Ramification in Iwasawa Theory and Splitting Conjectures

Chandrashekhar Khare, Jean-Pierre Wintenberger

RAMIFICATION IN IWASAWA THEORY AND SPLITTING CONJECTURES

CHANDRASHEKHAR KHARE AND JEAN-PIERRE WINTENBERGER

ABSTRACT. We make a reciprocity conjecture that extends Iwasawa's analogy of direct limits of class groups along the cyclotomic tower of a totally real number field F to torsion points of Jacobians of curves over finite fields. The extension is to generalised class groups and generalised Jacobians. We state some "splitting conjectures" which are equivalent to Leopoldt's conjecture.[1]

1. INTRODUCTION

For a number field F, with ring of integers $\mathcal{O}_F$, we may define the class group of F to be $\mathrm{Pic}(\mathcal{O}_F)$, i.e., the isomorphism classes of invertible sheaves on $\mathrm{Spec}(\mathcal{O}_F)$. Iwasawa deepened this formal analogy between class groups of number fields and Jacobians. He considered $\mathcal{X}_\infty^-$, the inverse limit under norm maps of the minus parts under complex conjugation of the Sylow p-sugroups of the class groups of $F(\mu_{p^n})$, where F is a totally real number field, p a fixed (odd) prime, and n varying. Iwasawa viewed $\mathcal{X}_\infty^- \otimes \mathbb{Q}_p$ as a p-adic vector space, which he proved to be finite dimensional, equipped with the action of γ, a generator for the p-part of $\mathrm{Gal}(F(\mu_{p^\infty})/F)$. He conjectured that the characteristic polynomial for this action should be the same as a certain p-adic L-function, at least when $F = \mathbb{Q}$. This was later called the main conjecture of Iwasawa theory which was proved by Mazur-Wiles (for $F = \mathbb{Q}$) and Wiles (for general totally real F). Iwasawa's conjecture can be viewed as an analog of the theorem of Weil which relates zeta-functions of curves over finite fields of characteristic p, to the characteristic polynomial for the action of Frobenius on the ℓ-adic Tate module of its Jacobian, for $\ell \neq p$.

In this paper we ask for an Iwasawa theoretic analog of a standard fact in the theory of generalised Jacobians, that holds over arbitrary base fields and is easier than Weil's result mentioned above. Namely, let X be a smooth projective curve over a field K with Jacobian J. We have the isomorphism $\mathrm{Ext}^1(J, \mathbb{G}_m) = \mathrm{Pic}^0(J) = J$. Let $P, Q \in X(K)$ be an ordered pair of distinct points, and consider the *generalised Jacobian* $J_{P,Q}$, the Jacobian of the singular curve X' obtained from X by identifying P with Q. Thus X' is a

CK was partially supported by NSF grants.
JPW is member of the Institut Universitaire de France.
[1]MR classification : 11R23

curve over K with nodal singularity. We have an exact sequence

$$0 \to \mathbb{G}_m \to J_{P,Q} \to J \to 0.$$

The standard fact alluded to earlier is that the class of $J_{P,Q}$ in $\mathrm{Ext}^1(J, \mathbb{G}_m)$ is given by the class of the degree 0 divisor $(P)-(Q)$. We make a reciprocity conjecture, see Conjecture **??**, that asks for an analogous formula in Iwasawa theory. To formulate this conjecture, we consider ramification at *auxiliary primes* in Iwasawa modules (see §**??**), define analogs of degree 0 divisors supported on Frobenius elements in certain Galois groups (see §**??**), and use a well-known pairing of Iwasawa (see §**??**). We prove an implication of the reciprocity conjecture (see Theorem **??** and Corollary **??**). The proof of the reciprocity conjecture has eluded us.

If the field K above is a finite field, then the extension class $(P)-(Q)$ is of finite order. Inspired by Iwasawa's analogy, we conjecture in our situation too that the extension classes in the reciprocity conjecture are of finite order. This leads to a splitting conjecture, see Conjecture **??**, that we show in Corollary **??** to be equivalent to the following standard conjecture:

Conjecture 1.1. *(Leopoldt) The cyclotomic $\mathbb{Z}_p$-extension F_∞/F is the unique $\mathbb{Z}_p$-extension of a totally real number field F.*

We denote by $\delta_{F,p}$, the integer such that the $\mathbb{Z}_p$-rank of the maximal abelian p-extension of F unramified outside p is $1+\delta_{F,p}$. The conjecture asserts that it is 0; $\delta_{F,p}$ is also called the Leopoldt defect (for F and p).

Our original motivation for this work was to search for a criterion for Leopoldt's conjecture that could be approached using Wiles' proof of the main conjecture [**?**] which draws on Hida's theory of Λ-adic Hilbert modular forms. This search led to Conjecture **??**. As Conjecture **??** is about odd extensions of $\mathcal{F}_\infty$, it might offer some access to methods that use Hilbert modular forms.

1.1. *Notation.* We fix a prime number p throughout. Except in paragraph **??**, we make the assumption that p is odd. We let F be a totally real number field. We operate within a fixed algebraic closure $\overline{F}$ of F. We have the cyclotomic $\Gamma(=\mathbb{Z}_p)$-extension of F that we denote by F_∞. We denote by γ a chosen topological generator of Γ, and by χ the p-adic cyclotomic character. The field F_∞ is contained in $\mathcal{F}_\infty = F(\mu_{p^\infty})$, whose real subfield we denote by F^∞; F_∞ is contained in F^∞. The degree $[\mathcal{F}_\infty : F_\infty]$ divides $p-1$ and $[\mathcal{F}_\infty : F^\infty] = 2$. We denote by $\mathcal{F}_n$ and F_n the extension $F(\mu_{p^{n+t}})$ and its real subfield respectively. Here t is the largest integer so that $F(\mu_p)$ contains the μ_{p^t} roots of unity. Hence $[\mathcal{F}_n : F(\mu_p)] = [F_n : F] = p^n$. For convenience we will assume throughout the paper that $F_\infty = F^\infty$, i.e., $[F(\mu_p) : F] = 2$. For a finite place q of a number field F we denote by $N(q)$ its norm, the order of the residue field at q. For a finite set of finite places Q of F, by the Q-units of F, denoted by E_Q, we mean elements of F^* which are units at all finite places outside Q.

For an abelian group M, we denote by $\widehat{M}$ its prop-p completion $\varprojlim_n M/M^{p^n}$.

We say that an abelian extension L of $\mathcal{F}_\infty$ is odd (or its Galois group is odd) if L is Galois over F and the complex conjugation of $\mathrm{Gal}(\mathcal{F}_\infty/F)$ acts on $\mathrm{Gal}(L/\mathcal{F}_\infty)$ by inversion.

By the $\mathbb{Z}_p$-rank of an $\mathbb{Z}_p$-module M, called the essential rank by Iwasawa, we mean the dimension of $M \otimes \mathbb{Q}_p$ as a vector space over $\mathbb{Q}_p$. For a $\Lambda = \mathbb{Z}_p[[T]] = \mathbb{Z}_p[[\Gamma]]$-module M, and an integer n, we denote by $M(n)$ the Λ-module with same underlying module M, and the Λ-action specified by $\gamma.m = \chi(\gamma)^n \gamma m$. We say that (possibly infinite) Galois extensions L, L' of a field K are almost linearly disjoint if the degree $[L \cap L' : K]$ is finite. Given a Galois extension L/K of algebraic (possibly infinite) extensions of $\mathbb{Q}$, we may talk about places of K and conjugacy class of decomposition groups, inertia groups at these places. If L/K has abelian Galois group we say that L/K is almost totally ramified at a set of places of K if the inertia groups at these places generate a subgroup of finite index of $\mathrm{Gal}(L/K)$.

1.2. *Acknowledgements.* We would like to thank Gebhard Böckle, John Coates, Najmuddin Fakhruddin, David Gieseker, Ralph Greenberg, Benedict Gross, Haruzo Hida, Tony Scholl, Chris Skinner, Kevin Ventullo for helpful conversations. The first author thanks the Département de Mathematiques of the Université de Strasbourg for its support during a visit in the summer of 2009 when some of the work reported on in this paper was done.

Part of the writing of this work was done during the authors' stay at the Institut Henri Poincare - Centre Emile Borel and IAS, Princeton. The authors thank these institutions for hospitality and support.

2. Some Kummer theory

In this section, we state some results on Kummer theory and $\mathbb{Z}_p$-extensions. They are basic to the work of this paper. See also lemma 2.2. of [**?**].

Let p be any prime number for this section, allowing $p = 2$.

2.1. **General fields.** Let F be any field of characteristic different from p. Recall that $\mathcal{F}_\infty$ is the cyclotomic extension $F(\mu_{p^\infty})$. Let L be an extension of $\mathcal{F}_\infty$. We say that L is *a Kummer $\mathbb{Z}_p$-extension* of $\mathcal{F}_\infty$ if L/F is Galois and it is such that $\mathrm{Gal}(L/\mathcal{F}_\infty) \simeq \mathbb{Z}_p$ is isomorphic to $\mathbb{Z}_p(1)$ as a $\mathrm{Gal}(\mathcal{F}_\infty/F)$-module. We let $\widehat{F^*}$ be the p-adic completion of the multiplicative groupe of F *i.e.* the projective limit $\varprojlim_n F^*/(F^*)^{p^n}$, the transition maps being induced by the identity.

We have the Kummer isomorphisms $\mathrm{K}_{F,n} : F^*/(F^*)^{p^n} \to H^1(G_F, \mu_{p^n})$. Taking the projective limits for n, we get an isomorphism $\mathrm{K}_F : \widehat{F^*} \to H^1(G_F, \mathbb{Z}_p(1))$, where the H^1 are continuous H^1, the topology of $\mathbb{Z}_p(1)$ being the p-adic one ([**?**]).

If $\bar{x} = (\bar{x}_n)_{n\in\mathbb{N}}$ is an element of $\widehat{F^*}$, we note $F_{\bar{x}}$ the extension of $\mathcal{F}_\infty$ which is the union of the Kummer extensions $F(\mu_{p^n}, x_n^{1/p^n})$, where $x_n \in F^*$ maps

to $\bar{x}_n$ in $F^*/(F^*)^{p^n}$. It is also the extension of $\mathcal{F}_\infty$ corresponding to the fixed field of the kernel of the homomorphism arising from the image of $\mathrm{K}_F(\bar{x})$ under the map $H^1(G_F, \mathbb{Z}_p(1)) \to \mathrm{Hom}(G_{\mathcal{F}_\infty}, \mathbb{Z}_p)(1)^0$, where the Hom are continuous homomorphisms and ^{0} means fixed by $\mathrm{Gal}(\mathcal{F}_\infty/F)$.

For a subgroup T of $\widehat{F^*}$, by $F(\mu_{p^\infty}, T^{\frac{1}{p^\infty}})$ we mean the compositum of all extensions of F obtained by adjoining, for all $n \in \mathbb{N}$, all p^n th roots of (lifts to F^* of) the image of T in $F^*/(F^*)^{p^n}$: it is the union of the fields $F_{\bar{x}}$ for $x \in T$. If T is a subgroup of F^* we still denote $F(\mu_{p^\infty}, T^{\frac{1}{p^\infty}})$ the extension defined by the image of T in $\widehat{F^*}$.

