Introduction to the work of M. Kakde on the non-commutative main conjectures for totally real fields

John Coates, Dohyeong Kim

August 28, 2011

These notes are aimed at providing a not too technical introduction to both the background from classical Iwasawa theory for, as well as a detailed discussion of, the principal result (see Theorem 5.1) of Mahesh Kakde's fundamental paper [12] proving, subject to the Iwasawa conjecture, the non-commutative main conjecture for totally real p-adic Lie extensions of a number field. Kakde's work is the beautiful development of ideas initiated by Kazuya Kato in his important paper [14]. The material covered roughly corresponds to the oral lectures given by one of us at the Workshop. We have not attempted here to discuss the detailed methods of proof used either by Kakde in his paper, or by Ritter and Weiss in their important related work [13], leaving all of this to the written material of the subsequent lecturers at the Workshop. We would also like to particularly thank R. Greenberg and K. Ardakov for some very helpful comments which have been included in the present manuscript. In particular, we are very grateful to Greenberg for providing us with a detailed explanation of his observation (Theorem 4.6) that Wiles' work (Theorems 4.4 and 4.5) on the abelian main conjecture for totally real number fields, can be extended to include the case of abelian characters, whose order is divisible by p.

1 Notation

Throughout, F will denote a totally real finite extension of $\mathbb{Q}$, and p an odd prime. As always μ_{p^n}, with $1 \leq n \leq \infty$, is the group of all p^n-th roots of unity. Write F^{cyc} for the unique $\mathbb{Z}_p$-extension of F contained in $F(\mu_{p^\infty})$, and put $\Gamma = Gal(F^{cyc}/F)$ so that $\Gamma \simeq \mathbb{Z}_p$.

Let Σ be a fixed finite set of finite primes of F which contains all the primes dividing p, and write F_Σ for the maximal extension of F, which is unramified outside the primes in Σ and the infinite primes of F. If L is any extension of F contained in F_Σ, put $G_\Sigma(L) = Gal(F_\Sigma/L)$. Also, define $M(L)$ to be the maximal abelian p-extension of L contained in F_Σ, and put

$$X(L) = Gal(M(L)/L).$$

Assume now that L is Galois over F, so that $M(L)$ is also Galois over F. There is a natural left action of $Gal(L/F)$ on $X(L)$ defined by $g \cdot x = \tilde{g}x\tilde{g}^{-1}$, where $\tilde{g}$ denotes any lifting of g in $Gal(L/F)$ to $Gal(M(L)/F)$. As usual, this left action extends to a left action of the Iwasawa algebra $\Lambda(Gal(L/F))$, which is defined by

$$\Lambda(Gal(L/F)) = \varprojlim_{U} \mathbb{Z}_p[Gal(L/F)/U],$$

where U runs over the open normal subgroups of $Gal(L/F)$. Also, if W is any abelian group, $W(p)$ will denote the p-primary subgroup of W.

A Galois extension F_∞ of F is defined to be *an admissible p-adic Lie extension of F* if (i) F_∞ is totally real, (ii) the Galois group of F_∞ over F is a p-adic Lie group, (iii) F_∞/F is unramified outside a finite set of primes of F, and (iv) F_∞ contains F^{cyc}. Given such an admissible p-adic Lie extension, we shall always put

$$G = Gal(F_\infty/F),\ H = Gal(F_\infty/F^{cyc}),\ \Gamma = Gal(F^{cyc}/F),$$

and take Σ to be a finite set of primes of F containing all primes which are ramified in F_∞/F. If I denotes the ring of integers of some finite extension of $\mathbb{Q}_p$, it will also be convenient to write $I[[\Gamma]]$ for the Iwasawa algebra of Γ with coefficients in I. Fixing a topological generator γ of Γ, we can, as usual, identify $I[[\Gamma]]$ with the ring $I[[T]]$ of formal power series in an indeterminate T with coefficients in I, by mapping γ to $1+T$. Finally, we shall write $\mathfrak{A}(G)$ for the set of Artin representations of G, and $L_S(\rho, s)$ for the complex Artin L-function, with the Euler factors for the primes in Σ removed, of each ρ in $\mathfrak{A}(G)$.

2 Iwasawa's work on the cyclotomic theory

.

We use the above notation, and we stress that the base field F is always assumed to be totally real. In his fundamental paper [1], Iwasawa proved the following basic result which is the starting point for the whole theory.

Theorem 2.1. *For all totally real number fields F, $X(F^{cyc})$ is a finitely generated and torsion $\Lambda(\Gamma)$-module, which has no non-zero finite $\Lambda(\Gamma)$-submodule. Moreover, we have*

$$H^2(G_\Sigma(F^{cyc}), \mathbb{Q}_p/\mathbb{Z}_p) = 0. \tag{1}$$

Recall that one form of Leopoldt's conjecture, which remains unproven, is the assertion that F^{cyc} is the unique $\mathbb{Z}_p$-extension of F. The above theorem is established by noting that $X(F^{cyc})$ being $\Lambda(\Gamma)$-torsion is seen, by using the full force of global class field theory, to be equivalent to the assertion that the defect in the Leopoldt conjecture (i.e. the difference between the $\mathbb{Z}$-rank of the unit group and the $\mathbb{Z}_p$-rank of its closure, in the p-adic topology, in the product of the local unit groups at the primes above p) is bounded as one mounts the finite layers of the $\mathbb{Z}_p$-extension F^{cyc}/F. This boundedness of the defect of Leopoldt is then, in turn, shown to be implied by the boundedness of capitulation of ideal classes in the extension F^{cyc}/F. Finally, Iwasawa gives an ingenious proof of the boundedness of this capitulation. The vanishing statement (1) is then a consequence of an Euler characteristic argument which shows that, in the case of a totally real base field F, the Pontrjagin duals of the two modules $H^i(G_\Sigma(F^{cyc}), \mathbb{Q}_p/\mathbb{Z}_p)(i = 1, 2)$ have the same $\Lambda(\Gamma)$-rank.

In addition, a celebrated conjecture of Iwasawa will play an important role in the non-abelian theory developed later. By the structure theory, a finitely generated $\Lambda(\Gamma)$-module W is $\Lambda(\Gamma)$-torsion if and only if $W/W(p)$ is a finitely generated $\mathbb{Z}_p$-module. Moreover, $W(p)$ is finite if and only if its Iwasawa μ-invariant is zero.

Conjecture A: For totally real F, $X(F^{cyc})$ is a finitely generated $\mathbb{Z}_p$-module.

Note that, if Conjecture A is true, Theorem 2.1 shows that $X(F^{cyc})$ is in fact a free $\mathbb{Z}_p$-module of finite rank. The classical Iwasawa $\mu = 0$ conjecture is the assertion that, for every finite extension K of $\mathbb{Q}$, the Galois group of the maximal unramified abelian p-extension of K^{cyc} is a finitely generated $\mathbb{Z}_p$-module. It is well known that, by using an argument from Kummer theory, this classical Iwasawa conjecture for the totally imaginary field $K = F(\mu_p)$ implies Conjecture A for the totally real field F.

So far, Conjecture A has only been proven when F is an abelian extension of $\mathbb{Q}$, where it is a consequence of the Ferrero-Washington theorem for the cyclotomic $\mathbb{Z}_p$-extension of the field $F(\mu_p)$, which is again an abelian extension of $\mathbb{Q}$.

3 Admissible p-adic Lie extensions of F

.

The later material in this book will be concerned with an arbitrary admissible p-adic Lie extension F_∞/F, and the $\Lambda(G)$ module $X(F_\infty)$. We stress that this means, in particular, that F_∞ must also be totally real.

