeta function of E for the extension F_∞/F) having the following property.

For any representation ρ of G which factors through a finite quotient Galois group, the value of $L_p(E, F_\infty/F)$ at ρ is $L(E, 1, \rho)/((\text{ period}) \times (\text{local term}))$.

Here $L(E, s, \rho)$ is the twist of $L(E, s)$ by ρ. The definitions of (period) and (local term) are given explicitly in [8] in the case $F = \mathbb{Q}$. In the case $F \neq \mathbb{Q}$, the definitions are given in [16] but they are not so explicit.

3.2.6. The idea that "zeta functions can live in K_1 of non-commutative group rings" may be true also for Selberg zeta functions. Such idea appears in the paper of Bass [1] for Ihara–Selberg zeta functions (Selberg zeta functions for p-adic fields). I learned about the work [1] from K. Hashimoto.

For a discrete co-compact torsion-free subgroup Γ of $\mathrm{SL}_2(\mathbb{R})/\{\pm 1\}$ and for a finite dimensional representation $\rho\colon \Gamma \to \mathrm{GL}_n(\mathbb{C})$, the Selberg zeta function of Γ with twist by ρ is defined to be $\prod_\gamma \det(1 - \rho(\gamma)N(\gamma)^{-s})^{-1}$ $(\Re(s) \gg 0)$ where γ ranges over all "prime elements" of Γ taken mod conjugacy. (Prime element means an element which is not an n-th power of any element for any $n \geq 2$. $N(\gamma) > 1$ is the absolute value of one of the eigen values of γ.)

I am not sure if it is reasonable to define the Selberg zeta function with values in $K_1(L^1(\Gamma))$, where $L^1(\Gamma)$ is the algebra of L^1-functions on Γ with the product structure by convolution, as follows.

$$\zeta_\Gamma(s) = \prod_\gamma (1 - \gamma N(\gamma)^{-s})^{-1}.$$

(The right-hand side is regarded as an element of $K_1(L^1(\Gamma))$.) For a finite dimensional unitary representation $\rho\colon \Gamma \to \mathrm{GL}_n(\mathbb{C})$, the ring homomorphism $L^1(\Gamma) \to M_n(\mathbb{C})$ induced by ρ defines a homomorphism $K_1(L^1(\Gamma)) \to K_1(M_n(\mathbb{C})) = \mathbb{C}^\times$ which sends $\zeta_\Gamma(s)$ to the Selberg zeta function of Γ with twist by ρ.

If $\mathrm{SL}_2(\mathbb{R})/\{\pm 1\}$ is replaced by $\mathrm{SL}_2(\mathbb{Q}_p)/\{\pm 1\}$, an analogue of the above $\zeta_\Gamma(s)$ is considered in Bass [1].

3.3. Main conjecture. We assume for simplicity that G is p-torsion-free in this subsection.

3.3.1. The localization theory in K-theory [46] gives exact sequences

$$K_1(\Lambda) \to K_1(\Lambda_S) \xrightarrow{\partial} K_0(\mathfrak{N}_H(G)) \to 0,$$
$$K_1(\Lambda) \to K_1(\Lambda_{S^*}) \xrightarrow{\partial} K_0(\mathfrak{M}_H(G)) \to 0.$$

Here for $\mathcal{C} = \mathfrak{N}_H(G)$ or $\mathfrak{M}_H(G)$, $K_0(\mathcal{C})$ denotes the Grothendieck group of $\mathcal{C}$, which is an abelian group defined by the following generators and relations. Generators: $[M]$ for objects M of $\mathcal{C}$. Relations: $[M] = [M'] + [M'']$ if M, M', M'' are objects of $\mathcal{C}$ such that there is an exact sequence $0 \to M' \to M \to M'' \to 0$. In the above first (resp. second) exact sequence, ∂ satisfies $\partial(s) = [\Lambda/\Lambda s]$ for $s \in S$ (resp. $s \in S^*$).

In the situation of §2 in which G is commutative, $\mathfrak{M}_H(G)$ coincides with the category of all finitely generated torsion Λ-modules, and for any finitely generated torsion Λ-module M and for any generator f of $\mathrm{Char}(M)$, we have $\partial(f) = [M]$ in $K_0(\mathfrak{M}_H(G))$. Hence $[M]$ can play the role of the characteristic ideal in §2.