Proposition 2.1. *The Kummer $\mathbb{Z}_p$-extensions of $\mathcal{F}_\infty$ are exactly the fields $F_{\bar{x}}$, for $\bar{x} \in \widehat{F^*}$ non-torsion. The torsion of $\widehat{F^*}$ is the group $\mu_{p^\infty}(F)$ of roots of unity of order a power of p if this group is finite, and is trivial if $F = \mathcal{F}_\infty$.*

Proof. Let $\bar{x} \in \widehat{F^*}$ be such that $\bar{x}^{p^a} = 1$. Write $\bar{x} = (\bar{x}_n)_n$ with $x_n \in F^*$. For every n, there exists $y_n \in F^*$ such that $x_n^{p^a} = y_n^{p^n}$. For $n \geq a$, it follows that $\epsilon_{n-a} := x_n y_n^{-p^{n-a}}$ is a p^a root of unity. We have $(\bar{x}_n) = (\bar{\epsilon}_n)$. If $\mu_{p^\infty}(F)$ is finite, it follows that there exists an $\epsilon \in \mu_{p^\infty}(F)$ such that the $\bar{\epsilon}_n$ for $n \in \mathbb{N}$ are the image of ϵ. If $\mu_{p^\infty}(F)$ is infinite, it is p-divisible, and it follows that the torsion of $\widehat{F^*}$ is trivial. This proves the part of the proposition concerning the torsion of $\widehat{F^*}$.

If $\mu_{p^\infty}(F)$ is infinite, the proposition follows from the fact that the Kummer map K_F is bijective. Let us suppose that $\mu_{p^\infty}(F)$ is finite.

Lemma 2.2. *The cohomology groups $H^1(\mathrm{Gal}(\mathcal{F}_\infty/F), \mu_{p^n}(\overline{F}))$ and $H^2(\mathrm{Gal}(\mathcal{F}_\infty/F), \mu_{p^n}(\overline{F}))$ are killed by a power p^a of p independent of n.*

Let us prove the proposition granted the lemma. As the projective system $\mathbb{Z}_p(1) = \varprojlim_n \mu_{p^n}(\overline{F})$ satisfies the Mittag-Leffler property, and the functor projective limit is left exact, Hochschild-Serre exact sequences for coefficients $\mu_{p^n}(\overline{F})$ give the following exact sequence:

$$(0) \to H^1(\mathrm{Gal}(\mathcal{F}_\infty/F), \mathbb{Z}_p(1)) \to H^1(G_F, \mathbb{Z}_p(1)) \to H^1(G_{\mathcal{F}_\infty}, \mathbb{Z}_p(1)),$$

and the H^1 with coefficients in $\mathbb{Z}_p(1)$ are the projective limit of the H^1 with coefficients in $\mu_{p^n}(\overline{F})$ (use cor. 2.7.6. of chap. 2 paragraph 7 of [**?**]). The lemma implies that $H^1(\mathrm{Gal}(\mathcal{F}_\infty/F), \mathbb{Z}_p(1))$ is torsion. It then follows from the above exact sequence, the fact that $H^1(G_{\mathcal{F}_\infty}, \mathbb{Z}_p(1)) = \mathrm{Hom}(G_{\mathcal{F}_\infty}, \mathbb{Z}_p(1))$ has no torsion, and the bijectivity of the Kummer map K_F, that the kernel of the map $\widehat{F^*} \to \mathrm{Hom}(G_{\mathcal{F}_\infty}, \mathbb{Z}_p(1))$ is the torsion subgroup of $\widehat{F^*}$. It follows that if $\bar{x}$ is not torsion, the extension $F_{\bar{x}}$ is a $\mathbb{Z}_p$ Kummer extension of $\mathcal{F}_\infty$.

Conversely, let L be a Kummer $\mathbb{Z}_p$-extension of $\mathcal{F}_\infty$. Let f be a continuous non zero morphism $G_{\mathcal{F}_\infty} \to \mathbb{Z}_p(1)$ whose kernel corresponds to L. Let f_n be the morphisms $G_{\mathcal{F}_\infty} \to \mu_{p^n}(\overline{F})$ defined by f. As $H^2(\mathrm{Gal}(\mathcal{F}_\infty/F), \mu_{p^n}(\overline{F}))$ is killed by p^a, $p^a f_n$ is the image of an element $\bar{x}_n$ of $F^*/(F^*)^{p^n}$. As

$H^1(\mathrm{Gal}(\mathcal{F}_\infty/F), \mu_{p^n}(\overline{F}))$ is killed by p^a, the $\bar{x}_n^{p^a}$ define an element $\bar{x}'$ in the projective limit $\varprojlim_n F^*/(F^*)^{p^n}$, hence of $\widehat{F^*}$. One has $\mathrm{K}_F(\bar{x}') = p^{2a}f$, hence $L = F_{\bar{x}'}$. This proves the proposition, granted the lemma.

Let us prove the lemma. Let F' be $F(\mu_p(\overline{F}))$ if $p \neq 2$ and $F(\mu_4(\overline{F}))$ if $p = 2$. By Hochschild-Serre spectral sequence , we reduce to the case $F = F'$. Note that if $\mu_{p^\infty}(F)$ is infinite, the lemma is obvious as $\mathcal{F}_\infty = F$. So we may suppose that $\mathrm{Gal}(\mathcal{F}_\infty/F)$ is isomorphic to $\mathbb{Z}_p$. Let γ a generator of $\mathrm{Gal}(\mathcal{F}_\infty/F)$ and $\chi_p(\gamma)$ its image by the cyclotomic character. The calculation of the cohomology of the procyclic group $\mathbb{Z}_p$ gives that $H^1(\mathrm{Gal}(\mathcal{F}_\infty/F), \mu_{p^n}(\overline{F}))$ is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})/(\chi_p(\sigma) - 1)$ and $H^2(\mathrm{Gal}(\mathcal{F}_\infty/F), \mu_{p^n}(\overline{F}))$ is trivial (prop. 1.7.7 of chap. 1 paragraph 7 of [**?**]). The lemma follows as $\chi_p(\gamma) \neq 1$. □

Remarks. It follows from the proof of the proposition that $\widehat{F^*}$ injects in $H^1(G_{\mathcal{F}_\infty}, \mathbb{Z}_p(1))$. It implies the following. Let $\bar{x}_i$, $i = 1, 2$, be two non-torsion elments of $\widehat{F^*}$. Then $F_{\bar{x}_1} = F_{\bar{x}_2}$ if and only if there exist a_1 and a_2 in $\mathbb{Z}_p$, non-zero, such that $\bar{x}_1^{a_1} = \bar{x}_2^{a_2}$.

The proof of the proposition implies that if T is a finitely generated subgroup of F^*, the Galois group of $F_T = F(\mu_{p^\infty}, T^{\frac{1}{p^\infty}})$ over $\mathcal{F}_\infty = F(\mu_{p^\infty})$ is a finitely generated $\mathbb{Z}_p$-module of the same $\mathbb{Z}_p$-rank as the closure of T in $\widehat{F^*}$.

2.2. **Number fields.** We suppose now that F is a finite extension of $\mathbb{Q}$. If $\mathfrak{q}$ is a prime of F, we denote by $F_\mathfrak{q}$ the completion of F at $\mathfrak{q}$. We denote by $v_\mathfrak{q}$ the valuation of $F_\mathfrak{q}$ normalized by $v_\mathfrak{q}(F_\mathfrak{q}^*) = \mathbb{Z}$. We still denote by $v_\mathfrak{q}$ the map $\widehat{F_\mathfrak{q}^*} \to \mathbb{Z}_p$ induced by $v_\mathfrak{q}$. We denote by $\mathrm{loc}_\mathfrak{q}$ the morphism $\widehat{F^*} \to \widehat{F_\mathfrak{q}^*}$ induced by the inclusion of F in $F_\mathfrak{q}$.

Proposition 2.3. *Let $\bar{x} \in \widehat{F^*}$ be non-torsion. Then, the Kummer extension $F_{\bar{x}}/\mathcal{F}_\infty$ is unramified at primes above $\mathfrak{q}$ if and only if $\mathrm{loc}_\mathfrak{q}(\bar{x})$ is torsion.*

Proof. Let us note $E = F_\mathfrak{q}$ and E_{ur} the maximal unramified extension of E. The proposition follows from proposition **??** and the fact that the kernel of $\widehat{E^*} \to \widehat{E_{\mathrm{ur}}^*}$ is torsion. For this fact, let ω be a uniformizer of E. If $\mathfrak{q}$ is not above p, we have $\widehat{E^*} \simeq \omega^{\mathbb{Z}_p}\mu_{p^\infty}(E)$ and $\widehat{E_{\mathrm{ur}^*}} \simeq \omega^{\mathbb{Z}_p}$. If $\mathfrak{q}$ is above p, we have $\widehat{E^*} \simeq \omega^{\mathbb{Z}_p}U_E^+$ and $\widehat{E_{\mathrm{ur}}^*} \simeq \omega^{\mathbb{Z}_p}U_{\widehat{E_{\mathrm{ur}}}}^+$, where U^+ are units that $\equiv 1$ mod.ω and $\widehat{E_{\mathrm{ur}}}$ is the completion of E_{ur}. The map $U_F^+ \to U_{\widehat{E_{\mathrm{ur}}}}^+$, is injective as $U_{E_{\mathrm{ur}}}^+$ is separated for the p-adic topology. □

Remark. The proof of the proposition shows that if $F_{\bar{x}}/F$ is unramified at $\mathfrak{q}$, $v_\mathfrak{q}(\bar{x}) = 0$, the converse being true if $\mathfrak{q}$ is not above p.

We now let Q be a finite set of primes of F. We denote by E_Q the Q-units *i.e.* the elements $x \in F^*$ such that $v_\mathfrak{q}(x) = 0$ for $\mathfrak{q} \notin Q$. The group E_Q is finitely generated. We write $\widehat{E_Q}$ its p-adic completion. As

if a power of $x \in F^*$ is a Q-unit, then x is a Q-unit, the natural maps $E_Q/E_Q^{p^n} \to F^*/(F^*)^{p^n}$ are injective, hence also the map $\widehat{E_Q} \to \widehat{F^*}$. We identify $\widehat{E_Q}$ to a subgroup of $\widehat{F^*}$.

Proposition 2.4. *a) An element $\bar{x} \in \widehat{F^*}$ belongs to $\widehat{E_Q}$ if and only if $v_{\mathfrak{q}}(\bar{x}) = 0$ for $\mathfrak{q} \notin Q$.*

b) If $\bar{x}$ is non-torsion, the Kummer $\mathbb{Z}_p$-extension $F_{\bar{x}}/\mathcal{F}_\infty$ is unramified outside Q only if $\bar{x} \in \widehat{E_Q}$. If the primes of F above p are in Q, the converse is true.

Proof. The second part of the proposition follows from the first one, the preceding proposition and the remark after the proposition **??**.

Let us prove the first part. The "only if" part is clear so let us prove the "if" part.