The first thing we should point out is that non-trivial examples of such admissible p-adic Lie extensions are not easy to come by. If Conjecture A is valid for F, we can always take F_∞ to be the field $M(F^{cyc})$. Moreover, it can be shown (see the Appendix) that, assuming Conjecture A is valid for F, we can find an admissible p-adic Lie extension of F such that (i) F_∞ is not contained in $M(F^{cyc})$, (ii) and G is pro-p with, only if the $\mathbb{Z}_p$-rank of $X(F^{cyc})$ is at least 2. Moreover, assuming that (i) Conjecture A is valid, (ii) that G is pro-p with no element of order p, and that (iii) G has dimension at least 2 as a p-adic Lie group, it follows from Theorem 2 below that $X(F_\infty) \neq 0$ if and only if the $\mathbb{Z}_p$-rank of $X(F^{cyc})$ is at least 2. Perhaps the most down to earth example of such an admissible p-adic Lie extension F_∞ with $X(F_\infty) \neq 0$ is to take F to be the maximal real subfield of the field generated over $\mathbb{Q}$ by the p-th roots of unity, where p is any odd prime such that at least two of the rational numbers

$$\zeta(\mathbb{Q}, -1), \zeta(\mathbb{Q}, -3), ..., \zeta(\mathbb{Q}, 4 - p)$$

have their numerators divisible by p (the smallest such prime is $p = 157$); here we take Σ to consist of the unique prime of F above p, and $\zeta(\mathbb{Q}, s)$ denotes the Riemann zeta function. It is the classical main conjecture for $X(F^{cyc})$ which guarantees that the $\mathbb{Z}_p$-rank of $X(F^{cyc})$ is at least 2 for such primes p. A much more esoteric example is given by Ramakrishna [2], who proves the existence of infinitely many Galois extensions L_∞ of $\mathbb{Q}$, which are totally real, whose Galois group J over $\mathbb{Q}$, is either $SL_2(\mathbb{Z}_7)$ or the quotient of $SL_2(\mathbb{Z}_7)$ by the subgroup generated by minus the identity $-I$ (where I is the unit matrix), and which are unramified outside a finite set T of primes of $\mathbb{Q}$. Thus we can take F_∞ to be the compositum of L_∞ and the cyclotomic $\mathbb{Z}_7$-extension of $\mathbb{Q}$. Note that if we define F to be the fixed field of the image in J of the group of matrices congruent to the identity modulo 7 in $SL_2(\mathbb{Z}_7)$, then the Galois group of F_∞/F will be pro-7, and have no element of order 7. Defining Σ to be the set of primes of F lying above either 7 or the primes in T, it follows from the above remarks that, assuming that Conjecture A is valid for F with p=7, then the $\mathbb{Z}_7$-rank of $X(F^{cyc})$ is at least 2, and $X(F_\infty) \neq 0$.

The full analogue of Theorem 2.1 for any admissible p-adic Lie extension is proven in the two papers [3], [7]. We say that a left $\Lambda(G)$-module W is $\Lambda(G)$-torsion if every element of W is annihilated by a non-zero divisor in $\Lambda(G)$.

Theorem 3.1. *For every admissible p-adic Lie extension F_∞/F, $X(F_\infty)$ is a finitely generated torsion $\Lambda(G)$-torsion module. Morevover, if G has no element of order p, then $X(F_\infty)$ has no non-zero pseudo-null submodule.*

Assuming that G is both pro-p and has no element of order p, it follows from the final assertion of Theorem 3.1 and the results of [7] that there is an exact sequence of $\Lambda(G)$-modules

$$0 \to X(F_\infty)(p) \to \bigoplus_{j=1}^{j=t} \Lambda(G)/p^{n_j}\Lambda(G) \to D \to 0, \tag{2}$$

where D is a pseudo-null $\Lambda(G)$-module. One then defines $\mu_G(X(F_\infty)) = n_1 + \cdots + n_t$. In particular, we have $X(F_\infty)(p) = 0$ if and only if $\mu_G(X(F_\infty)) = 0$. We shall see below that a suitable form of Conjecture A implies a strong statement about the module $X(F_\infty)$, which shows, in particular, that $\mu_G(X(F_\infty)) = 0$.

In our present state of knowledge, we do not know how to even formulate the main conjecture using the result of this theorem alone (we cannot define a characteristic element for $X(F_\infty)$ assuming only that it is finitely generated and torsion over $\Lambda(G)$, even if we impose the additional hypothesis that $\mu_G(X(F_\infty)) = 0$.). In order to overcome this difficulty, we follow [5] and introduce the category $\mathfrak{M}_H(G)$ consisting of all finitely generated $\Lambda(G)$-modules W such that $W/W(p)$ is finitely generated over $\Lambda(H)$, where we recall that $H = Gal(F_\infty/F^{cyc})$. While it seems very reasonable to conjecture that $X(F_\infty)$ always belongs to the category $\mathfrak{M}_H(G)$, we unfortunately cannot prove this unconditionally at present. Nevertheless, assuming this conjecture, the following result is proven in the Appendix.

Theorem 3.2. *Assume that the p-adic Lie extension F_∞/F is such that (i) G is pro-p and has no element of order p, (ii) G has dimension at least 2 as a p-adic Lie group, and (iii) $X(F_\infty)$ belongs to the category $\mathfrak{M}_H(G)$. Then $\mu_G(X(F_\infty)) = \mu_\Gamma(X(F^{cyc}))$, and $X(F_\infty)/X(F_\infty)(p)$ has $\Lambda(H)$-rank equal to $r-1$, where r is the $\mathbb{Z}_p$-rank of $X(F^{cyc})/X(F^{cyc})(p)$.*

Our present inability to prove that $X(F_\infty)$ lies in the category $\mathfrak{M}_H(G)$ leads us to work with a stronger conjecture in the subsequent analytic and algebraic arguments.

Iwasawa Conjecture: The admissible p-adic Lie extension F_∞/F will be said to satisfy the *Iwasawa conjecture* if there exists a finite extension F' of F in F_∞ such that (i) the Galois group of F_∞ over F' is pro-p, and (ii) $X(F'^{cyc})$ is a finitely generated $\mathbb{Z}_p$-module.

We remark that, by the theorem of Ferrero-Washington, this Iwasawa conjecture is true for all p-adic Lie extensions F_∞/F such that F is an abelian extension of $\mathbb{Q}$ and the Galois group G is pro-p. In particular, when F is an abelian extension of $\mathbb{Q}$ and $F_\infty = M(F^{cyc})$, the Iwasawa conjecture is valid.

Theorem 3.3. . *Assume that the p-adic Lie extension F_∞/F satisfies the Iwasawa Conjecture. Then $X(F_\infty)$ is finitely generated over $\Lambda(H)$, and $X(F_\infty)(p) = 0$.*

Proof. Put $H' = Gal(F_\infty/F'^{cyc})$. Then we have the exact sequence of inflation restriction

$$0 \to H^1(H', \mathbb{Q}_p/\mathbb{Z}_p) \to Hom(X(F'^{cyc}), \mathbb{Q}_p/\mathbb{Z}_p) \to Hom(X(F_\infty)_{H'}, \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(H', \mathbb{Q}_p/\mathbb{Z}_p).$$

Now $H^i(H', \mathbb{Q}_p/\mathbb{Z}_p)$ is a cofinitely generated $\mathbb{Z}_p$-module for all $i \geq 0$. Hence, assuming that $X(F'^{cyc})$ is a finitely generated $\mathbb{Z}_p$-module, it follows that $X(F_\infty)_{H'}$ is also a finitely generated $\mathbb{Z}_p$-module. But, as H' is pro-p, $\Lambda(H')$ is a local ring, and so it follows from Nakayama's lemma that $X(F_\infty)$ is finitely generated over $\Lambda(H')$, and so all the more so over $\Lambda(H)$. To prove the final assertion of the theorem, we note that we can find an open subgroup H'' of H' such that H'' is pro-p and has no element of order p (possibly $H'' = 0$). Since $X(F_\infty)$ is also finitely generated over $\Lambda(H'')$, a theorem of Venjakob asserts that every $\Lambda(G)$ submodule of $X(F_\infty)$, which is $\Lambda(H'')$-torsion, is pseudo-null as a $\Lambda(G)$-module, and so must be zero by Theorem 3.1. In particular, this shows that $X(F_\infty)(p) = 0$. □

4 The classical abelian main conjecture

In this section, we discuss the classical abelian main conjecture for an arbitrary admissible p-adic Lie extension F_∞/F which will be assumed throughout this section to satisfy the:-

Abelian Hypothesis. $G = Gal(F_\infty/F)$ is an abelian p-adic Lie group of dimension 1.

As before, S will denote the set of primes of F which ramify in F_∞. We fix a lifting of $\Gamma = Gal(F^{cyc}/F)$ to G, which we denote by the same symbol Γ. Thus, since G is abelian, this means that we have $G = H \times \Gamma$. We define K to be the fixed field of the subgroup

Γ of G, so that $K \cap F^{cyc} = F$, and F_∞ is the compositum of K and F^{cyc}. Let $\hat{H}$ be the group of 1-dimensional characters of H. Write

$$\kappa_F : Gal(F(\mu_{p^\infty})/F) \to \mathbb{Z}_p^\times$$

for the cyclotomic character. As we can view Γ as a subgroup of $Gal(F(\mu_{p^\infty})/F)$, it makes sense to consider the restriction of κ_F to Γ. In what follows, we then consider κ_F as a character of G by defining it always to be trivial on H.