The following is the main conjecture. ([43], [8]. Generalizations to motives are explained in the complementary paper [16] to [8].)

Conjecture 3.3.2. (1) In Case I, the homomorphism $\partial\colon K_1(\Lambda_S) \to K_0(\mathfrak{N}_H(G))$ sends $L_p(F_\infty/F)$ to $[X] - [\mathbb{Z}_p]$.

(2) In Case II, if f is an element of $K_1(\Lambda_{S^*})$ such that $\partial(f) = [X]$, we have $L_p(E, F_\infty/F) \equiv f$ modulo the image of $K_1(\bar{\Lambda}) \to K_1(\bar{\Lambda}_{\bar{S}^*})$.

3.4. Complements

3.4.1. In Case I, a main conjecture was formulated and studied by Ritter–Weiss ([39] etc.) under the assumption that H is finite (H can have p-torsion).

3.4.2. For an elliptic curve E with super-singular reduction at p, it is not known how to formulate p-adic zeta functions in non-commutative Iwasawa theory.

3.4.3. In history, studies of delicate properties of algebraic varieties motivated progress in the theory of commutative rings. Similarly, I expect that via non-commutative Iwasawa theory, delicate aspects in number theory motivate progress in the theory of non-commutative rings. The structure theorem of torsion modules over non-commutative Iwasawa type algebras by Coates–Schneider–Sujatha [9] is one such example.

3.4.4. An interesting aspect of non-commutative Iwasawa theory of elliptic curves is the relative prevalence, compared to the cyclotomic theory, of global root numbers equal to -1 (in the case of twists of an elliptic curve by self dual Artin characters of certain non-commutative p-adic Lie extensions, see, for example, Dokchitser [14], and Rohrlich [36]). This phenomenon has long been important in the study of Heegner points on elliptic curves, and recently H. Darmon and Y. Tian have obtained the first deep results about Heegner points in non-commutative Iwasawa theory of elliptic curves ([13], [11]).

3.4.5. As in Huber–Kings [19], §3.3, we can expect that non-commutative Iwasawa theory is strong enough to unify Iwasawa theories of all motives. This would imply that there are many still unknown congruences between p-adic zeta functions of different motives and also between modular forms of different algebraic groups.

In the rest of this section, assuming that G is isomorphic to a non-commutative semi-direct product of two copies of $\mathbb{Z}_p$, I report some conjectural congruences between p-adic zeta functions in commutative Iwasawa theory which would be implied by non-commutative Iwasawa theory. We can show conversely (Proposition 3.4.9, which I learned from D. Burns) that in Case I, under the same assumption, the existence of p-adic zeta function and the main conjecture in non-commutative Iwasawa theory are reduced to these conjectural congruences between p-adic zeta functions in commutative Iwasawa theory.

3.4.6. Assume that G is isomorphic to a non-commutative semi-direct product of two copies of $\mathbb{Z}_p$.

Then $H \simeq \mathbb{Z}_p$. Let $e \geq 1$ be the integer such that $H/[G,H]$ is of order p^e. Let $\Gamma = G/H$ and for $n \geq 0$, let $\Gamma_n \subset \Gamma$ be the unique subgroup of Γ of index $p^{\max(n-e,0)}$. Define commutative rings R_n and $R'_n \subset Q(R_n)$ $(n \geq 0)$ as follows: $R_n = \mathbb{Z}_p[\zeta_{p^{\min(n,e)}}][[\Gamma_n]]$, and R'_n is the local ring of R_n at the unique prime ideal of height 1 containing p. In [23], homomorphisms

$$\theta = (\theta_n)_n \colon K_1(\mathbb{Z}_p[[G]]) \to \prod_{n\geq 0} R_n^\times, \quad \theta' = (\theta'_n)_n \colon K_1(\mathbb{Z}_p[[G]]_S) \to \prod_{n\geq 0} (R'_n)^\times$$

such that θ' induces θ are defined. Furthermore subgroups

$$\Phi \subset \prod_{n\geq 0} R_n^\times, \quad \Phi' \subset \prod_{n\geq 0} (R'_n)^\times$$

such that $\Phi = \left(\prod_{n\geq 0} R_n^\times\right) \cap \Phi'$ are defined by using certain congruences.

The congruences defining Φ and Φ' are rather involved, and so for simplicity, I introduce them here only in the case $e = 1$.