Let p^a be a power of p that kills the p-primary part of the class group of the ring O_Q of Q integers (elements $x \in F$ such that $v_{\mathfrak{q}}(x) \geq 0$ for $\mathfrak{q} \notin Q$).

Let $x = (\bar{x}_n)$ be in $\widehat{F^*}$ such that $v_{\mathfrak{q}}(x) = 0$ if $\mathfrak{q} \notin Q$. Let $x_n \in F^*$ be a lift $\bar{x_n}$. Let $I(x_n)$ be the rank one projective O_Q-module generated by x_n. As $v_{\mathfrak{q}}(x_n)$ is divisibleby p^n for $\mathfrak{q} \notin Q$, there is rank one projective O_Q-module I_n such that $I(x_n) = I_n^{p^n}$. The rank one module $I_n^{p^a}$ is free. Let $y_n \in O_Q$ be a generator. We have $I(x_n) = I(y_n)^{p^{n-a}}$, hence there is ϵ_n a unit in O_Q such that $x_n = y_n^{p^{n-a}}\epsilon_n$. We see that x_n and ϵ_n have the same image in $F^*/(F^*)^{p^{n-a}}$. It follows that the ϵ_n define an element ϵ of $\widehat{E_Q}$ with image x in $\widehat{F^*}$. The proposition is proved. □

We will need the following lemma:

Lemma 2.5. *Let T a finitely generated subgroup of F^*, and let Q be a finite set of finite places of F. Let $F_T = F(\mu_{p^\infty}, T^{\frac{1}{p^\infty}})$ be the compositum of the extensions F_t for $t \in T$. Then the $\mathbb{Z}_p$-rank of $\mathrm{Gal}(F_T/\mathcal{F}_\infty)$ equals the rank of T. Furthermore, the $\mathbb{Z}_p$-rank of the subgroup generated by the inertia groups above Q in $\mathrm{Gal}(F_T/\mathcal{F}_\infty)$ is the same as the $\mathbb{Z}_p$-rank of the closure of (the diagonal image of) T in $\Pi_{v\in Q}\widehat{F_v^*}$.*

Proof. The first part of the lemma follows from the remark at the end of the last paragraph. It follows from Dirichlet's theorem on finiteness of the rank of units that the rank of the closure of T in $\widehat{F^*}$ equals the rank of T.

Let us prove the second part. For $v \in Q$, let v' be a prime of $\mathcal{F}_\infty$ above v and let $I_{v'}$ be the inertia subgroup of $\mathrm{Gal}(F_T/\mathcal{F}_\infty)$ at v'. As the action of $\mathrm{Gal}(\mathcal{F}_\infty/F)$ on $\mathrm{Gal}(F_T/\mathcal{F}_\infty)$ is by the cyclotomic character χ_p, one easily sees that the subgroup $I_{v'}$ does not depend of v' and we call it I_v. We have the following commutative diagram:

$$\begin{array}{ccc} T & \to & \mathrm{Hom}(\mathrm{Gal}(F_T/\mathcal{F}_\infty), \mathbb{Z}_p(1)) \\ \downarrow & & \downarrow \\ \prod_{v\in Q} \widehat{F_v^*} & \to & \prod_{v\in Q} \mathrm{Hom}(I_v, \mathbb{Z}_p(1)). \end{array}$$

The lemma follows from the fact that the horizontal arrows have torsion kernels by propositions **??** and **??**.

□

3. Elements of Iwasawa theory

Let $\mathcal{L}_\infty$ be the maximal abelian p-extension of $\mathcal{F}_\infty$ that is unramified everywhere. We set $\mathcal{X}_\infty = \mathrm{Gal}(\mathcal{L}_\infty/\mathcal{F}_\infty)$. It decomposes as $\mathcal{X}_\infty = \mathcal{X}_\infty^+ \oplus \mathcal{X}_\infty^-$ under the action of complex conjugation which corresponds to $\mathcal{L}_\infty$ being the compositum of two linearly disjoint extensions $\mathcal{L}_\infty^+$ and $\mathcal{L}_\infty^-$. The Galois group $\mathcal{X}_\infty$ (respectively $\mathcal{X}_\infty^+, \mathcal{X}_\infty^-$) is the inverse limit of the p-parts of the class groups, denoted by $\mathcal{A}_n$, of $\mathcal{F}_n$ (resp., + and − parts, $\mathcal{A}_n^+$ and $\mathcal{A}_n^-$) ($n \geq 0$) under the norm maps. It is conjectured by Greenberg that $\mathcal{X}_\infty^+$ is a finite group. We have the theorem of Iwasawa that under the natural Galois action of $\Lambda = \mathbb{Z}_p[[T]]$, $\mathcal{X}_\infty$ is a finitely generated torsion Λ-module.

Let M_∞ be the maximal abelian p-extension of F_∞ that is unramified outside p. We set $Y_\infty = \mathrm{Gal}(M_\infty/F_\infty)$. Again by a theorem of Iwasawa, Y_∞ is a finitely generated torsion Λ-module. (It is a consequence of the "weak Leopoldt conjecture" that he proved.) We denote by $Y'_\infty = \mathrm{Gal}(M_\infty/F)$, which sits inside an exact sequence

$$0 \to Y_\infty \to Y'_\infty \to \mathbb{Z}_p \to 0. \tag{1}$$

We call the last map the degree map. Thus Y_∞ is the $\mathbb{Z}_p$-submodule of Y'_∞ of elements of degree 0.

Recall a couple of facts:

- $Y_\infty, \mathcal{X}_\infty^-$ have no non-zero finite Λ-submodules (cf. Propositions 15.36 and 13.28 of [**?**]). This may also be deduced from 11.4.4 of [**?**] which states that $\mathcal{X}_\infty^-$ is the adjoint of a finitely generated torsion Λ-module, and th. 11.4.8 of [**?**].
- $Y_\infty \otimes \mathbb{Q}_p$ and $\mathcal{X}_\infty^- \otimes \mathbb{Q}_p$ are finite dimensional $\mathbb{Q}_p$-vector spaces. The μ-invariant of F_∞ is not known to be zero, and thus we do not know if Y_∞ is a finitely generated $\mathbb{Z}_p$-module.

3.1. *Iwasawa involution and adjoints.* For a Λ-module X we denote by X^0 the module whose underlying module is the same but where the Λ action, denoted by . is defined by $f(T).x = f((1+T)^{-1} - 1)x$ with the action on the right the original action. (This corresponds to defining the new Γ-action to be $\gamma.x = \gamma^{-1}x$). It gives an involution on the category of Iwasawa modules. For a discrete Λ-module M, we endow $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ with the Λ-action defined by $\gamma f(m) = f(\gamma^{-1}m)$. More generally for Γ-modules, either discrete or compact, M, N, we endow $\mathrm{Hom}_{\mathbb{Z}_p}(M, N)$ the group of continuous $\mathbb{Z}_p$-linear homomorphisms with the Λ-module structure given by $\gamma f(m) = \gamma f(\gamma^{-1}m)$.

Lemma 3.1. *For a Λ-module M, such that $M \otimes \mathbb{Q}_p$ is a finite dimensional vector space, we have a non-canonical $\Lambda \otimes \mathbb{Q}_p$-isomorphism* $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p) = M^0 \otimes \mathbb{Q}_p$.

Proof. This follows from the elementary fact that over a field K, a matrix $\in M_n(K)$ and its transpose are conjugate under the action of $\mathrm{GL}_n(K)$. $\square$

We denote by $\alpha(X)$ the adjoint of X see §1 of article 52 of [**?**], or §15.5 of [**?**] and $\tilde{\alpha}(X) = \alpha(X)^0$.

Lemma 3.2. *(Iwasawa) We have that X and $\alpha(X)$ are pseudo-isomorphic.*

3.2. *Iwasawa pairing.* The following basic theorem of Iwasawa and Coates is important for us.

Theorem 3.3. *(i) We have a perfect, Γ-equivariant, $\mathbb{Z}_p$-linear pairing*

$$Y_\infty \times \mathcal{A}_\infty^- \to \mathbb{Q}_p/\mathbb{Z}_p(1),$$

which we call the Iwasawa pairing, equivalently

$$Y_\infty = \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{A}_\infty^-, \mathbb{Q}_p/\mathbb{Z}_p(1)),$$

which we call the Iwasawa isomorphism.

(ii) We have that $\tilde{\alpha}(\mathcal{X}_\infty^-)$ is pseudo-isomorphic to $\mathrm{Hom}(\mathcal{A}_\infty^-, \mathbb{Q}_p/\mathbb{Z}_p)$.

(iii) We have a natural Γ-equivariant, $\mathbb{Q}_p$-linear perfect pairing

$$(Y_\infty \otimes \mathbb{Q}_p) \times (\mathcal{X}_\infty^- \otimes \mathbb{Q}_p) \to \mathbb{Q}_p(1),$$

or equivalently

$$Y_\infty \otimes \mathbb{Q}_p = \mathrm{Hom}_{\mathbb{Q}_p}(\mathcal{X}_\infty^- \otimes \mathbb{Q}_p, \mathbb{Q}_p(1)).$$

Proof. (i) This is in [**?**] and [**?**] (see also Proposition 13.32 of [**?**] or Theorem 11.4.3 of [**?**]).

(ii) Proposition 15.34 of [**?**] and its proof, or Theorem 11.1.8 of [**?**].

(iii) Theorem 11.1.8 of [**?**] gives an isomorphism of $Y_\infty = \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{A}_\infty^-, \mathbb{Q}_p/\mathbb{Z}_p(1))$ to $\alpha(\mathcal{X}'_\infty)(1)$ where $\mathcal{X}'_\infty$ is a sub Λ-module of $\mathcal{X}_\infty$ of finite index. The natural map $\alpha(\mathcal{X}_\infty)(1) \to \alpha(\mathcal{X}'_\infty)(1)$ is an isomorphism after $\otimes\mathbb{Q}_p$. It is the same for the natural map $\alpha(\mathcal{X}_\infty/\{p^\infty - \text{torsion}\})(1) \to \alpha(\mathcal{X}_\infty)(1)$. As for X finitely generated torsion Λ-module without p-torsion, $\alpha(X)$ is isomorphic to $\mathrm{Hom}_{\mathbb{Z}_p}(X, \mathbb{Z}_p)$ (corollary 1.5.7. of [**?**]), we get an isomorphism of $\alpha(\mathcal{X}_\infty/p^* - \mathrm{tors})(1)$ to $\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{X}_\infty, \mathbb{Z}_p(1))$.

$\square$

4. Degree 0 divisors on Frobenius elements

We observe that $(\gamma - 1)Y_\infty$ is the closed commutator subgroup of Y'_∞. Thus as $Y'_\infty = \mathrm{Gal}(M_\infty/F)$ and M_∞ is ramified only at the places above p, for each finite place q of F away from p we can consider the *Frobenius element* Frob_q of $Y'_\infty/(\gamma-1)Y_\infty$. As no prime q of F is fully decomposed in the cyclotomic extension F_∞/F, we see that $\deg(\mathrm{Frob}_q) \neq 0$ for every q.