While complex L-functions can be defined in great generality via Euler products, nothing like this seems to be true in the p-adic world, and, at present, our only way to define p-adic L is via p-adic interpolation of essentially algebraic special values of complex L-functions. Viewing an element χ in $\hat{H}$ as being complex valued, let $L_\Sigma(\chi, s)$ be the imprimitive complex L-function attached to χ, with the Euler factors corresponding to the primes in Σ omitted from its Euler product. The following basic result is due to Siegel.

Theorem 4.1. *For each χ in $\hat{H}$, and each even integer $n > 0$, $L_\Sigma(\chi, 1-n)$ belongs to the field $\mathbb{Q}(\chi)$, which is generated over $\mathbb{Q}$ by the values of χ.*

In fact, Siegel's proof shows that

$$L_\Sigma(\chi^\sigma, 1-n) = L_\Sigma(\chi, 1-n)^\sigma \tag{3}$$

for all σ in the absolute Galois group of $\mathbb{Q}$, and all even integers $n > 0$, and even allows us to define this value intrinsically when the character χ is no longer assumed to have complex values. In fact, we shall assume from now on that the χ in $\hat{H}$ all have values in the algebraic closure of $\mathbb{Q}_p$.

Let $\mathcal{O}$ be the ring of integers of the field obtained by adjoining the values of all χ in $\hat{H}$ to $\mathbb{Q}_p$, and let $\Lambda_\mathcal{O}(G)$ be the Iwasawa algebra of G with coefficients in $\mathcal{O}$. Write $Q_\mathcal{O}(G)$ for the ring of fractions of $\Lambda_\mathcal{O}(G)$ (i.e. the localization of this ring with respect to its set of non-zero divisors). An element μ of $Q_\mathcal{O}(G)$ is defined to be a *pseudo-measure* on G if $(\sigma - 1)\mu$ is in $\Lambda_\mathcal{O}(G)$ for all σ in G. If $\psi : G \to \mathcal{O}^\times$ is any continuous homomorphism, which is distinct from the trivial homomorphism of G, which we denote by $\mathbf{1}$, it is easily seen that one can define the integral of ψ against μ, which we denote by

$$\int_G \psi d\mu,$$

and which is a well defined element of the fraction field of $\mathcal{O}$. The following theorem, which generalizes many earlier results starting with Kummer, is due to Cassou-Nogues and Deligne-Ribet.

Theorem 4.2. *Assume that F_∞/F satisfies the abelian hypothesis. Then there exists a unique pseudo-measure $\zeta_{F_\infty/F}$ on $G = H \times \Gamma$ such that, for all χ in $\hat{H}$, we have*

$$\int_G \chi {\kappa_F}^n d\zeta_{F_\infty/F} \ = \ L_\Sigma(\chi, 1-n), \tag{4}$$

for all integers $n > 0$ with $n \equiv 0$ mod δ, where $\delta = [F(\mu_p) : F]$.

This theorem is easily seen to imply the following assertion. For each character χ in $\hat{H}$, let $\mathcal{O}_\chi$ be the ring of integers of the field obtained by adjoining the values of χ to $\mathbb{Q}_p$, and let $\mathcal{O}_\chi[[\mathrm{T}]]$ be the ring of formal power series in an indeterminate T with coefficients in $\mathcal{O}_\chi$. Fix, for the remainder of this section, a topological generator γ of Γ. Then, if $\chi \neq \mathbf{1}$, there exists a unique formal power series $W_\chi(T)$ in $\mathcal{O}_\chi[[\mathrm{T}]]$ such that

$$W_\chi(\kappa_F(\gamma)^n - 1) = L_\Sigma(\chi, 1-n),$$

for all integers $n > 0$ with $n \equiv 0 \bmod \delta$. In addition, if $\chi = \mathbf{1}$, there exists a unique power series $W_{\mathbf{1}}(T)$ in $\mathbb{Z}_p[[\mathrm{T}]]$ such that

$$W_{\mathbf{1}}(\kappa(\gamma_F)^n - 1)/(\kappa_F(\gamma)^n - 1) = \zeta_\Sigma(F, 1-n),$$

where $\zeta_\Sigma(F, s)$ denotes the complex zeta function of F, with the Euler factors removed at the primes in Σ. Let π_χ be any fixed local parameter for the ring $\mathcal{O}_\chi$. We plainly can write

$$W_\chi(T) = \pi_\chi^{\mu_\chi} V_\chi(T), \tag{5}$$

where μ_χ is a non-negative integer, and $V_\chi(T)$ is a power series in $\mathcal{O}_\chi[[\mathrm{T}]]$, with at least one of its coefficients a unit in $\mathcal{O}_\chi$. It is conjectured that we always have $\mu_\chi = 0$ for every F_∞/F and every χ in $\hat{H}$, but this has only been proven in the case $F = \mathbb{Q}$ by Ferrero-Washington, and it is unknown for every other totally real base field other than $\mathbb{Q}$.

The aim of the abelian main conjecture is to give a precise relation between the analytic pseudo-measure $\zeta_{F_\infty/F}$ on the one hand, and the algebraic structure of the arithmetic $\Lambda_{\mathcal{O}}(G)$-module $X(F_\infty)$ on the other hand. However, the exact formulation of this relationship is not straightforward from a classical point of view, because there is no known structure theory for finitely generated torsion $\Lambda_{\mathcal{O}}(G)$-modules when p divides the order of H. For each χ in $\hat{H}$, let

$$e_\chi = \#(H)^{-1} \sum_{h \in H} \chi(h) h^{-1}$$

be the orthogonal idempotent of χ in the group ring of H with coefficients in the field of fractions $\mathcal{L}$ of $\mathcal{O}_\chi$. The simplest thing to do is to simply consider

$$Z(F_\infty) = X(F_\infty) \otimes_{\mathbb{Z}_p} \mathcal{L}, \;\; Z(F_\infty)_\chi = e_\chi Z(F_\infty), \tag{6}$$

which are both finite dimensional vector spaces over $\mathcal{L}$ by Theorem 2.1. We then define $R_\chi(T)$ to be the characteristic polynomial of $\gamma - 1$ acting on $Z(F_\infty)_\chi$. We omit the proof of the following technical lemma, which is due to Greenberg (see [10], Proposition 1).

Lemma 4.3. *Let χ be any element of $\hat{H}$, and let K' be any intermediate field between F and K such that χ is trival on $Gal(K/K')$. Write χ' for χ, when viewed as a character of $Gal(K'/F)$, and let F'_∞ be the compositum of K' and F^{cyc}. Then $Z(F_\infty)_\chi$ is isomorphic to $Z({F'}_\infty)_{\chi'}$ as representations of Γ.*

In particular, this lemma shows that the polynomial $R_\chi(T)$ depends only the character χ of H, and not on the particular finite extension of F such that χ factors through the Galois group over F of this extension.

The first fundamental result of Wiles (see Theorem 1.3 of [11]) in the direction of the main conjecture for all totally real number fields F is the following.

Theorem 4.4. *Assume that F_∞/F satisfies the abelian hypothesis. Then, for all characters χ of H, we have*

$$V_\chi(T)\mathcal{O}_\chi[[\mathrm{T}]] = \mathrm{R}_\chi(\mathrm{T})\mathcal{O}_\chi[[\mathrm{T}]]. \tag{7}$$

The problem with this result is that it does not tell us anything about the μ-invariants on either the analytic or the algebraic sides. Of course, the analytic μ-invariant is the integer μ_χ appearing in (5), and is valid for all characters χ of H, irrespective of whether the order of χ is divisible by p or not. The definition of the algebraic μ-invariant is much more delicate. We first explain what to do in the easy case, when the order of χ is prime to p. Assuming this to be the case, we may also suppose that K is exactly the fixed field of the kernel of χ, as this does not change the polynomial $R_\chi(T)$ by Lemma 4.3. Define

$$X(F_\infty)_\chi = e_\chi(X(F_\infty) \otimes_{\mathbb{Z}_p} \mathcal{O}_\chi).$$

Now, by Theorem 2.1, $X(F_\infty)_\chi$ is a finitely generated torsion $\mathcal{O}_\chi[[\mathrm{T}]]$-module, and thus, by the well known structure theory for such modules and the Weierstrass preparation theorem, it has a characteristic ideal of the form $C_\chi(T)\mathcal{O}_\chi[[\mathrm{T}]]$, where $C_\chi(\mathrm{T})$ is a polynomial in $\mathcal{O}_\chi[\mathcal{T}]$ of such that

$$C_\chi(T) = \pi_\chi^{\nu_\chi} R_\chi(T), \tag{8}$$

for some integer $\nu_\chi \geq 0$; here $R_\chi(T)$ is, as above the characteristic polynomial of $\gamma - 1$ acting on $Z(F_\infty)_\chi$. The second fundamental result of Wiles (see Theorem 1.4 of [11]) is the following.