Let $(a_n)_n$ be an element of $\prod_{n\geq 0} R_n^\times$ (resp. $\prod_{n\geq 0}(R'_n)^\times$). Let $b_n = a_n N_n(a_0)^{-1}$ where N_n is the norm map

$$\mathbb{Z}_p[[\Gamma]]^\times \to \mathbb{Z}_p[[\Gamma_n]]^\times \quad (\text{resp. } (\mathbb{Z}_p[[\Gamma]]_{(p)})^\times \to (\mathbb{Z}_p[[\Gamma_n]]_{(p)})^\times).$$

Let $c_n = b_n\varphi(b_{n-1})^{-1}$ for $n \geq 1$ where φ is the ring homomorphism induced by the p-th power homomorphism $\Gamma_{n-1} \to \Gamma_n$. Then in the case $e = 1$, $(a_n)_n$ belongs to Φ (resp. Φ') if and only if the following congruences are satisfied:

$$c_n^{p^{n-1}} \equiv N_n(N'\big(\textstyle\prod_{i=1}^{n-1} c_i)\big) \bmod p^{2(n-1)}(\zeta_p - 1) \quad \text{for any } n \geq 1$$

where N' denotes the norm map $R_1^\times \to \mathbb{Z}_p[[\Gamma]]^\times$ (resp. $(R_1')^\times \to (\mathbb{Z}_p[[\Gamma]]_{(p)})^\times$).

Proposition 3.4.7 ([23]). (1) *The map* $\theta\colon K_1(\mathbb{Z}_p[[G]]) \to \prod_{n\geq 0} R_n^\times$ *is injective and induces an isomorphism* $K_1(\mathbb{Z}_p[[G]]) \xrightarrow{\simeq} \Phi$.

(2) *The image of* $\theta'\colon K_1(\mathbb{Z}_p[[G]]_S) \to \prod_{n\geq 0} (R_n')^\times$ *is contained in* Φ'.

3.4.8. Assume that we are in Case I. For $n \geq 0$, let F_n be the finite extension of F contained in F^{cyc} corresponding to the subgroup Γ_n of Γ. Let $G_n \subset G$ be the inverse image of Γ_n in G. Then there is a one-dimensional representation $\chi_n\colon G_n \to \overline{\mathbb{Q}}^\times$ of G_n of order p^n whose restriction to H is still of order p^n. The p-adic L-function ξ_n of the totally real field F_n associated to the character χ_n belongs to $Q(R_n)$. The main conjecture of Iwasawa theory of F_n proved by Wiles shows that

(1) $(\xi_n) = \mathrm{Char}(X_n)$ for $n \geq 1$, and $I(R_0)\xi_0 = \mathrm{Char}(X_0)$

where X_n is the Iwasawa module of the Iwasawa theory of F_n associated to χ_n and $I(R_0)$ is the kernel of $R_0 = \mathbb{Z}_p[[\Gamma]] \to \mathbb{Z}_p; \sigma \mapsto 1$ $(\sigma \in \Gamma)$.

I did not explain the definitions of θ_n and θ_n', but the maps θ_n' have the following properties (2) and (3).

(2) Let ξ be an element of $K_1(\Lambda_S)$. Then ξ has the property of the p-adic zeta function $L_p(F_\infty/F)$ stated in 3.2.5 if and only if $\theta_n'(\xi) = \xi_n$ for all $n \geq 0$.

(3) If X belongs to $\mathfrak{N}_H(G)$ and f is an element of $K_1(\Lambda_S)$ such that $\partial(f) = [X] - [\mathbb{Z}_p]$, then $(\theta_n'(f)) = \mathrm{Char}(X_n)$ for $n \geq 1$, and $I(R_0)\theta_0'(f) = \mathrm{Char}(X_0)$.

If the p-adic zeta function $L_p(F_\infty/F) \in K_1(\Lambda_S)$ in non-commutative Iwasawa theory exists, then by the above (2) and by Prop. 3.4.7 (2), $(\xi_n)_n$ should be contained in Φ'. This shows that the p-adic L functions ξ_n in commutative Iwasawa theory should satisfy special congruences between them (which are not proven yet).