We have an exact sequence of $\mathbb{Z}_p$-modules deduced from (**??**) that will also be of importance to us:

$$0 \to Y_\infty/(\gamma-1)Y_\infty \to Y'_\infty/(\gamma-1)Y_\infty \to \mathbb{Z}_p \to 0. \tag{2}$$

We consider a finite set of finite places $Q = \{q\}$ of F away from p, and thus unramified in M_∞/F.

Definition 4.1. *Let M'_Q be the $\mathbb{Z}_p$-submodule of $Y'_\infty/(\gamma-1)Y_\infty$ generated by the Frob_q's for $q \in Q$, and M_Q the $\mathbb{Z}_p$-submodule of M'_Q that is mapped to 0 under the map $Y'_\infty/(\gamma-1)Y_\infty \to \mathbb{Z}_p$ of (**??**). We call M_Q the (degree 0) Frobenius module (attached to Q).*

Lemma 4.2. *M_Q is the $\mathbb{Z}_p$-span of the degree 0, $\mathbb{Z}_p$-submodules $M_{q,q'}$ generated by $\mathrm{Frob}_q, \mathrm{Frob}_{q'}$ for $q, q' \in Q$, where in fact we may hold a $q' \in Q$ fixed as long as the subgroup generated by the image of $\mathrm{Frob}_{q'}$ in Γ contains that generated by Frob_q for all $q \in Q$.*

Proof. Note that the image of Frob_q in Γ of (at least) one element $q \in Q$ generates the subgroup of Γ generated by the Frob_q's for $q \in Q$. We choose one such and call it q'. Thus if we have an element $\alpha = \sum_{q\in Q} a_q \mathrm{Frob}_q \in M_Q, a_q \in \mathbb{Z}_p$, of degree 0, we can rewrite α as $\sum_{q\in Q\setminus\{q'\}}(a_q\mathrm{Frob}_q - a_{q,q'}\mathrm{Frob}_{q'})$ for some $a_{q,q'} \in \mathbb{Z}_p$ such that the degree of $a_q\mathrm{Frob}_q - a_{q,q'}\mathrm{Frob}_{q'}$ is 0. □

We will need to consider in the applications more particular choices of the set Q.

Proposition 4.3. *There is a finite set of primes $Q = \{q\}$ of F away from p such that Frob_q's for $q \in Q$ topologically generate $Y'_\infty/(\gamma-1)Y_\infty$. For such Q, M_Q equals $Y_\infty/(\gamma-1)Y_\infty$. We may further impose that the image of the Frob_q in Γ is a generator for all $q \in Q$.*

Proof. It is enough to choose a finite set of q's so that the Frob_q's generate the (finite extension given by the) maximal abelian $(p, \cdots, p)$ extension of F that is unramified outside p, and such that q is inert in F_∞/F. By Burnside's theorem such Frob_q's generate $Y'_\infty/(\gamma-1)Y_\infty$. The $\mathbb{Z}_p$-module M_Q of degree 0 is by our choice all of $Y_\infty/(\gamma-1)Y_\infty$, the degree 0 submodule of $Y'_\infty/(\gamma-1)Y_\infty$. □

In the next lemma, we consider compact groups M with a continuous action of Γ that comes from a structure of Λ-module of finite type on M, and the topology on M is the $\mathfrak{m}_\Lambda$-topology, where $\mathfrak{m}_\Lambda$ is the maximal ideal of Λ. Equivalently, M is the projective limit of a projective system of finite p-groups M_n with compatible actions of $\Gamma/p^n\Gamma$ and $M/\mathfrak{m}_\Lambda M$ is finite.

Definition 4.4. *For such a continuous Γ-module M, we define $H^1(\Gamma, M)$ by $M/(\gamma-1)M$ for γ any topological generator of Γ. It is independent of choice of the generator γ.*

Remark. $H^1(\Gamma, M)$ is also the continuous H^1.

The following lemma follows from snake lemma :

Lemma 4.5. *From an exact sequence of Γ-modules*

$$0 \to M_1 \to M \to M_2 \to 0$$

we get an exact sequence of abelian groups

$$0 \to M_1^\Gamma \to M^\Gamma \to M_2^\Gamma \to H^1(\Gamma, M_1).$$

For M as above, we denote by $H^1(\Gamma, M \otimes \mathbb{Q}_p)$ the continuous cohomology where $M \otimes \mathbb{Q}_p$ carries the group topology that induces on $M/\{p^\infty - \text{torsion}\}$ its topology. By compactness of Λ and flatness of $\mathbb{Q}_p$ over $\mathbb{Z}_p$, it is isomorphic to $H^1(\Gamma, M) \otimes \mathbb{Q}_p$.

The following proposition is well known :

Proposition 4.6. *Leopoldt's conjecture is equivalent to the finiteness of $H^1(\Gamma, Y_\infty) = Y_\infty/(\gamma - 1)Y_\infty$. Leopoldt's conjecture is also equivalent to the vanishing of $H^1(\Gamma, Y_\infty \otimes \mathbb{Q}_p)$.*

Proof. Observe that $Y'_\infty/(\gamma - 1)Y_\infty$ is the Galois group of the maximal abelian p extension of F unramified outside p. □

Thus, via Proposition **??**, Leopoldt's conjecture is equivalent to the finiteness of M_Q's of the proposition.

For later use we note:

Corollary 4.7. *The M_Q's for $Q = \{q_1, q_2\}$'s that are inert in F_∞/F span the finitely generated $\mathbb{Z}_p$-module $Y_\infty/(\gamma - 1)Y_\infty$.*

5. Reciprocity and splitting conjectures

We now consider a finite set of primes Q of F away from p and such that the image of Frob_q for $q \in Q$ generates Γ. We let m be the cardinality of Q. For each n consider the Sylow p-subgroup of the minus part of the ray class group of conductor Q_n, the ideal generated by the product of the primes above $\{q\}$ of $\mathcal{F}_n$. We denote this by $\mathcal{A}_{n,Q}^-$.

Definition 5.1. *Let $\mathcal{K}_{n,Q}^-$ denote the subgroup of the Sylow p-subgroup of $(\mathcal{O}_{\mathcal{F}_n}/Q_n)^*$ on which complex conjugation $\in \mathrm{Gal}(\mathcal{F}_n/F)$ acts by -1, modulo the image of the p-power roots of unity $\mu_{p^{n+t}}$ of $\mathcal{F}_n$.*

Lemma 5.2. *The group $\mathcal{K}_{n,Q}^-$ is isomorphic as a $\mathrm{Gal}(\mathcal{F}_n/F)$-module to $(\mu_{p^{n+t}})^m$ modulo the diagonally embedded $\mu_{p^{n+t}}$.*

Proof. If q_n is a prime of $\mathcal{F}_n$ above q, the p-Sylow of the multiplicative group $(k_{q_n})^*$ of the residue field of q_n is isomorphic by the reduction map modulo q_n to $\mu_{p^{n+t}}$. This follows from the fact that the primes in Q are inert in F_∞/F and that $\mu_{p^{n+t}}$ is the Sylow p-subgroup of the torsion subgroup of $\mathcal{F}_n^*$. To conclude, note that these isomorphisms are compatible with the action of $\mathrm{Gal}(\mathcal{F}_n/F)$ if q is inert in $\mathcal{F}$, and with the action of $\mathrm{Gal}(\mathcal{F}_n/\mathcal{F})$ if q split in $\mathcal{F}$. □

Lemma 5.3. *We have the exact sequence for each $n \geq 0$:*

$$0 \to \mathcal{K}_{n,Q}^- \to \mathcal{A}_{n,Q}^- \to \mathcal{A}_n^- \to 0 \tag{3}$$

We have the following commutative diagram where the vertical maps are induced by the inclusion maps $\mathcal{F}_n \hookrightarrow \mathcal{F}_{n+1}$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{K}_{n,Q}^- & \longrightarrow & \mathcal{A}_{n,Q}^- & \longrightarrow & \mathcal{A}_n^- & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{K}_{n+1,Q}^- & \longrightarrow & \mathcal{A}_{n+1,Q}^- & \longrightarrow & \mathcal{A}_{n+1}^- & \longrightarrow & 0 \end{array}$$

We also have the following commutative diagram where the vertical maps are induced by the norm maps $\mathcal{F}_{n+1} \to \mathcal{F}_n$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{K}_{n+1,Q}^- & \longrightarrow & \mathcal{A}_{n+1,Q}^- & \longrightarrow & \mathcal{A}_{n+1}^- & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{K}_{n,Q}^- & \longrightarrow & \mathcal{A}_{n,Q}^- & \longrightarrow & \mathcal{A}_n^- & \longrightarrow & 0 \end{array}$$

All the vertical maps in the first diagram are injective, and the first vertical map of the second commutative diagram is surjective.

Proof. The horizontal exact sequences follow from:

–If $\mathrm{Cl}_{\mathcal{F}_n}$ and $\mathrm{Cl}_{\mathcal{F}_n,Q_n}$ denote the ray class group of conductor 1 and Q_n of $\mathcal{F}_n$ respectively then we have an exact sequence

$$0 \to (\mathcal{O}_{\mathcal{F}_n}/Q_n)^*/\bar{E}_{\mathcal{F}_n} \to \mathrm{Cl}_{\mathcal{F}_n,Q_n} \to \mathrm{Cl}_{\mathcal{F}_n} \to 0$$

with $\bar{E}_{\mathcal{F}_n}$ the image of the global units $\mathcal{O}_{\mathcal{F}_n}^*$.

– For $\epsilon \in \mathcal{O}_{\mathcal{F}_n}^*$, $\epsilon/\bar{\epsilon}$ is a root of unity of $\mathcal{F}_n$.

– $p > 2$.

The commutativity of the diagrams is obvious.

Proposition 13.26 of [**?**] proves the injectivity of $\mathcal{A}_n^- \to \mathcal{A}_{n+1}^-$. The injectivity of the map $\mathcal{K}_{n,Q}^- \to \mathcal{K}_{n+1,Q}^-$ follows by inspection. This in turn yields the injectivity of $\mathcal{A}_{n,Q}^- \to \mathcal{A}_{n+1,Q}^-$.

Note that the norm map $\mathcal{K}_{n+1,Q}^- \to \mathcal{K}_{n,Q}^-$ is surjective as norm maps induce surjective maps between multiplicative groups of finite extensions of finite fields.