Theorem 4.5. *Assume that F_∞/F satisfies the abelian hypothesis. If χ in $\hat{H}$, has order prime to p, we have*

$$\mu_\chi = \nu_\chi. \tag{9}$$

In particular, when combined with Theorem 4.4, this result proves the main conjecture asserting that

$$W_\chi(T)\mathcal{O}_\chi[[\mathrm{T}]] = \mathrm{C}_\chi(\mathrm{T})\mathcal{O}_\chi[[\mathrm{T}]], \tag{10}$$

for all characters χ of H of order prime to p.

We are very grateful to R. Greenberg (private communication) for the following explanation of how one can define the analogue of the algebraic μ-invariant ν_χ appearing in

(8) even for characters χ of H whose order is divisible by p, and then show that the main conjecture (10) still remains valid for such characters. As we shall need to vary the base field F in this argument, for the remainder of this section we shall write $W_{F,\chi}(T)$, $\mu_{F,\chi}$,... to indicate the dependence of the above quantities on the base field F. Fix a character χ of H, whose order is divisible by p. We shall assume that K is the fixed field of the kernel of χ. Now we can write χ in the form $\chi = \psi\rho$, where ψ is a character of H of order prime to p, and ρ has p-power order. Define $\rho' = \rho^p$, and write L', L for the fixed fields of $\mathrm{Ker}(\rho')$, $\mathrm{Ker}(\rho)$, respectively. We can now take the restriction ψ_L (resp. $\psi_{L'}$) of ψ to the absolute Galois group of L (resp. the absolute Galois group of L'). Then K is the fixed field of $\mathrm{Ker}(\psi_L)$, and we define K' to be the fixed field of $\mathrm{Ker}(\psi_{L'})$. Thus we have the tower of fields

$$F \subset L' \subset L \subset K' \subset K. \tag{11}$$

Write F'_∞ for the compositum of K' with F^{cyc}, and, as before, let F_∞ be the compositum of K with F^{cyc}. To lighten our notation, put

$$\mathrm{J} = \mathcal{O}_\psi,\ \mathrm{I} = \mathcal{O}_\rho,\ \mathrm{E} = \mathcal{O}_\chi, \tag{12}$$

so that E is the ring generated over J by the values of ρ. We first observe that, up to a pseudo-isomorphism of Γ-modules, we can identify $X(F'_\infty)$ with a quotient of $X(F_\infty)$. Indeed, let P (resp. P') be the Sylow p-subgroup of $Gal(K/F)$ (resp. $Gal(K'/F)$), and put

$$\Omega = Ker(P \to P'), \tag{13}$$

so that Ω has order p. Then the natural map from $X(F_\infty)_\Omega$ to $X(F'_\infty)$, which is the dual of the restriction map on Galois cohomology, has finite kernel and cokernel. Indeed, the cokernel is finite because it is dual to $H^1(Gal(K/K'), \mathbb{Q}_p/\mathbb{Z}_p)$, and the kernel is finite because it is dual to a submodule of $H^2(Gal(K/K'), \mathbb{Q}_p/\mathbb{Z}_p)$. In particular, it follows that $X(F_\infty)_\Omega$ and $X(F'_\infty)$ have the same characteristic power series as Γ-modules. We then define

$$\Pi(F_\infty) = Ker(X(F_\infty) \to X(F_\infty)_\Omega). \tag{14}$$

Explicitly, we have $\Pi(F_\infty) = (\tau - 1)X(F_\infty)$, where τ is any generator of Ω. Now the group ring $\mathbb{Z}_p[P]$ acts on $\Pi(F_\infty)$, and this action factors through an action of the ring

$$B = \mathbb{Z}_p[P]/(1 + \tau + ... + \tau^{p-1})\mathbb{Z}_p[P].$$

But evaluation at the character ρ defines an isomorphism from B onto the ring I. Thus we see that $\Pi(F_\infty)$ has a natural structure as an $I[[\Gamma]]$-module. Now ψ is a faithful character of $Gal(K/L)$ of order prime to p, and thus, for any $\mathbb{Z}_p[Gal(K/L)]$-module A, we may define

$$A_\psi = e_\psi(A \otimes_{\mathbb{Z}_p} J).$$

In particular, we have

$$\Pi(F_\infty)_\psi = Ker(X(F_\infty)_\psi \to (X(F_\infty)_\psi)_\Omega). \tag{15}$$

It is clear that $\Pi(F_\infty)_\psi$ has a structure as an $E[[\Gamma]]$-module, because I acts on $\Pi(F_\infty)$. Moreover, since $X(F_\infty)$ is a finitely generated torsion $\mathbb{Z}_p[[\Gamma]]$-module, it follows that $\Pi(F_\infty)_\psi$ is a finitely generated torsion $E[[\Gamma]]$-module. As before, let π_χ be any local parameter of the ring $E = \mathcal{O}_\chi$. Then, by the structure theory for finitely generated torsion $E[[\Gamma]]$-modules, $\Pi(F_\infty)_\psi$ will have a characteristic ideal of the form $\mathfrak{C}_\chi(T)E[[\mathrm{T}]]$, where $\mathfrak{C}_\chi(T)$ is a polynomial such that

$$\mathfrak{C}_\chi(T) = \pi_\chi^{\nu_\chi}\mathfrak{R}_\chi(\mathrm{T}), \tag{16}$$

where ν_χ is some integer ≥ 0, and $\mathfrak{R}_\chi(\mathrm{T})$ is a monic polynomial in $E[T]$. It is this integer ν_χ which we define to be the algebraic μ-invariant of χ when p divides the order of χ. On the other hand, since $(X(F_\infty)_\psi)_\Omega$ is pseudo-isomorphic as a $J[[\Gamma]]$-module to $X(F'_\infty)_\psi$, it follows from (15) that the μ-invariant of $\Pi(F_\infty)_\psi$ as a $J[[\Gamma]]$-module must be equal to $\nu_{\psi,L} - \nu_{\psi,L'}$, where the subscripts L and L' indicate that these invariants are now taken with respect to these respective base fields. But, as E is a totally ramified extension of J of degree $p^{m-1}(p-1)$, where p^m is the exact order of the character ρ, it is clear that the μ-invariant of $\Pi(F_\infty)_\psi$ as an $E[[\Gamma]]$-module is equal to to its μ-invariant as a $J[[\Gamma]]$-module. This is because the residue fields of J and E have the same order. Hence we obtain

$$\nu_\chi = \nu_{\psi,L} - \nu_{\psi,L'}. \tag{17}$$

Recall that he analytic invariant μ_χ is defined by the equation (5). As Greenberg has remarked, we can now easily establish the following generalization of Theorem 4.5.