Conversely, assume $(\xi_n)_n \in \Phi'$. From the above (1), we can deduce $X \in \mathfrak{N}_H(G)$. Let f be an element of $K_1(\Lambda_S)$ such that $\partial(f) = [X] - [\mathbb{Z}_p]$. Then by (1) and (3), we have $(\xi_n) = (\theta_n'(f))$ for any $n \geq 0$. Hence $u_n := \xi_n\theta_n'(f)^{-1}$ is a unit of R_n. By Prop. 3.4.7 (2), $(u_n)_n \in \big(\prod_{n\geq 0} R_n^\times\big) \cap \Phi' = \Phi$. Hence by Prop. 3.4.7 (1), $(u_n)_n$ comes from an element u of $K_1(\Lambda)$. By (2), uf is the p-adic zeta function of F_∞/F in the non-commutative Iwasawa theory (which we were looking for), and $\partial(uf) = [X] - [\mathbb{Z}_p]$. This proves

Proposition 3.4.9. *Assume that we are in Case* I, *and assume that* G *is non-commutative and is a semi-direct product of two copies of* $\mathbb{Z}_p$. *If the family* $(\xi_n)_{n\geq 0}$ *of* p*-adic*

zeta functions in commutative Iwasawa theory belongs to Φ' (*i.e. satisfies special congruences*)*, then the* p*-adic zeta function for* F_∞/F *in non-commutative Iwasawa theory exists and the main conjecture in non-commutative Iwasawa theory for* F_∞/F *is true.*

From §2 we can have the idea that "the proofs of the main conjectures in commutative Iwasawa theory will be obtained by the modular form method and the Euler system method as in §2". The author learned from D. Burns not only Proposition 3.4.9 but also the following idea: "the proofs of the main conjectures in non-commutative Iwasawa theory might not be at infinite distance, but might be deduced from the main conjecture in commutative Iwasawa theory plus special congruences between p-adic zeta functions in commutative Iwasawa theory".

References

[1] Bass, H., The Ihara-Selberg zeta function of a tree lattice. *Internat. J. Math.* **3** (1992), 717–797.

[2] Beilinson, H., Higher regulators and values of L-functions. Current problems in mathematics **24** (1984), 181–238.

[3] Bertolini, M., and Darmon, H., Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions. *Ann. of Math.* **162** (2005), 1–64.

[4] Birch, B., J., and Swinnerton-Dyer, H. P. F., Notes on elliptic curves. I. *J. Reine Angew. Math.* **212** (1963), 7–25; II. *J. Reine Angew. Math.* **218** (1965), 79–108.

[5] Bloch, S., and Kato, K., L-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift*, Vol. I, Progr. Math. 86, Birkhäuser, Boston, MA, 1990, 333–400.

[6] Breuil, C., Conrad, B., Diamond, F., and Taylor, R., On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.* **14** (2001), 843–939.

[7] Burns, D., and Flach, M., Tamagawa numbers for motives with (non-commutative) coefficients I. *Documenta Math.* **6** (2001), 501–570; II, *Amer. J. Math.* **125** (2003), 475–512.

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

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

[10] Coates, J., and Wiles, A., On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.* **39** (1977), 223–251.

[11] Darmon, H., and Tian, Y., Heegner points over false Tate curve extension. Talk in Montreal; preprint.

[12] Deligne, P., Valeurs de fonctions L et périodes d'intégrales. In *Automorphic forms, representations and L-functions*, Part 2, Proc. Symp. Pure Math. 33, Amer. Math. Soc., Providence, R.I., 1979, 313–346.

[13] Dokchitser, T., and Dokchitser, V., Computations in non-commutative Iwasawa theory (with an appendix by J. Coates and R. Sujatha). *Proc. London Math. Soc.* **94** (2007), 211–272.

[14] Dokchitser V., Root numbers of non-abelian twists of elliptic curves. *Proc. London Math. Soc.* **91** (2005), 300–324.

[15] Fontaine, J.-M., and Perrin-Riou, B., Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L. In *Motives* (Seattle, WA, 1991), Proc. Symp. Pure Math. 55, Part 1, Amer. Math. Soc., Providence, RI, 1994, 599–706.

[16] Fukaya, T., and Kato, K., A formulation of conjectures on p-adic zeta functions in non-commutative Iwasawa theory. *Trudy Sankt-Peterburgskugo Matematicheskogo Obshchestva* **12** (2005), 1–101; English version to appear in Amer. Math. Soc. Transl. Ser. 2, Proc. St Petersburg Math. Soc.