□

Corollary 5.4. *Consider the exact sequence (**??**).*

(1) *Taking direct limits of the exact sequence (**??**) as n varies, we get an exact sequence of discrete Λ-modules:*

$$0 \to \mathbb{Q}_p/\mathbb{Z}_p(1)^{m-1} \to \mathcal{A}_{\infty,Q}^- \to \mathcal{A}_\infty^- \to 0. \tag{4}$$

*Note further that as the first non-zero term of the sequence (**??**) is divisible, we have a $\mathbb{Z}_p$-linear section $f : \mathcal{A}_\infty^- \to \mathcal{A}_{\infty,Q}^-$.*

(2) *Taking inverse limits of terms of the exact sequence (**??**) with respect to norm maps we get the exact sequence of compact Γ-modules:*

$$0 \to \varprojlim \mathcal{K}_{n,Q}^- \simeq \mathbb{Z}_p(1)^{m-1} \to \varprojlim \mathcal{A}_{n,Q}^- \to \varprojlim \mathcal{A}_n^- \to 0. \tag{5}$$

which by class field theory is isomorphic to the exact sequence

$$0 \to I_Q \to \mathrm{Gal}(\mathcal{L}^-_{\infty,Q}/\mathcal{F}_\infty) \to \mathrm{Gal}(\mathcal{L}^-_\infty/\mathcal{F}_\infty) \to 0,$$

with $\mathcal{L}^-_{\infty,Q}$ the maximal abelian odd p-extension of $\mathcal{F}_\infty$ that is unramified outside the places above Q, and I_Q the subgroup of $\mathrm{Gal}(\mathcal{L}^-_{\infty,Q}/\mathcal{F}_\infty)$ generated by the inertia groups at the primes above Q of $\mathcal{F}_\infty$. We set $\mathcal{X}^-_{\infty,Q} = \mathrm{Gal}(\mathcal{L}^-_{\infty,Q}/\mathcal{F}_\infty)$ thus obtaining the exact sequence of Λ-modules

$$0 \to \mathbb{Z}_p(1)^{m-1} \to \mathcal{X}^-_{\infty,Q} \to \mathcal{X}^-_\infty \to 0. \tag{6}$$

Proof. The exactness in part (2) follows using Mittag-Leffler criterion Prop. 2.7.3 of [**?**]. □

5.1. *Cohomology classes:* We consider $m = 2$ (recall that m is the number of elements of Q). The exact sequence (**??**), gives rise to a cyclic $\mathbb{Z}_p$-submodule of $H^1(\Gamma, \mathrm{Hom}(\mathcal{A}^-_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1))) = H^1(\Gamma, Y_\infty)$ the latter isomorphism by Iwasawa duality. We define a cocycle corresponding to the above extension $c_\gamma \in \mathrm{Hom}(\mathcal{A}^-_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1))$ by $c_\gamma = \gamma f - f$ where f is a $\mathbb{Z}_p$-linear section $\mathcal{A}^-_\infty \to \mathcal{A}^-_{\infty,Q}$ which we know exists by Cor. **??**. The class of the cocycle $[c_\gamma]$ does not depend on the choice of the section f. We can also obtain $[c_\gamma]$ as follows. From the exact sequence (**??**), taking $\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{A}^-_\infty, -)$, using the divisibility of $\mathbb{Q}_p/\mathbb{Z}_p(1)$ we deduce the exact sequence

$$0 \to \mathrm{Hom}(\mathcal{A}^-_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1)) \to \mathrm{Hom}(\mathcal{A}^-_\infty, \mathcal{A}^-_{\infty,Q}) \to \mathrm{Hom}(\mathcal{A}^-_\infty, \mathcal{A}^-_\infty) \to 0,$$

and then taking Γ-invariants, Lemma **??** gives

$$0 \to \mathrm{Hom}(\mathcal{A}^-_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1))^\Gamma \to \mathrm{Hom}(\mathcal{A}^-_\infty, \mathcal{A}^-_{\infty,Q})^\Gamma \to \mathrm{Hom}(\mathcal{A}^-_\infty, \mathcal{A}^-_\infty)^\Gamma \to^\delta$$

$$H^1(\Gamma, \mathrm{Hom}(\mathcal{A}^-_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1))).$$

The cohomology class $[c_\gamma]$ is $\delta(\mathrm{id})$. We see that (**??**) splits as a sequence of Λ-modules if and only if $[c_\gamma] = 0$.

The $\mathbb{Z}_p$-module generated by $[c_\gamma]$ in the cohomology group, we call $N_Q \subset H^1(\Gamma, \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{A}^-_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1))) = H^1(\Gamma, Y_\infty)$, the latter being induced by the Iwasawa isomorphism.

5.2. *The reciprocity conjecture.*

Conjecture 5.5. *(Reciprocity conjecture) Under the Iwasawa isomorphism, N_Q is mapped isomorphically to M_Q (both of them are pro-p cyclic groups as $m = 2$).*

We view this as a reciprocity conjecture as we have the isomorphism (induced by the Iwasawa isomorphism)

$$H^1(\Gamma, Y_\infty) = H^1(\Gamma, \mathrm{Hom}(\mathcal{A}^-_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1))),$$

natural $\mathbb{Z}_p$-lines M_Q and N_Q on both sides associated to pairs of primes (q_1, q_2) such that the image of their Frobenius generates Γ. The conjecture predicts that these lines are exchanged under the Iwasawa isomorphism.
Remark: We may make a $\mathbb{Q}_p$ version of this conjecture. Namely we conjecture that the $\mathbb{Q}_p$-span of the class in $H^1(\Gamma, Y_\infty \otimes \mathbb{Q}_p)$ arising from the extension (**??**) made using the pairing $Y_\infty \times X_\infty^- \to \mathbb{Q}_p(1)$, is the same as $M_Q \otimes \mathbb{Q}_p$. (If we assume the Leopoldt conjecture this is simply asserting that $0 = 0$!)

5.3. *Heuristic justification for the conjecture vis a vis generalised Jacobians.* We develop an analogy mentioned in the introduction a little further by considering a direct analog of Conjecture **??** for function fields. Assume that X is a smooth projective defined over a finite field k, $P, Q \in X(k), P \neq Q$, with $J, J_{P,Q}$ as before. Let ℓ be a prime different from the characteristic of k. Consider the exact sequences of $\Gamma = \hat{\mathbb{Z}} = \mathrm{Gal}(\overline{k}/k)$ modules

$$0 \to \mathbb{Z}_\ell(1) \to \mathrm{Ta}_\ell(J_{P,Q}) \to \mathrm{Ta}_\ell(J) \to 0,$$

which splits as abelian groups. It is easily seen that it splits up to isogeny as Γ-modules using the Weil bounds on eigenvalues of Frobenius. The corresponding fact for number fields is unknown, and in analogy with function fields we conjecture it below.

Using the Weil pairing we get isomorphisms

$$H^1(\Gamma, \mathrm{Hom}_{\mathbb{Z}_\ell}(J(\overline{k})[\ell^\infty], \mathbb{Q}_\ell(1)/\mathbb{Z}_\ell(1))) \simeq H^1(\Gamma, \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathrm{Ta}_\ell(J), \mathbb{Z}_\ell(1)))$$

$$\simeq H^1(\Gamma, \mathrm{Ta}_\ell(J)) = J(k)[\ell^\infty].$$

Then just as we did in a similar situation earlier we can form a cyclic subgroup of $H^1(\Gamma, \mathrm{Ta}_\ell(J)) = J(k)[\ell^\infty]$ which arises from the extension classes arising from the exact sequence above. As N. Fakhruddin explained to us, in this case one can indentify this extension class with the projection of $(P) - (Q)$ to the ℓ-part of $J(k)$, in perfect analogy with our Conjecture **??**. One may allow K to be any field in the above considerations, by using the Kummer map $\widehat{J(K)} \to H^1(G_K, \mathrm{Ta}_\ell(J))$ where $\widehat{J(K)}$ is the pro-ℓ completion of $J(K)$, instead of the isomorphism $H^1(\Gamma, \mathrm{Ta}_\ell(J)) = J(k)[\ell^\infty]$ when K is a finite field.

5.4. *Splitting conjectures.*

5.4.1. *Splitting of ramification away from p.* We make the following splitting conjecture motivated by analogy with generalised Jacobians over finite fields.

Conjecture 5.6. *The exact sequence (**??**) $\otimes \mathbb{Q}_p$, i.e.,*

$$0 \to \mathbb{Q}_p(1)^{m-1} \to \mathcal{X}_{\infty,Q}^- \otimes \mathbb{Q}_p \to \mathcal{X}_\infty^- \otimes \mathbb{Q}_p \to 0,$$

of Γ-modules splits.

5.4.2. *Splitting of ramification at p.* We make an analogous conjecture for splitting of a certain (cyclotomic) part of the ramification at p. We recall the following results of Iwasawa.

Lemma 5.7. *(Iwasawa) Let $\wp'_1, \cdots, \wp'_{s'}$ be the places above p of $\mathcal{F}_\infty$, and $\wp_1, \cdots, \wp_s$ the places of F above p. Denote by $\mathcal{F}_{\infty,i} = \cup \mathcal{F}_{n,i}$ the corresponding extension of the completion of F for $i = 1, \cdots, s'$. Let $G_{\wp_j}$ be decomposition subgroups of $G = \mathrm{Gal}(\mathcal{F}_\infty/F)$ at the places $\wp_j$ of F.*

Let $\mathcal{U}_i := \lim_{\leftarrow} U^1_{\mathcal{F}_{n,i}}$, where $U^1_{\mathcal{F}_{n,i}}$ are the principal units in the completion $\mathcal{F}_{n,i}$ and the inverse limit is with respect to the norm maps. Let $\mathcal{U} = \Pi_{i=1}^{s'} \mathcal{U}_i$, which is a $\mathbb{Z}_p[[G]]$-module. Then we have an isomorphism of $\mathbb{Z}_p[[G]]$-modules $\mathcal{U} \simeq (\bigoplus_{j=1}^{s} \mathrm{Ind}_{G_{\wp_j}}^{G} \mathbb{Z}_p(1)) \bigoplus \mathbb{Z}_p[[G]]^{[F:\mathbb{Q}]}$.

Proof. This follows easily from Theorem 11.2.4 of [**?**].

□

Corollary 5.8. *Recall that s is the number of places above p of F. Let N_∞ be the maximal odd abelian p-extension N_∞ of $\mathcal{F}_\infty$ such that Γ acts by the p-adic cyclotomic character χ on the inertia subgroups above p, and let N'_∞ be the maximal odd abelian p-extension N'_∞ of $\mathcal{F}_\infty$ that is unramified outside p, and such that Γ acts by the p-adic cyclotomic character χ on the inertia subgroups above p.*

– 1. The $\mathbb{Z}_p$-rank of the group I_p generated by inertia groups at the places above p of $\mathcal{F}_\infty$ in the Galois group $\mathrm{Gal}(N_\infty/\mathcal{F}_\infty)$ is $[F : \mathbb{Q}] + s$.

– 2. The $\mathbb{Z}_p$-rank of the group I'_p generated by the inertia groups at the places above p of $\mathcal{F}_\infty$, in the Galois group $\mathrm{Gal}(N'_\infty/\mathcal{F}_\infty)$ is $[F : \mathbb{Q}] + s - 1$.

Proof. By class field theory, for every n, the image of inertia above p in the Galois group of the maximal abelian odd p-extension of $\mathcal{F}_n$ is isomorphic to $U^1_{\mathcal{F}_n}$. The first part of the corollary then follows from the last lemma and the fact that the image of inertia above p in $\mathrm{Gal}(N_\infty/\mathcal{F}_\infty)$ is isomorphic theory to $\mathcal{U}/(\gamma' - \chi(\gamma'))$ where γ' is a generator of $\mathrm{Gal}(\mathcal{F}_\infty/F)$. Similarly the image of inertia above p in $\mathrm{Gal}(N'_\infty/\mathcal{F}_\infty)$ is isomorphic by class field theory to $\frac{\mathcal{U}/(\gamma' - \chi(\gamma'))}{\mathbb{Z}_p(1)}$. □

We call $\mathcal{X}^-_{\infty,p} = \mathrm{Gal}(N'_\infty/\mathcal{F}_\infty)$. We have an exact sequence of Λ-modules :

$$0 \to I'_p \otimes \mathbb{Q}_p \to \mathcal{X}^-_{\infty,p} \otimes \mathbb{Q}_p \to \mathcal{X}^-_\infty \otimes \mathbb{Q}_p \to 0, \tag{7}$$

We know by Cor. **??** that $I'_p \otimes \mathbb{Q}_p$ is isomorphic to $\mathbb{Q}_p(1)^{[F:\mathbb{Q}]+s-1}$ as Λ-module.