Theorem 4.6. *Assume that F_∞/F satisfies the abelian hypothesis, where H is an arbitrary finite abelian group. Then, for all characters χ of H , we have*

$$\mu_\chi = \nu_\chi. \tag{18}$$

Proof. Since we can view ψ, which has order prime to p, as a character of both $Gal(K/L)$ and $Gal(K'/L')$, we can apply Theorem 4.5 to both of the extensions F_∞/L and F'_∞/L'. We conclude that

$$\mu_{\psi,L} = \nu_{\psi,L},\ \mu_{\psi,L'} = \nu_{\psi,L'}, \tag{19}$$

where again the subscripts L and L' mean the invariants are taken relative to the respective base fields. Thus it follows from (17) that

$$\nu_\chi = \mu_{\psi,L} - \mu_{\psi,L'}. \tag{20}$$

To conclude the proof, we need an analytic argument. Let $\mathcal{D}$ be the set of characters of $Gal(L/F)$ which do not factor through $Gal(L'/F)$. Plainly $\mathcal{D}$ consists of all the characters

$\eta = \rho^a$, where a runs over the integers mod p^m which are prime to p. It then follows easily from the Artin formalism for complex L-functions that

$$W_{\psi,L}(T) = W_{\psi,L'}(T) \times \prod_{\eta} W_{\psi\eta,F}(T), \tag{21}$$

where now η runs over all elements of $\mathcal{D}$. Write Δ for the Galois group of the fraction field of E over the fraction field of J, and recall that this extension is totally ramified of degree $p^{(m-1)}(p-1)$. We conclude easily from (3) that all of the power series $W_{\psi\eta,F}(T)$ with $\eta \in \mathcal{D}$ are conjugate under the action of Δ. Hence, since our extension is totally ramified, it follows that all of these power series must have the same μ-invariant, which must be equal to μ_χ because χ is one of the characters in $\mathcal{D}$. Noting that the invariants $\mu_{\psi,L}$ and $\mu_{\psi,L'}$ are defined using a local parameter of the unramified extension J of $\mathbb{Z}_p$, it now follows from (21) that

$$\mu_{\psi,L} - \mu_{\psi,L'} = \mu_\chi. \tag{22}$$

Combining (21) and (22), the proof of the theorem is now complete. □

In particular, when combined with Theorem 4.4, Theorem 4.6 proves the abelian main conjecture in general, asserting that, for every character χ of H we have

$$W_\chi(T)\mathcal{O}_\chi[[\mathrm{T}]] = \pi_\chi^{\nu_\chi}\mathrm{R}_\chi(\mathrm{T})\mathcal{O}_\chi[[\mathrm{T}]]. \tag{23}$$

5 The non-abelian main conjecture

Throughout this section, F_∞/F will be an arbitrary admissible p-adic Lie extension, which we will always assume for simplicity satisfies:-

Hypothesis B. The group $G = Gal(F_\infty/F)$ has no element of order p.

While the non-abelian main conjecture can be formulated for all admissible p-adic Lie extensions, the point of imposing this hypothesis is that it makes the whole discussion of the homological properties of the G-module $X(F_\infty)$ much simpler. In particular, Hypothesis B implies that the Iwasawa algebra $\Lambda(G)$ has finite global dimension, and that G has finite p-homological dimension, which is equal to the dimension of G as a p-adic Lie group. Note that Iwasawa [1] has proven that, for every finite extension F of $\mathbb{Q}$, there is no non-zero finite $\Lambda(\Gamma)$-submodule of $X(F^{cyc})$. Hence, whenever Conjecture A is valid for F (for example, when F is an abelian extension of $\mathbb{Q}$), it follows that Hypothesis B is valid in the important example given by taking $F_\infty = M(F^{cyc})$. Note also that Leopoldt's conjecture implies that such a G must be non-commutative whenever $F_\infty \neq F^{cyc}$.

We now rapidly recall the statement of the main conjecture. As in [5], let S be the subset of $\Lambda(G)$ defined by

$$S = \{f \in \Lambda(G) : \Lambda(G)/\Lambda(G)f \text{ is a finitely generated } \Lambda(H) - \text{module.}\}. \tag{24}$$

Further, let S^* be the subset of $\Lambda(G)$ consisting of all elements $p^n s$, where n is some integer ≥ 0, and s is in S. Then the following results are proven by rather elementary arguments in [5]. Firstly, S, and so also S^*, are multiplicatively closed sets of non-zero divisors in $\Lambda(G)$, which satisfy the left and right Ore condition. Thus we can define the localized rings $\Lambda(G)_S$ and $\Lambda(G)_{S*}$, which are, of course, non-commutative once G is not abelian. Secondly, let $\mathfrak{N}_H(G)$ (resp. $\mathfrak{M}_H(G)$) be the category of all finitely generated left $\Lambda(G)$-modules W such that W (resp. $W/W(p)$) is finitely generated over $\Lambda(H)$. Then $\mathfrak{N}_H(G)$ (resp. $\mathfrak{M}_H(G)$) is precisely the category of finitely generated left $\Lambda(G)$-modules which are S-torsion (resp. S^*-torsion). Write $K_0(\mathfrak{N}_H(G))$ (resp. $K_0(\mathfrak{M}_H(G))$) for the Grothendieck groups of these two categories. For any ring R with unit, denote by $K_1(R)$ the K_1-group of R. By classical algebraic K-theory, we have boundary maps

$$\partial : K_1(\Lambda(G)_S) \to K_0(\mathfrak{N}_H(G)),\ \partial^* : K_1(\Lambda(G)_{S^*}) \to K_0(\mathfrak{M}_H(G)), \tag{25}$$

whose kernel in both cases is the relevant image of $K_1(\Lambda(G))$. Moreover, it is shown in [5] that both of these maps are surjective. Thus, for each module W in the category $\mathfrak{N}_H(G)$ (resp. $\mathfrak{M}_H(G)$), we define a *characteristic element* of W to be any ζ_W in $K_1(\Lambda(G)_S)$ (resp. $K_1(\Lambda(G)_{S^*})$ such that $\partial(\zeta_W)$ (resp. $\partial^*(\zeta_W)$) is equal to the class of W in the relevant K_0.

Granted that our $\Lambda(G)$-module $X(F_\infty)$ lies in the appropriate category, the main conjecture, will, as always, assert that its characteristic element can be taken to be a p-adic L-function, in a sense that we now make precise. Firstly, as is explained in [5], we can always evaluate an element ζ of $K_1(\Lambda(G)_S)$ (resp. $K_1(\Lambda(G)_{S^*})$ at any continuous homomorphism from G into $GL_n(\mathcal{O})$, where $\mathcal{O}$ is the ring of integers of some finite extension of $\mathbb{Q}_p$, obtaining a well-defined value $\zeta(\rho)$ in the fraction field of $\mathcal{O}$, or the value ∞. In particular, let $\mathfrak{A}(G)$ be the set of all Artin representations of G. Thus an element ρ of $\mathfrak{A}(G)$ will be a homomorphism

$$\rho : G \to GL_n(\mathcal{O}), \tag{26}$$

which factors through a finite quotient of G, where again $\mathcal{O}$ is the ring of integers of some finite extension of $\mathbb{Q}_p$. For each $\rho \in \mathfrak{A}(G)$, write $L_\Sigma(\rho, s)$ for the complex L-function of ρ, with the Euler factors for the primes in Σ omitted from its Euler product. Now, combining Theorem 4.1 with Brauer's theorem on finite groups, it follows that, for each even integer $n > 0$ and each ρ in $\mathfrak{A}(G)$, the value $L_\Sigma(\rho, 1-n)$ is an algebraic number satisfying

$$L_\Sigma(\rho^\sigma, 1-n) = L_\Sigma(\rho, 1-n)^\sigma, \tag{27}$$

for all σ in the absolute Galois group of $\mathbb{Q}$. We then have the following conjectural analogue of Theorem 4.2.

Conjecture C. For every admissible p-adic Lie extension F_∞/F, there exists $\zeta_{F_\infty/F}$ in $K_1(\Lambda(G)_{S^*})$ such that

$$\zeta_{F_\infty/F}(\rho\kappa_F^n) = L_\Sigma(\rho, 1-n), \tag{28}$$

for all $\rho \in \mathfrak{A}(G)$ and all integers $n > 0$ with $n \equiv 0 \mod [F(\mu_p) : F]$; here κ_F is the character giving the action of the absolute Galois group of F on the group of all p-power roots of unity.

Granted the existence of this p-adic L-function, the general main conjecture can now be stated as follows. If W is any module in $\mathfrak{M}_H(G)$, write $[W]$ for the class of W in the Grothendieck group of this category.

Conjecture D. Let F_∞/F be an admissible p-adic Lie extension satisfying Hypothesis B. Assume that $X(F_\infty)$ belongs to the category $\mathfrak{M}_H(G)$, and that there exists $\zeta_{F_\infty/F}$ in $K_1(\Lambda(G)_{S^*})$ satisfying (28) . Then

$$\partial^*(\zeta_{F_\infty/F})) = [X(F_\infty)] - [\mathbb{Z}_p]. \tag{29}$$

In his remarkable paper [12], Kakde has proven this main conjecture, provided the admissible p-adic Lie extension satisfies the generalized Iwasawa conjecture.

Theorem 5.1. *Assume that F_∞/F is an admissible p-adic Lie extension satisfying Hypothesis B. If the generalized Iwasawa conjecture holds for F_∞/F, then there exists $\zeta_{F_\infty/F}$ in $K_1(\Lambda(G)_S)$, satisfying* (28) *for all $\rho \in \mathfrak{A}(G)$ and all integers $n > 0$ with $n \equiv 0$ mod $[F(\mu_p) : F]$, and such that*

$$\partial(\zeta_{F_\infty/F}) = [X(F_\infty)] - [\mathbb{Z}_p].$$

The lectures in this conference are aimed primarily at an account of his proof. The most important unconditional case of this theorem is as follows.