[17] Greenberg, R., Iwasawa theory for p-adic representations. In *Algebraic number theory*, Adv. Stud. Pure Math. 17, Academic Press, Boston, MA, 1989, 97–137.

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

[19] Huber, A., and Kings, G., Equivariant Bloch-Kato conjecture and non-abelian Iwasawa main conjecture. In *Proceedings of the International Congress of Mathematicians* (Beijing, 2002), Vol. II, Higher Ed. Press, Beijing 2002, 149–162.

[20] Iwasawa, K., Analogies between number fields and function fields. In *Collected Papers*, Vol. II, Springer-Verlag, Tokyo 2001, 606–611.

[21] Kato, K., Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}. I. In *Arithmetic algebraic geometry* (Trento, 1991), Lecture Notes in Math. 1553, Springer-Verlag, Berlin 1993, 50–163.

[22] Kato, K., p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque* **295** (2004), 117–290.

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

[24] Kubota, K., and Leopoldt, H.-W., Eine p-adische Theorie der Zetawerte. I. *J. Reine Angew. Math.* **214/215** (1964), 328–339.

[25] Kolyvagin, V. Euler systems. In *The Grothendieck Festschrift*, Vol. II, Progr. Math. 87, Birkhäuser, Boston, MA, 1990, 435–483.

[26] Kurihara, M., Iwasawa theory and Fitting ideals. *J. Reine Angew. Math.* **561** (2003), 39–86.

[27] Kurihara, M., On the structure of ideal class groups of CM-fields. *Documenta Math.* Extra Vol. (2003), 539–563.

[28] Kurihara, M., On the structure of Iwasawa modules. *Sūrikaisekikenkyūsho Kōkyūroku* **1451** (2005), 216–224.

[29] Mazur, B., and Swinnerton-Dyer, P, Arithmetic of Weil curves. *Invent. Math.* **25** (1974), 1–61.

[30] Mazur, B., Tate, J., and Teitelbaum, J, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.* **84** (1986), 1–48.

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

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

[33] McConnell, J. C., and Robson, J. C., *Noncommutative Noetherian rings*. Grad. Stud. in Math. 30, Amer. Math. Soc., Providence, RI, 2001.

[34] Perrin-Riou, B., Fonctions L p-adiques des représentations p-adiques. *Astérisque* **229** (1995).

[35] Ribet, K. A., A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. *Invent. Math.* **34** (1976), 151–162.

[36] Rohrlich, D. E., Root numbers of semi-stable elliptic curves in division towers. *Math. Res. Lett.* **13** (2–3) (2006), 359–376.

[37] Rubin, K., The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.* **103** (1991), 25–68.

[38] Rubin, K., *Euler systems*. Ann. of Math. Stud. 147, Princeton University Press, Princeton, NJ, 2000.

[39] Ritter, J. and Weiss, A., Toward equivariant Iwasawa theory, II. *Indag. Math.* (*N.S.*) **15** (2004), 549–572.

[40] Schneider, P., Motivic Iwasawa theory. In *Algebraic number theory*, Adv. Stud. Pure Math. 17, Academic Press, Boston, MA, 1989, 421–456.

[41] Skinner, C., Main conjectures and modular forms. Preprint.

[42] Thaine, F., On the ideal class groups of real abelian number fields. *Ann. of Math.* **128** (1988), 1–18.

[43] Venjakob, O., Characteristic elements in non-commutative Iwasawa theory. *J. Reine Angew. Math.* **583** (2005), 193–236.

[44] Wiles, A., The Iwasawa conjecture for totally real fields. *Ann. of Math.* **131** (1990), 493–540.

[45] Wiles, A., Modular elliptic curves and Fermat's last theorem. *Ann. of Math.* **141** (1995), 443–551.

[46] Weibel, C., and Yao, D., Localization for the K theory of noncommutative rings. In *Algebraic K-theory, commutative algebra, and algebraic geometry* (Santa Margherita Ligure, 1989), Contemp. Math. 126, Amer. Math. Soc., Providence, RI, 1992, 219–230.

Department of Mathematics, Kyoto University, Sakyo, Kyoto, Kyoto 606, Japan
E-mail: kzkt@math.kyoto-u.ac.jp