We make in the situation another splitting conjecture.

Conjecture 5.9. *The exact sequence (**??**) of Λ-modules splits.*

6. Relation to Leopoldt's conjecure

We show that the splitting conjectures are equivalent to Leopoldt's conjecture.

We begin with some generalities. We denote by F_p^* the group $\Pi_{v|p}F_v^*$, U_F the group $\Pi_{v|p}U_{F_v}$ with U_{F_v} the units of F_v. We denote by U_F^1 the group $\Pi_{v|p}U_{F_v}^1$ of 1-units.

Definition 6.1. – *We say that a Λ map $M \to N$ of compact finitely generated torsion Λ-modules is an isogeny if the kernel and cokernel are torsion abelian groups (necessarily of bounded exponent and finitely generated as Λ-modules).*

– *If*

$$0 \to K \to M \to N \to 0$$

is a sequence of compact finitely generated torsion Λ-modules, we say that it splits up to isogeny if the sequence of Λ-modules

$$0 \to K \otimes \mathbb{Q}_p \to M \otimes \mathbb{Q}_p \to N \otimes \mathbb{Q}_p \to 0$$

splits.

We have a lemma that is a direct consequence of the definition.

Lemma 6.2. *Consider an exact sequence*

$$0 \to K \to M \to N \to 0$$

of compact finitely generated torsion Λ-modules. It splits up to isogeny if and only if M has a Λ-submodule N' with the natural map $N' \to N$ an isogeny.

The following lemma is easily proved.

Lemma 6.3. *Conjecture* **??***, in the case $Q = \{q_1, q_2\}$ with q_i inert in F_∞/F, is true if and only if there is a $\mathbb{Z}_p$-extension L_Q of $\mathcal{F}_\infty$ that is Galois over F, ramified at q_1, q_2 and unramified everywhere else, and on which complex conjugation acts by -1.*

Note that Γ acts on $\mathrm{Gal}(L_Q/\mathcal{F}_\infty)$ by the p-adic cyclotomic character as the q_i are inert in F_∞/F, and thus L_Q is a $\mathbb{Z}_p$-Kummer extension of $\mathcal{F}_\infty$, with $L_Q/\mathcal{F}_\infty$ unramified outside the primes above Q, and ramified at all the primes in Q. Leopoldt's conjecture predicts that there is a unique such extension.

Proof. Only the "only if" direction needs proof. Assume that the conjecture is true. Then by the previous lemma we get $X \subset \mathcal{X}_{\infty,Q}^-$ a Λ-submodule with $X \to \mathcal{X}_\infty^-$ having kernel and cokernel killed by a power of p. We define L_Q as the subfield of $\mathcal{L}_{\infty,Q}^-$ which under the Galois correspondence is such that it is Galois over $\mathcal{F}_\infty$, and its Galois group over $\mathcal{F}_\infty$ is the quotient of $\mathcal{X}_{\infty,Q}^-/X$ by its p-power torsion. □

Theorem 6.4. *Consider $Q = \{q_1, q_2\}$ a tuple of primes of F, inert in F_∞/F. Then the exact sequence in Conjecture **??** splits if and only if the degree 0 Frobenius submodule M_Q of $Y_\infty/(\gamma-1)Y_\infty$ is a finite group.*

Proof. Consider the 1-units U_F^1 of $\Pi_{v|p}F_v^*$, and the subgroup $\overline{E_F^1}$ the closure of the global units E_F^1 that are 1 mod v for all $v|p$. We note the standard exact sequence from class field theory:

$$0 \to U_F^1/\overline{E_F^1} \to Y'_\infty/(\gamma-1)Y_\infty \to C \to 0, \tag{8}$$

where $Y'_\infty/(\gamma-1)Y_\infty$ is the Galois group of the maximal abelian p-extension of F unramified outside p, where C is the Sylow p-subgroup of the ideal class group of F (cf. Chapter 13 of [**?**]).

By Lemma **??** we have to show that the existence of an L_Q as in its statement is equivalent to M_Q being finite. Recall that $\widehat{F_p^*}$ is the product $\prod_{v|p}\widehat{F_v^*}$ for v the primes of F above p and we have a natural localisation map $\mathrm{loc}_p : \widehat{F^*} \to \widehat{F_p^*}$. By the results of §**??**, the existence of a $\mathbb{Z}_p$-Kummer extension L_Q of F, such that $L_Q/\mathcal{F}_\infty$ is ramified precisely at all the primes above Q, is equivalent to the existence of an element α of $\widehat{E_Q} \subset \widehat{F^*}$ such that $v_t(\alpha) \neq 0$ for $t = q_1, q_2$, and $\mathrm{loc}_p(\alpha)$ is torsion. By replacing α by a power of α, we can suppose that $\mathrm{loc}_p(\alpha)$ is trivial.

Suppose that the exact sequence of Conjecture 5.9. splits. Then we get an α as above. Its image by the map $\widehat{E_Q} \to U_F^1/\overline{E_F^1} \to Y'_\infty/(\gamma-1)Y_\infty$ is $\mathrm{Frob}_{q_1}^{a_1}\mathrm{Frob}_{q_2}^{a_2}$ for $a_i \in \mathbb{Z}_p$. It is trivial as $\mathrm{loc}_p(\alpha)$ is trivial. As $v_t(\alpha) \neq 0$ for $t = q_1, q_2$, we get that $a_i \neq 0$ and this produces a non-trivial $\mathbb{Z}_p$-linear relation between Frob_{q_1} and Frob_{q_2}, hence M_Q is finite.

Conversely suppose that M_Q is finite. Let, for $i = 1, 2$, α_i be elements of F^* which generates a power of the ideal q_i. As M_Q is finite, the images of α_1 and α_2 in $U_F^1/\overline{E_F^1}$ are $\mathbb{Z}_p$-linearly independent. It follows that there exists a_1 and a_2 non zero elements of $\mathbb{Z}_p$ and $\alpha_3 \in \overline{E_F^1}$ such that $\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3 = 1$ in U_F^1. Lifting α_3 to $\epsilon \in \widehat{E_F^1}$, we get an element $\alpha := \alpha_1^{a_1}\alpha_2^{a_2}\epsilon \in \widehat{F^*}$. It satisfies the required properties : $v_{q_i}(\alpha) \neq 0$ and $\mathrm{loc}_p(\alpha) = 1$. The theorem follows. □

Corollary 6.5. *Conjecture **??** is true for all tuples of primes $Q = \{q_1, q_2\}$ which are inert in F_∞/F if and only if Leopoldt's conjecture is true.*

Proof. We need only prove that the truth of Conjecture **??** for tuples $Q = \{q_1, q_2\}$ inert in F_∞/F implies Leopoldt's conjecture. For this we note (cf. Cor. **??**) that the M_Q's span the finitely generated $\mathbb{Z}_p$-module $Y_\infty/(\gamma-1)Y_\infty$ for such Q. By the theorem, Conjecture **??** implies that M_Q is of finite order. □

Remark. The fact that Leopoldt's conjecture implies the splitting of the exact sequence of conjecture **??** also follows as then the Λ-modules $\mathbb{Q}_p(1)^{m-1}$ and $\mathcal{X}_\infty^- \otimes \mathbb{Q}_p$ have characteristic polynomials which are prime to each other.

Proposition 6.6. *Conjecture* **??** *is equivalent to Leopoldt's conjecture.*

Proof. Consider E'_F the group of p-units of F. By the unit theorem it has $\mathbb{Z}$-rank $[F:\mathbb{Q}]+s-1$. Let $\mathcal{L}=\mathcal{F}_\infty({E'_F}^{1/p^\infty})$: it is the maximal abelian p-extension of $\mathcal{F}_\infty$ which is ramified only at primes above p and such that the action of Γ on $\mathrm{Gal}(\mathcal{L}/\mathcal{F}_\infty)$ is via the p-adic cyclotomic character. By the first part of lemma **??**, the $\mathbb{Z}_p$-rank of $\mathrm{Gal}(\mathcal{L}/\mathcal{F}_\infty)$ equals the $\mathbb{Z}$-rank of E'_F, *i.e.* $[F:\mathbb{Q}]+s-1$. By the second part of the lemma, the subgroup of $\mathrm{Gal}(\mathcal{L}/\mathcal{F}_\infty)$ generated the inertia subgroups above p has $\mathbb{Z}_p$-rank ($\mathbb{Z}_p$-rank of the submodule $\overline{E_F^1}$ of U_F^1)+s. One version of Leopoldt's conjecture is that ($\mathbb{Z}_p$-rank of the submodule $\overline{E_F^1}$ of U_F^1)= $[F,\mathbb{Q}]-1$. We see that Leopoldt's conjecture is equivalent to the assertion that $\mathcal{L}$ is almost totally ramified over $\mathcal{F}_\infty$.

If Leopoldt's conjecture is true, the morphism $\mathbb{Q}_p\otimes_{\mathbb{Z}_p} I'_p \to \mathbb{Q}_p\otimes_{\mathbb{Z}_p}\mathrm{Gal}(\mathcal{L}/\mathcal{F}_\infty)$ is surjective, hence bijective as the source and the target have the same dimension. We see that $\mathcal{X}_{\infty,p}^- \to \mathrm{Gal}(\mathcal{L}/\mathcal{F}_\infty)$ defines an up tho isogeny splitting of (7).

Suppose that (7) splits up to isogeny. Let $\mathcal{L}'$ be the extension of $\mathcal{F}_\infty$ defined by this splitting. Then $\mathcal{L}'$ is unramified outside p and acted via the p-adic cyclotomic character by Γ as it is on I'_p. It follows that $\mathcal{L}'\subset\mathcal{L}$. As $\mathcal{L}'$ is almost totally ramified and $\mathrm{Gal}(\mathcal{L}'/\mathcal{F}_\infty)$ has $\mathbb{Z}_p$ rank $[F:\mathbb{Q}]+s-1$, it follows that the rank of the subgroup of $\mathrm{Gal}(\mathcal{L}/\mathcal{F}_\infty)$ generated by the inertia subgroups above p is $[F:\mathbb{Q}]+s-1$. One deduces that $\mathcal{L}$ is almost totally ramified over $\mathcal{F}_\infty$, hence Leopoldt's conjecture is true.

□

7. Some evidence for the reciprocity conjecture

Using the Kummer theory of §**??**, when (**??**) splits after tensoring with $\mathbb{Q}_p$ as Λ-modules, we measure precisely its failure to split over $\mathbb{Z}_p$. This then lends support to our reciprocity conjecture.