Corollary 5.2. *Let F be a real abelian field, and take $F_\infty = M(F^{cyc})$. Then there exists $\zeta_{F_\infty/F}$ in $K_1(\Lambda(G)_S)$, satisfying* (28) *for all $\rho \in \mathfrak{A}(G)$ and all integers $n > 0$ with $n \equiv 0$ mod $[F(\mu_p) : F]$, and such that*

$$\partial(\zeta_{F_\infty/F}) = [X(F_\infty)] - [\mathbb{Z}_p].$$

For example, if we take F to be the maximal real subfield of $\mathbb{Q}(\mu_{157})$, take Σ to consist of the unique prime of F above p , and let $F_\infty = M(F^{cyc})$, then $H = {\mathbb{Z}_p}^2$, and Theorem 6.6 shows that $X(F_\infty)$ is non-zero, being isomorphic as a $\Lambda(H)$-module to a submodule of finite index of $\Lambda(H)$.

We end by briefly discussing possible applications of Theorem 5.1. Write $d+1$, where d is an integer ≥ 0, for the dimension of G. We continue to assume that G has no element of order p, so that G has p-homological dimension equal to $d+1$. At present, all known applications of Theorem 5.1 are to the computation of the G-Euler characteristics of certain twists of the the Iwasawa module $X(F_\infty)$. If W is any finitely generated $\Lambda(G)$-module, we recall that W is said to have finite G-Euler characteristic if all of the homology groups $H_i(G, W)$ are finite for all $i = 0, ..., d+1$, and then this Euler characteristic is defined to be

$$\chi(G, W) = \prod_{i=0}^{d+1} (\#(H_i(G, W)))^{(-1)^i}. \tag{30}$$

Similarly, if V is any finitely generated $\Lambda(\Gamma)$-module, we have the analogous notion of it having a finite Γ-Euler characteristic, defined by

$$\chi(\Gamma, V) = \#(H_0(\Gamma, V))/\#(H_1(\Gamma, V)).$$

Moreover, the Hochschild-Serre spectral sequence shows that W will have finite G-Euler characteristic if and only if the Γ-modules $H_i(H, W)$ have finite Γ-Euler characteristic for all $i = 0, ..., d$, and when this is the case, we will have

$$\chi(G, W) = \prod_{i=0}^{d} \chi(\Gamma, H_i(H, W))^{(-1)^i}. \tag{31}$$

Also, if m is any integer, $W(m)$ will denote as usual the m-fold Tate twist of W (i.e. the tensor product over $\mathbb{Z}_p$ of W with the m-fold tensor product with itself of the Tate module of μ_{p^∞}, endowed with the diagonal action of the absolute Galois group of F). Note also that when m is any integer with $m \equiv 0 \bmod [F(\mu_p) : F]$, G acts on $\mathbb{Z}_p(m)$.

Our aim now is to see what can be proven about the G-Euler charactersitic of $X(F_\infty)(-n)$ when n is any integer > 0 with $n \equiv 0 \bmod [F(\mu_p) : F]$. In the special case when $F_\infty = F^{cyc}$, it is a classical consequence of the abelian main conjecture that, for such integers $n > 0$, $X(F^{cyc})(-n)$ has finite Γ-Euler characteristic, given by

$$\chi(\Gamma, X(F^{cyc})(-n)) = |w_n(F)\zeta_\Sigma(F, 1-n)|_p^{-1}, \tag{32}$$

where $w_n(F)$ denotes the largest integer r such that the Galois group of $F(\mu_r)$ over F has exponent n. In the general case, the following proposition holds:-

Proposition 5.3. *Let n be any integer > 0 with $n \equiv 0$ mod $[F(\mu_p) : F]$. Then $X(F_\infty)(-n)$ has finite G-Euler characteristic if and only if $\mathbb{Z}_p(-n)$ has finite G-Euler characteristic. Moreover, assuming that these Euler characteristics are finite, we have*

$$\chi(G, X(F_\infty)(-n))/\chi(G, \mathbb{Z}_p(-n)) = |\zeta_\Sigma(F, 1-n)|_p^{-1}. \tag{33}$$

Proof. We first note that H acts trivially on $\mathbb{Z}_p(-n)$ when $n \equiv 0 \bmod [F(\mu_p) : F]$. Thus Proposition (6.1) gives immediately an isomorphism of Γ-modules

$$H_i(H, X(F_\infty)(-n)) \simeq H_{i+2}(H, \mathbb{Z}_p(-n)), \tag{34}$$

for all $i \geq 1$. Similarly, Proposition (43) gives the exact sequence of Γ-modules

$$0 \longrightarrow H_2(H, \mathbb{Z}_p(-n)) \longrightarrow H_0(H, X(F_\infty)(-n)) \longrightarrow X(F^{cyc})(-n) \longrightarrow H_1(H, \mathbb{Z}_p(-n)) \longrightarrow 0. \tag{35}$$

Now $X(F_\infty)(-n)$ has finite G-Euler characteristic if and only if the

$$H_i(H, X(F_\infty)(-n)) \;\; (i = 0, ..., d) \tag{36}$$

all have finite Γ-Euler characteristics. As $X(F^{cyc})(-n)$ has finite Γ-Euler characteristic, we conclude from the exact sequences (33) and (35) that the Γ-modules (36) will have finite Euler characteristics if and only if the Γ-modules $H_i(H, \mathbb{Z}_p(-n))$, for $i = 2, ..., d$, all have finite Euler characteristics. Moreover, $H_1(H, \mathbb{Z}_p(-n))$ has finite Euler characteristic since it is a quotient of $X(F^{cyc})(-n)$, and

$$\chi(\Gamma, H_0(H, \mathbb{Z}_p(-n))) = |w_n(F)|_p^{-1}. \tag{37}$$

Combining these results, it follows that $X(F_\infty)(-n)$ has finite G-Euler characteristic if and only if $\mathbb{Z}_p(-n)$ has finite G-Euler characteristic. Moreover, assuming these Euler characteristics are finite, and using (31) and (32), the assertion (33) follows immediately, completing the proof. □

It is perhaps worth remarking that, assuming the finiteness of the G-Euler characteristics of $X(F_\infty)(-n)$ and $\mathbb{Z}_p(-n)$, and also that $X(F_\infty)$ belongs to the category $\mathfrak{M}_H(G)$, one can also deduce (33) from the non-commutative main conjecture (Conjecture D). Moreover, in the special case when $F_\infty = M(F^{cyc})$ and $H = \mathbb{Z}_p$, then it is well known (see the remark at the end of the Appendix) that $X(F_\infty) = 0$, so that, in this case, $\chi(G, \mathbb{Z}_p(-n))$ is indeed finite, and, by virtue of (33), is given by

$$\chi(G, \mathbb{Z}_p(-n))) = |\zeta_\Sigma(F, 1-n)|_p. \tag{38}$$

When G has dimension at least 3 as a p-adic Lie group, it seems highly likely that $\mathbb{Z}_p(-n)$ should have finite G-Euler characteristic for all integers $n > 0$ with $n \equiv 0 \bmod [F(\mu_p) : F]$. However, it does not seem easy to formulate a general conjecture for the value of this Euler characteristic, assuming that it is finite. We briefly mention two very different specific cases.

Lemma 5.4. *Let F_∞/F be an admissible p-adic Lie extension such that H is isomorphic to an open subgroup of $SL_2(\mathbb{Z}_p)$. Then $\chi(G, \mathbb{Z}_p(-n)) = 1$ for all integers $n > 0$ with $n \equiv 0$ mod $[F(\mu_p) : F]$.*

Proof. We have $H_0(H, \mathbb{Z}_p) = \mathbb{Z}_p$, and we are grateful to K. Ardakov for pointing out to us that standard arguments with Lie algebra cohomology show that $H_i(H, \mathbb{Z}_p)$ is finite for $i = 1, 2$, and has $\mathbb{Z}_p$-rank 1 for $i = 3$, and that G acts trivially on all of these homology groups modulo their torsion subgroups. Now, as H acts trivially on $\mathbb{Z}_p(-n)$, we can move this Tate twist inside the H-homology groups. Since the Γ-homology of a finite module is 1, it now follows immediately from (31) and the multiplicativity of the Γ-Euler characteristics in exact sequences, that $\mathbb{Z}_p(-n)$ has finite G-Euler characteristic equal to 1. □

Secondly, consider the case when H is abelian, say $H = \mathbb{Z}_p{}^d$, with $d \geq 2$. We then have

$$H_1(H, \mathbb{Z}_p) = H. \tag{39}$$

and it is well known that $H_i(H, \mathbb{Z}_p)$ is the i-th exterior power of H as a $\mathbb{Z}_p$-module. Now the abelian main conjecture shows that $H(-n)$ has finite Γ-Euler characteristic for all integers $n > 0$ with $n \equiv 0 \bmod [F(\mu_p) : F]$. However, we do not know enough about the roots of the p-adic zeta function of F at present to be able to prove that the i-th exterior power of H has finite Γ-Euler characteristic for any of $i = 2, ..., d$, for all such integers n. Thus we cannot even establish the finiteness of the G-Euler characteristic of $\mathbb{Z}_p(-n)$, let alone compute its exact value. However, if we make the additional hypothesis that n is divisible by a sufficiently large power of p, one easily sees that

$$\chi(\Gamma, H_0(H, \mathbb{Z}_p(-n))) = |w_n(F)|_p^{-1}, \prod_{i=1}^{d} \chi(\Gamma, H_i(H, \mathbb{Z}_p(-n)))^{(-1)^i} = 1. \tag{40}$$

Thus for all positive integers n, with $n \equiv 0 \bmod [F(\mu_p) : F]$ and n divisible by a sufficiently large power of p, we conclude that $\mathbb{Z}_p(-n)$ has finite G-Euler characteristic given by

$$\chi(G, \mathbb{Z}_p(-n)) = |w_n(F)|_p^{-1}.$$

6 Appendix

.

Throughout, we assume that both F_∞/F is an admissible p-adic Lie extension of totally real fields, and we shall establish some results relating $X(F_\infty)$ to $X(F^{cyc})$. We recall that if $\mathcal{G}$ is a p-adic Lie group, and A is a discrete p-primary $\mathcal{G}$-module, then it is well known that, for all $i \geq 0$, the Pontryagin dual of $H^i(\mathcal{G}, A)$ is canonically isomorphic to the homology group $H_i(\mathcal{G}, B)$, where $B = \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ is the compact Pontryagin dual of A.

Proposition 6.1. *Let F_∞/F be any admissible p-adic Lie extension. Then, for all $i \geq 1$, we have*

$$H_i(H, X(F_\infty)) \simeq H_{i+2}(H, \mathbb{Z}_p).$$

Proof. Since (1) is valid not only for F itself, but also for every finite extension of F contained in F_∞, we conclude that

$$H^i(G_S(F_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = 0 \ (i \geq 2). \tag{41}$$

Applying the Hochschild-Serre spectral sequence to $G_S(F^{cyc})$ and its closed normal subgroup $G_S(F_\infty)$, we conclude from (41) (see Theorem 3 of [6]) that, for all $j \geq 1$, there is a long exact sequence

$$H^j(H, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^j(G_S(F^{cyc}), \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^{j-1}(H, X(F_\infty)) \longrightarrow \tag{42}$$

$$H^{j+1}(H, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^{j+1}(G_S(F^{cyc}), \mathbb{Q}_p/\mathbb{Z}_p).$$

Taking $j = i + 1$ with $i \geq 1$, and again using (1), the proof of the proposition is complete after taking Pontrjagin duals. □

Proposition 6.2. *For any admissible p-adic Lie extension F_∞/F, we have the exact sequence*

$$0 \longrightarrow H_2(H, \mathbb{Z}_p) \longrightarrow H_0(H, X(F_\infty)) \longrightarrow X(F^{cyc}) \longrightarrow H_1(H, \mathbb{Z}_p) \longrightarrow 0. \tag{43}$$

.

Proof. Takeing $j = 1$ in (42), we obtain result on noting that the first arrow on the left in (42) is injective, and the group on the right in (42) is still zero. □

We assume now that G is pro-p of dimension $d+1$ with $d \geq 1$, and that G no element of order p. We recall that $\mu_G(X(F_\infty))$ is defined via the exact sequence (2). If V is any finitely generated torsion $\Lambda(\Gamma)$-module, we write $\mu_\Gamma(V)$ for its classical μ-invariant. Since G has finite homological dimension, these mu-invariants, for p-primary modules, are well known to be related to Euler characteristics as follows (see Corollary 1.7 of [8]). If A is a finitely generated p-primary $\Lambda(G)$-module, and B is a finitely generated p-primary $\Lambda(\Gamma)$-module, define the Euler characteristics

$$\chi(G, A) = \prod_{i=0}^{d+1} (\#(H_i(G, A)))^{(-1)^i},\ \chi(\Gamma, B) = \#(H_0(\Gamma, B))/\#(H_1(\Gamma, B)).$$

Then we have

$$p^{\mu_G(A)} = \chi(G, A),\ p^{\mu_\Gamma(B)} = \chi(\Gamma, B). \tag{44}$$

Lemma 6.3. *Assume that G is pro-p of dimension $d+1$ with $d \geq 1$, and that G has no element of order p. Then $H_i(H, X(F_\infty)(p))$ is a finitely generated torsion torsion $\Lambda(\Gamma)$-module for all $i \geq 0$, and*

$$\mu_G(X(F_\infty)) = \sum_{i=0}^{d} (-1)^i \mu_\Gamma(H_i(H, X(F_\infty)(p))). \tag{45}$$

Proof. The first assertion is obvious. To prove the second, we note that, for $i \geq 1$, the Hochschild-Serre spectral sequence gives the exact sequence

$$0 \longrightarrow H_0(\Gamma, H_i(H, X(F_\infty)(p))) \longrightarrow H_i(G, X(F_\infty)(p)) \longrightarrow H_1(\Gamma, H_{i-1}(H, X(F_\infty)(p))) \longrightarrow 0\ ,$$

whence we obtain

$$\chi(G, X(F_\infty)(p)) = \prod_{i=0}^{d} \chi(\Gamma, H_i(H, X(F_\infty)(p))^{(-1)^i}.$$

The conclusion of the lemma is now clear from (44). □

Define the $\Lambda(G)$-module Y_∞ by the exact sequence

$$0 \to X(F_\infty)(p) \to X(F_\infty) \to Y_\infty \to 0. \tag{46}$$

Since $X(F_\infty)$ is annihilated by p^n for all sufficiently large n, we can view Y_∞ as a $\Lambda(G)$-submodule of $X(F_\infty)$, and so we also have a short exact sequence

$$0 \longrightarrow Y_\infty \longrightarrow X(F_\infty) \longrightarrow W_\infty \longrightarrow 0\ , \tag{47}$$

for some $\Lambda(G)$-module W_∞.

Proposition 6.4. *Assume that G is pro-p of dimension $d+1$ with $d \geq 1$, and that G has no element of order p. Then $H_i(H, Y_\infty)$ is a finitely generated torsion $\Lambda(\Gamma)$-module for all $i \geq 0$. Moreover, $H_d(H, Y_\infty) = 0$.*

Proof. We first prove that all the groups $H_i(H, Y_\infty)$ are torsion $\Lambda(\Gamma)$-modules. Taking H-homology of (46), we obtain, for each $i \geq 1$, the exact dequence

$$H_i(H, X(F_\infty)) \to H_i(H, Y_\infty) \to H_{i-1}(H, X(F_\infty)(p)).$$

The first term is finitely generated over $\mathbb{Z}_p$ by Proposition 6.1, and the third term is annihilated by a power of p. Therefore $H_i(H, Y_\infty)$ is $\Lambda(\Gamma)$-torsion. The assertion for $i = 0$ follows from (43), since $X(F^{cyc})$ is $\Lambda(\Gamma)$-torsion and $H_j(H, \mathbb{Z}_p)$ is a finitely generated over $\mathbb{Z}_p$-module for all $j \geq 0$. To prove the second assertion, we note that H has homological dimension d. Thus, taking H-homology exact of (47), we get the exact sequence

$$0 \to H_d(H, Y_\infty) \to H_d(H, X(F_\infty)). \tag{48}$$

But, as $d \geq 1$, we have $H_d(H, X(F_\infty)) \simeq H_{d+2}(H, \mathbb{Z}_p)$, and the latter group is zero since the homological dimension of H is d. □