We define G to be the group $Y'_\infty/(\gamma-1)Y_\infty$. Hence the exact sequence (**??**) becomes :

$$0\to U_F^1/\overline{E_F^1}\to G\to C\to 0, \tag{9}$$

We define the quotient G' of G by the image in $U_F^1/\overline{E_F^1}$ of the roots of unity, denoted by μ, of p-power order of the product F_p^* of the multiplicative groups of completions of F at primes above p. We consider as before $Q=\{q_1,q_2\}$ with q_1 and q_2 distinct primes not above p and inert in F_∞/F. Recall that $\leq_\infty$ is the maximal abelian p-extension which is unramified everywhere.

Theorem 7.1. *Assume that the order of the degree 0 Frobenius module M_Q is finite. It is equivalent to assuming that a Kummer $\mathbb{Z}_p$-extension $L_Q/\mathcal{F}_\infty$ exists with $L_Q/\mathcal{F}_\infty$ unramified at a place if and only if it does not lie above a prime in Q (cf. Lemma* **??** *and Theorem* **??***). Then for any such L_Q, the*

degree $[L_Q \cap \mathcal{L}_\infty^- : \mathcal{F}_\infty]$ *is divisible by the order* m_Q *of the image of* M_Q *in* G'*. Furthermore there exists such an* L_Q *with* $[L_Q \cap \mathcal{L}_\infty^- : \mathcal{F}_\infty] = m_Q$*.*

Note that if Leopoldt's conjecture is true for F and p, then such an L_Q exists and is unique.

Proof. In the first part of the proof, let us fix L_Q as in the statement of the theorem and let us prove that $[L_Q \cap \mathcal{L}_\infty^- : \mathcal{F}_\infty]$ is divisible by m_Q.

By the Kummer theory in §**??**, one gets an $\alpha \in \widehat{F^*}$, in fact even in the p-adic completion $\widehat{E_Q}$ of the Q-units of F^*, such that $L_Q = F(\mu_{p^\infty}, \alpha^{\frac{1}{p^\infty}})$. We may assume that $\alpha \notin (\widehat{F^*})^p$ equivalently not in $(\widehat{E_Q})^p$.

Lemma 7.2. *For each* n*,* $F(\mu_{p^\infty}, \alpha^{\frac{1}{p^n}})$ *is cyclic of order* p^n *over* $\mathcal{F}_\infty$*. The valuations* $v_{q_1}(\alpha)$ *and* $v_{q_2}(\alpha)$ *are non zero and generate the same ideal ideal in* $\mathbb{Z}_p$*. If* (p^a) *is this ideal, we have* $p^a = [L_Q \cap \mathcal{L}_\infty^- : \mathcal{F}_\infty]$

Proof. The first part of the lemma follows from $H^1(\mathrm{Gal}(\mathcal{F}_\infty/F), \mu_p) = 0$. This is a consequence of $\mu_p(F) = 1$.

Consider the map $\widehat{F^*} \to \widehat{\mathbb{Q}^*} \to \widehat{\mathbb{Q}_p^*}$, where the first arrow is induced by the norm and the second one by the localisation map loc_p. It sends α to $N(q_1)^{v_{p_1}(\alpha)} N(q_2)^{v_{p_2}(\alpha)}$. Its image in $U^1_{\mathbb{Z}_p}$ is trivial as $\mathrm{loc}_p(\alpha)$ is torsion. As q_1 and q_2 are inert in F_∞, the norms $N(q_1)$ and $N(q_2)$ have images in $U^1_{\mathbb{Z}_p}$ such that that $N(q_1)-1$ and $N(q_2)-1$ topologically generate the same ideal in $\mathbb{Z}_p$. The second part of the lemma follows.

The third part follows from the fact that $\mathcal{F}_n(\alpha^{1/p^a})$ is unramified at q_i for $n + t \geq a$ if and only if p^a divides $v_{q_i}(\alpha)$ and the first part of the lemma. □

By the Kummer theory in §**??** we deduce that $\alpha \in \widehat{E_Q}$ of the first paragraph of the proof has the properties:

– $\mathrm{loc}_p(\alpha)$ is torsion, and hence the natural norm map $\widehat{E_Q} \to \widehat{\mathbb{Q}_p^*}$ evaluates α to 1.

– $v_t(\alpha) = 0$ for $t \notin Q$

– $v_{q_i}(\alpha) \neq 0$ and generate the same ideal say (m) in $\mathbb{Z}_p$.

– $\alpha \notin (\widehat{F^*})^p$

We note that the $\mathbb{Z}_p$-submodule M_Q of G is generated by any element of the form $\mathrm{Frob}_{q_1}^{a_1}\mathrm{Frob}_{q_2}^{a_2}$ with $a_i \in \mathbb{Z}_p^*$, such that its image in $\mathrm{Gal}(F_\infty/F)$ is trivial. An explicit generator is gotten by taking $a_1 = -\log_{\langle N(q_1)\rangle}\langle N(q_2)\rangle), a_2 = 1$ where by $\langle N(q_i)\rangle$ we mean the projection of $N(q_i)$ to Γ in the decomposition $\mathbb{Z}_p^* = \mathbb{Z}/(p-1)\mathbb{Z} \times \Gamma$.

Consider the image of such an α in the Galois group G' by the map $\widehat{E_Q} \to U_F^1 \to G \to G'$. On the one hand it is trivial as $\mathrm{loc}_p(\alpha)$ is torsion. But on the other hand, as $\mathrm{loc}_p(N(\alpha)) = 1$, it is also of the form $(\mathrm{Frob}_{q_1}^{a_1}\mathrm{Frob}_{q_2}^{a_2})^m$ with Frob_{q_i} denoting the Frobenius at q_i in the abelian Galois group G', and with $a_i \in \mathbb{Z}_p^*$. From this we deduce that m_Q divides m. By Lemma **??** we

deduce that the degree $[L_Q \cap \mathcal{L}_\infty^- : \mathcal{F}_\infty]$ is divisible by the order m_Q of the image of M_Q in G'. This finishes the first part of the proof.

The following lemma finishes the proof of the theorem.

Lemma 7.3. *There is an element $\alpha \in \widehat{F^*}$ such that*
– $\mathrm{loc}_p(\alpha)$ *is torsion*
– $v_t(\alpha) = 0$ *for* $t \notin Q$
– $(v_{q_1}(\alpha)) = (v_{q_2}(\alpha)) = (m_Q)$ *as ideals in* $\mathbb{Z}_p$.

We note for later use that if M_Q is trivial we get an element $\alpha \in \widehat{F^*}$ such that
– $\mathrm{loc}_p(\alpha) = 1$
– $v_t(\alpha) = 0$ *for* $t \notin Q$
– $(v_{q_1}(\alpha)) = (v_{q_2}(\alpha)) = \mathbb{Z}_p$.

Consider $L_\alpha = \mathcal{F}_\infty(\alpha^{\frac{1}{p^\infty}})$ with α as in the first part of the lemma. By §**??** we get that L_α is a $\mathbb{Z}_p$-Kummer extension such that $L_\alpha/\mathcal{F}_\infty$ is ramified exactly at the primes above q_1, q_2. Furthermore by Lemma **??**, $[L_\alpha \cap \mathcal{L}_\infty^- : \mathcal{F}_\infty] = m_Q$.

Thus we only need to prove the lemma. We recall the exact sequence (**??**) from earlier:

$$0 \to Y_\infty/(\gamma - 1)Y_\infty \to Y'_\infty/(\gamma - 1)Y_\infty \to \mathbb{Z}_p \to 0.$$

Recall that M_Q is a submodule of $Y_\infty/(\gamma - 1)Y_\infty$. Consider a generator F_Q of M_Q which we may write as $\mathrm{Frob}_{q_1}^{a_1}\mathrm{Frob}_{q_2}^{a_2}$ with $a_i \in \mathbb{Z}_p$. We note again that $a_i \in \mathbb{Z}_p^*$ by the assumption that the primes in Q are inert in F_∞/F. Let n be the order of the prime to p part of the class group of F. Then we may regard $(q_1^{a_1}q_2^{a_2})^{nm_Q}$ as a well-defined element α' of $\widehat{E_Q}/\widehat{E_F}$ as follows. Choose m large enough so that $q_i^{p^m}$ has image in the class group Cl_F of F of order prime to p. Choose $b_i \in \mathbb{Z}$ so that a_i is congruent to b_i modulo p^m: write $a_i = b_i + p^m c_i$ with $c_i \in \mathbb{Z}_p$. Note that $(q_1^{b_1}q_2^{b_2})^{nm_Q}$ has trivial image in the class group Cl_F, as $(\mathrm{Frob}_{q_1}^{a_1}\mathrm{Frob}_{q_2}^{a_2})^{m_Q}$ is trivial in G', and thus gives rise to a well-defined element β of E_Q/E_F whose image in $\widehat{E_Q}/\widehat{E_F}$ we denote by the same symbol. Here we are using the exact sequence (**??**). Furthermore $(q_1^{np^mc_1}q_2^{np^mc_2})^{m_Q}$ gives rise to a well-defined element β' of $\widehat{E_Q}/\widehat{E_F}$. Thus taking product $\beta\beta'$ we see that altogether $(q_1^{a_1}q_2^{a_2})^{nm_Q}$ gives rise to a well-defined element α' of $\widehat{E_Q}/\widehat{E_F}$ independent of choice of m. Furthermore, the natural map $\widehat{E_Q}/\widehat{E_F} \to U_F^1/\overline{E_F^1}\mu$ sends α' to 1.

Choose $\alpha'' \in \widehat{E}_Q$ which projects to α', and by choice maps to an element of $\overline{E_F^1}\mu$ under the natural map $\widehat{E_Q} \to U_F^1$. Thus the image of α'' in F_p^*/μ is the image of an e' for $e' \in \overline{E_F^1}$. Let e be any inverse image of e' under the natural map $\widehat{E_F} \to \overline{E_F^1}$. We set $\alpha = \alpha''.e^{-1}$, and see that $\mathrm{loc}_p(\alpha)$ is torsion, $\alpha \in \widehat{E_Q}$, and $(v_{q_i}(\alpha)) = (m_Q)$. The second part of the lemma follows by a similar argument.

□

We may verify one consequence of our reciprocity conjecture as (ii) of the following corollary:

Corollary 7.4. *(i) The exact sequence (??) of Λ-modules splits if and only if $m_Q = 1$.*

(ii) For a tuple of primes $Q = \{q_1, q_2\}$ inert in F_∞/F, M_Q trivial implies that the exact sequence (??) of Λ-modules splits.

Proof. (i) The sequence (**??**) splits if and only if there is a Kummer $\mathbb{Z}_p$-extension L_Q as in the theorem with the property that $L_Q \cap \mathcal{L}_\infty^-$ is trivial. This is equivalent by the theorem to $m_Q = 1$.

(ii) By the lemma **??** in the proof above, under the assumption that M_Q is trivial we get an element α of $\widehat{E_Q}$ such that $\mathrm{loc}_p(\alpha) = 1$, and $v_{q_i}(\alpha)$ is a unit for q_i in Q. Then for any n, the extension of $\mathcal{F}_n$ given by $\mathcal{F}_n(\alpha^{\frac{1}{p^{n+t}}})$ is cyclic of degree p^{n+t}, unramified outside the primes above Q, and has no non-trivial unramified subextension. By class field theory this provides a compatible sequence of splittings of the exact sequences (**??**), and thus a splitting of (**??**).

□

Remark: We may also verify the converse of part (ii) of the corollary in some situations, for instance when $\mathcal{F}_\infty/F$ has a unique prime above p and is totally ramified at this prime.

8. Even extensions of Iwasawa modules

We state the theorem of Iwasawa proved in U4 of [**?**].

Theorem 8.1. *(Iwasawa) Leopoldt's conjecture is equivalent to the following statement: For any set of finite places Q disjoint from S_p the map*

$$H^1(S_p \cup Q, \mathbb{Q}_p/\mathbb{Z}_p) \to \prod_{v \in Q} H^1(I_v, \mathbb{Q}_p/\mathbb{Z}_p)^{D_v}$$

is surjective.

Remark: Iwasawa stated his criterion as: Leopoldt's conjecture, cf. Conjecture **??**, is true if and only for every prime q prime to p of F, the image of inertia at the prime q in $\mathrm{Gal}(F_{p,q}/F)$, with $F_{p,q}$ the maximal abelian p-extension of F unramified outside p, q, has order $e(q)$, the p-part of the order of the multiplicative group of the residue field at q, denoted by k_q^*.

Now we transcribe the result of Iwasawa into an Iwasawa theoretic setting, i.e., a statement over $\mathcal{F}_\infty$. It stands in counterpoint to the situation in the odd case.

Consider a finite set of primes Q away from p of F such that their norm is 1 modulo p. (if $v \in Q$ is such that p does not divide $N(q)-1$, $H^1(I_v, \mathbb{Q}_p/\mathbb{Z}_p)^{D_v}$ is trivial). We consider the maximal abelian p-extension $M_\infty(Q)$ of F_∞ that is unramified outside p and Q with Galois group $Y_{\infty,Q}$. We assume for simplicity that Q contains only one place q

Then we have an exact sequence of Γ or Λ-modules:

$$0 \to K_Q \to Y_{\infty,Q} \to Y_\infty \to 0 \tag{10}$$

where the Iwasawa module K_Q is simply given by $\Lambda/((1+T)^{p^b} - u^{p^b})$ where $\gamma(\zeta_{p^n}) = \zeta_{p^n}^u$ and $u^{p^b} - 1$ is divisible by the same power of p as $N(q)-1$. One sees this as in [**?**] using Kummer theory, which also shows that the exact sequence (**??**) splits up to isogeny.

Lemma 8.2. *Leopoldt's conjecture is true for F, p if and only if the exact sequence (**??**) remains exact on going modulo T for each choice of q.*

Proof. Note that the sequence (**??**) remains exact on going modulo T if and only if the image of an inertia group above q in $\mathrm{Gal}(F_{p,q}/F)$ is of order the p-part of $N(q) - 1$, namely $e(q)$. Then we are done by the equivalence of Theorem **??**. □

It is interesting to note that in the odd case the sequence (**??**) remains exact on going modulo T, while its splitting up to isogeny (for all Q) is equivalent to Leopoldt's conjecture. In the even case, the exact sequence (**??**) does split up to isogeny, as shown by Greeenberg in loc. cit. using Kummer theory, but its remaining exact on going modulo T is equivalent to Leopoldt's conjecture. Iwasawa's criterion, and the one in this paper, are dual in a sense that gains precision using considerations in the next section.

9. Appendix

P. Colmez showed us a nice argument using L-functions which, assuming $F/\mathbb{Q}$ is a totally real finite Galois extension of $\mathbb{Q}$, proves that if Leopoldt's conjecture is false then $\zeta_{F,p}(s)$ has to vanish at $s = 1$ where $\zeta_{F,p}(s)$ is the Deligne-Ribet p-adic L-function of F. We note that by [**?**] and [**?**], the Leopoldt conjecture is true if and only if $\zeta_{F,p}(s)$ has a pole at $s = 1$.

We give Colmez's argument. The p-adic zeta function $\zeta_{F,p}(s)$ has a factorisation into certain p-adic Artin L-functions (cf. [**?**])

$$\zeta_{F,p}(s) = \Pi_\chi L_{\mathbb{Q},p}(s,\chi)^{\chi(1)},$$

with χ running through the irreducible p-adic representations of $\mathrm{Gal}(F/\mathbb{Q})$. Note that for χ a non-trivial representation, $L_{F,p}(s,\chi)$ is entire by the p-adic form of the Artin conjecture which is proved in [**?**] to follow from the main conjecture. The factor for χ the trivial representation has a simple pole at $s = 1$, and for other non-trivial abelian characters χ, the corresponding factor does not vanish at $s = 1$, by the known case of the Leopoldt conjecture for abelian extensions of $\mathbb{Q}$ (cf. [**?**]). Thus if the Leopoldt conjecture is false for F, p, for a representation χ of dimension at least 2, $L_{\mathbb{Q},p}(1,\chi)$ vanishes and this by the factorisation formula forces $\zeta_{F,p}(1)$ to vanish.

We now give a simple algebraic argument, to deduce from the known cases of the Leopoldt conjecture for abelian extensions of $\mathbb{Q}$, that the Leopoldt defect $\delta_{F,p}$ can never be 1 for $F/\mathbb{Q}$ a totally real finite Galois extension. It is

an apparent strengthening of Colmez's result as it could conceivably happen that $\delta_{F,p} = 1$ while $\zeta_{F,p}(1) = 0$ ("non-semisimplicty of Leopoldt zeros"). It will be nice to remove the assumption that $F/\mathbb{Q}$ is Galois; this seems to require other methods.

Proposition 9.1. *For $F/\mathbb{Q}$ a totally real finite Galois extension and a prime p, the Leopoldt defect $\delta_{F,p}$ is never 1.*

Proof. Suppose that $\delta_{F,p} = 1$. Let us call N the compositum of the $\mathbb{Z}_p$-extensions of F. Let $L = \mathrm{Gal}(N/F)$: L is a free $\mathbb{Z}_p$-module of rank 2. The inclusion $F_\infty \subset N$ gives a surjective morphism $L \to \Gamma$. Let H_1 be the Galois group of $F/\mathbb{Q}$. We see that the action of H_1 on $\mathbb{Q}_p \otimes L$ factors though the character η giving the action of H_1 on $\mathbb{Q}_p \otimes (L/\Gamma)$. Hence the action of H_1 on L factors through η. Let H be the kernel of η and F_η the field corresponding to H. The next lemma implies the existence of an extension N' of F_η of Galois group a free $\mathbb{Z}_p$-module of rank 2 such that $N = N'F$. This is impossible as F_η is abelian over $\mathbb{Q}$ and we know Leopoldt conjecture for F_η and p.

Lemma 9.2. *Let $1 \to L \to G \to H \to 1$ be an exact sequence of profinite groups with L a free $\mathbb{Z}_p$-module of finite rank d. We suppose that H is finite and acts trivially on L. Then, there exists a free $\mathbb{Z}_p$-module L' of rank d and a surjective morphism $G \to L'$.*

Let $o \in H^2(H, L)$ be the cohomology class defined by the extension. Let us prove first that the conclusion of the lemma is equivalent to that there exists an inclusion $L \hookrightarrow L'$ of $\mathbb{Z}_p$-modules of rank d such that the image o' of o in $H^2(H, L')$ is trivial.

Indeed, if there exists $L \hookrightarrow L'$ such that o' is trivial, the pushout exact sequence $1 \to L' \to G' \to H \to 1$ has a trivialisation $G' \to L'$. If we compose it with the morphism $G \to G'$ we get a morphism $G \to L'$ that coincide on L with the inclusion $L \hookrightarrow L'$.

Conversely, if we have a surjection $G \to L'$, its restriction to L has a finite index image as H is finite. This implies that this restriction is injective. The morphism $G \to L'$ extends to the pushout G' as a trivialisation of the pushout exact sequence.

Let us prove the lemma when H is a p-group. Let us prove it in this case by induction on the cardinality of H. If H is trivial, there is nothing to prove. Otherwise, let $H' \subset H$ be a central subgroup of order p. Let G'' be the inverse image of H' in G. As the action of H on L is trivial and H' is cyclic, the group G'' is abelian. If G'' has no torsion, we can apply the induction hypothesis to the exact sequence $1 \to G'' \to G \to H/H' \to 1$ to get a surjective morphism of G in $(\mathbb{Z}_p)^d$. If G'' has torsion T, T is cyclic of order p and $G \to H$ induces an isomorphism of T to H'. We apply the induction hypothesis to the exact sequence $1 \to L \to G/T \to H/H' \to 1$. We get a surjective morphism of G/T to $(\mathbb{Z}_p)^d$ hence a surjective morphism of G to $(\mathbb{Z}_p)^d$.

Let us prove the lemma in the general case. Let H_p a p-Sylow of H. Let $L \hookrightarrow L'$ be such that the image of the restriction of o' to H_p vanishes. The morphism $H^2(H, L') \to H^2(H_p, L')$ is injective. This follows from the injectivity of the maps $H^2(H, L'/p^n L') \to H^2(H_p, L'/p^n L')$ and Mittag-Leffler. We see that o' is trivial and this proves the lemma.

□

References

[1] John Coates. K-theory and Iwasawa's analogue of the Jacobian. Algebraic K-theory II, SLN 341, p. 502-520.

[2] Armand Brumer. On the units of algebraic number fields. Mathematika 14, 1967, 121124.

[3] Pierre Colmez. Résidu en s=1 des fonctions zeta p-adiques. Invent. Math. 91 (1988), no. 2, 371389.

[4] Manfred Kolster, Thong Nguyen Quang Do, Vincent Fleckinger. Twisted S-units, p-adic class number formulas, and the Lichtenbaum conjectures, Duke Math. J.,84,1996,679-717.

[5] Ralph Greenberg. On p-adic L-functions and Cyclotomic fields II. Nagoya Math. J., 67, 1977, p. 139-158.

[6] Ralph Greenberg. On p-adic Artin L-functions. Nagoya Math. J. 89 (1983), 77–87.

[7] Kenkichi Iwasawa. Collected Papers I and II. Springer-Verlag.

[8] J. Neukirch, A. Schmidt, K. Wingberg. Cohomology of number fields. Springer-Verlag.

[9] Jean-Pierre Serre. Sur le résidu de la fonction zeta p-adique d'un corps de nombres. C. R. Acad. Sci. Paris Sr. A-B 287 (1978), no. 4, A183A188.

[10] Larry Washington. Introduction to Cyclotomic Fields (2nd edition). Springer-Verlag.

[11] Andrew Wiles. The Iwasawa conjecture for totally real fields. Ann. of Math. (2) 131 (1990), no. 3, 493–540.

E-mail address: shekhar84112@gmail.com

Department of Mathematics, UCLA, Los Angeles, CA 90095-1555, U.S.A.

E-mail address: wintenb@math.u-strasbg.fr

Université de Strasbourg, Département de Mathématique, Membre de l'Institut Universitaire de France, 7, rue René Descartes, 67084, Strasbourg Cedex, France