Proposition 6.5. *Assume that G is pro-p of dimension $d+1$ with $d \geq 1$, and that G has no element of order p. Then we have*

$$\mu_G(X(F_\infty)) = \mu_\Gamma(X(F^{cyc})) - \sum_{i=0}^{d-1} (-1)^i \mu_\Gamma(H_i(H, Y_\infty)).$$

Proof. From (43), we know that $\mu_\Gamma(X(F^{cyc})) = \mu_\Gamma(H_0(H, X(F_\infty)))$ since the first and last terms in (43) are finitely generated over $\mathbb{Z}_p$. Taking H-homology of (46), we obtain the exact sequence

$$H_1(H, X(F_\infty)) \longrightarrow H_1(H, Y_\infty) \longrightarrow X(F_\infty)(p)_H \longrightarrow X(F_\infty)_H \longrightarrow (Y_\infty)_H \longrightarrow 0\ . \tag{49}$$

By Proposition 6.1, $H_1(H, X(F_\infty)) = H_3(H, \mathbb{Z}_p)$ is finitely generated over $\Lambda(H)$. Hence we obtain

$$\mu_\Gamma(X(F_\infty)) = \mu_\Gamma((X(F_\infty))_H) - \mu_\Gamma((Y_\infty)_H) + \mu_\Gamma(H_1(H, Y_\infty)).$$

Morever, for $i \geq 1$, homology exact sequence derived from (46) yields

$$\mu_\Gamma(H_i(H, X(F_\infty)(p))) = \mu_\Gamma(H_{i+1}(H, Y_\infty))$$

since for all $i \geq 1$, again by Proposition 6.1, $H_i(H, X(F_\infty)) = H_{i+2}(H, \mathbb{Z}_p)$ is finitely generated over $\mathbb{Z}_p$. The assertion of the proposition now follows immediately (45). $\square$

Recall that when H is pro-p and has no elements of order p, we define the rank of Y_∞ as a $\Lambda(H)$-module by

$$\mathrm{rk}_{\Lambda(H)} Y_\infty = \dim_{Q(H)} Y_\infty \otimes_{\Lambda(H)} Q(H),$$

where $Q(H)$ is the skew field of fractions of $\Lambda(H)$.

Theorem 6.6. *Assume that G is pro-p of dimension $d+1$ with $d \geq 1$, and that G has no element of order p. Suppose further that $X(F_\infty)$ is in the category $\mathfrak{M}_H(G)$. Let r be the $\mathbb{Z}_p$-rank of $X(F^{cyc})/X(F^{cyc})(p)$. Then $\mu_G(X(F_\infty)) = \mu_\Gamma(X(F^{cyc}))$ and the $\Lambda(H)$-rank of $X(F_\infty)/X(F_\infty)(p)$ is $r-1$.*

Proof. Our hypothesis that $X(F_\infty)$ is in $\mathfrak{M}_H(G)$ implies that Y_∞ is finitely generated as a $\Lambda(H)$-module. Hence the $H_i(H, Y_\infty)$ are finitely generated as $\mathbb{Z}_p$-modules for all $i \geq 0$, and hence have Γ μ-invariant equal to 0. Thus Proposition 6.5 gives immediately that $\mu_G(X(F_\infty)) = \mu_\Gamma(X(F^{cyc}))$. Now we compute the $\Lambda(H)$-rank of Y_∞. Since H is pro-p and has no elements of order p, it is well known that

$$\mathrm{rk}_{\Lambda(H)} V = \sum_{i \geq 0} (-1)^i \mathrm{rk}_{\mathbb{Z}_p} H_i(H, V), \tag{50}$$

for any finitely generated $\Lambda(H)$-module V. Now using the long exact sequence of (46), we see immediately that $\mathrm{rk}_{\mathbb{Z}_p} H_i(H, Y_\infty) = \mathrm{rk}_{\mathbb{Z}_p} H_i(H, X(F_\infty))$ for all $i \geq 0$. On the other hand, since the $\Lambda(H)$-module $\mathbb{Z}_p$ clearly as $\Lambda(H)$-rank 0, we have

$$\begin{aligned}
0 &= \sum_{i \geq 0} (-1)^i \mathrm{rk}_{\mathbb{Z}_p} H_i(H, \mathbb{Z}_p) \\
&= \sum_{i=0}^{2} (-1)^i \mathrm{rk}_{\mathbb{Z}_p} H_i(H, \mathbb{Z}_p) + \sum_{i \geq 1} (-1)^i \mathrm{rk}_{\mathbb{Z}_p} H_i(H, X(F_\infty)) \\
&= 1 + \mathrm{rk}_{\mathbb{Z}_p} X(F_\infty)_H - r + \sum_{i \geq 1} (-1)^i \mathrm{rk}_{\mathbb{Z}_p} H_i(H, X(F_\infty)) \\
&= 1 - r + \sum_{i \geq 0} (-1)^i \mathrm{rk}_{\mathbb{Z}_p} H_i(H, Y_\infty) \\
&= 1 - r + \mathrm{rk}_{\Lambda(H)} Y_\infty.
\end{aligned}$$

The first and last equalities are (50), the second is Proposition 6.1, and the third follows from the inflation-restriction sequence

$$0 \to H_2(H, \mathbb{Z}_p) \to H_1(G_S(F_\infty), \mathbb{Z}_p)_H \to H_1(G_S(F^{cyc}), \mathbb{Z}_p) \to H_1(H, \mathbb{Z}_p) \to 0.$$

$\square$

Remark 6.7. Notice that the hypotheses of the above theorem imply, in particular, that necessarily $r \geq 1$. We are grateful to Ralph Greenberg for pointing out to us that this fact is a consequence of Proposition 3.9.1 in [9], which is also known as Burnside Basis Theorem. Indeed, as he remarked to us, one can easily deduce from this Burnside Basis Theorem that if Conjecture A holds for F and $X(F^{cyc})$ has $\mathbb{Z}_p$-rank at most 1, then $M(F^{cyc})$ is the maximal pro-p extension of F, which is unramified outside S.

The simplest unconditional example of Theorem 6.6 is as follows. Take F to be the maximal real subfield of $\mathbb{Q}(\mu_p)$ for an add prime p, and Σ to consist of the unique prime of F above p. Since Conjecture A is valid for F by the theorem of Ferrero-Washington, we can take $F_\infty = M(F^{cyc})$. By Theorem 2.1, the Galois group G is then pro-p and has no element of order p, and the subgroup H is a free $\mathbb{Z}_p$-module of rank $r \geq 0$. Moreover, $X(F_\infty)$ is a finitely generated $\Lambda(H)$-module, which has no $\Lambda(H)$-torsion by Theorem 3.1. The classical theory of cyclotomic fields tells us that $r \geq 1$ if and only if p is an irregular prime, and $X(F_\infty)$ is zero when $r = 1$. When $r \geq 2$, Theorem 6.6 and the classical commutative structure theory of finitely generated $\Lambda(H)$-modules shows that there is an exact sequence

$$0 \to X(F_\infty) \to \Lambda(H)^{r-1} \to D \to 0,$$

where D is a pseudo-null $\Lambda(H)$-module. The smallest prime p for which $r \geq 2$ is $p = 157$, and the largest value of r for $p < 12,000,000$ is $r = 7$.

References

[1] K. Iwasawa, *On $\mathbb{Z}_p$-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.

[2] R. Ramakrishna, *Deforming Galois representations and the the conjectures of Serre and Fontaine-Mazur*, Annals of Math., **156** (2002), 115-154.

[3] Y. Ochi, O. Venjakob, *On ranks of Iwasawa modules over p-adic Lie extensions*, Math. Proc. Cambridge Phil. Soc. **135** (2003), 25-43.

[4] O. Venjakob, *On the Iwasawa theory of p-adic Lie extensions*, Compositio Math. **138** (2003), 1-54.

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

[6] G. Hochschild, J-P. Serre, *Cohomology of group extensions*, Serre's Collected Papers, v. **I**, 110-134.

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

[8] S. Howson, *Euler characteristics as invariants of Iwasawa modules*, Proc. London Math. Soc. (3) **85** (2002), 634-658.

[9] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, Springer-Verlag, (2000)

[10] R. Greenberg, *On p-adic Artin L-functions*, Nagoya Math J. **89** (1983), 77-87.

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

[12] M. Kakde, *The main conjecture of Iwasawa theory for totally real fields*, to appear, (2011).

[13] J. Ritter, A. Weiss, *On the "main conjecture of equivariant Iwasawa theory"*, to appear, (2010).

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