

# RAMIFICATION IN IWASAWA MODULES

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. INTRODUCTION

For a number field  $F$ , with ring of integers  $\mathcal{O}_F$ , we may define the class group of  $F$  to be  $\text{Pic}(\mathcal{O}_F)$ , i.e., the isomorphism classes of invertible sheaves on  $\text{Spec}(\mathcal{O}_F)$ . 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  $p$ -subgroups 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  $\gamma$ , a generator for the  $p$ -part of  $\text{Gal}(F(\mu_{p^\infty})/F)$ . 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  $\ell$ -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  $\text{Ext}^1(J, \mathbb{G}_m) = \text{Pic}^0(J) = J$ . 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 curve over  $K$  with nodal singularity. We have an exact sequence

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

---

CK was partially supported by NSF grants.

JPW is member of the Institut Universitaire de France.

The standard fact alluded to earlier is that the class of  $J_{P,Q}$  in  $\text{Ext}^1(J, \mathbb{G}_m)$  is given by the class of the degree 0 divisor  $(P) - (Q)$ . We make a reciprocity conjecture, see Conjecture 5.5, that asks for an analogous formula in Iwasawa theory. To formulate this conjecture, we consider ramification at *auxiliary primes* in Iwasawa modules (see §5), define analogs of degree 0 divisors supported on Frobenius elements in certain Galois groups (see §4), and use a well-known pairing of Iwasawa (see §3). We prove an implication of the reciprocity conjecture (see Theorem 7.1 and Corollary 7.4). 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 5.6, that we show in Corollary 6.5 to be equivalent to the following standard conjecture:

**Conjecture 1.1.** (*Leopoldt*) *The cyclotomic  $\mathbb{Z}_p$ -extension  $F_\infty/F$  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, and  $\delta_{F,p}$  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 [9] which draws on Hida's theory of  $\Lambda$ -adic Hilbert modular forms. This search led to Conjecture 5.6. As Conjecture 5.6 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 2, 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  $F_\infty$ . We denote by  $\gamma$  a chosen topological generator of  $\Gamma$ , and by  $\chi$  the  $p$ -adic cyclotomic character. The field  $F_\infty$  is contained in  $\mathcal{F}_\infty = F(\mu_{p^\infty})$ , whose real subfield we denote by  $F^\infty$ ;  $F_\infty$  is contained in  $F^\infty$ . 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  $\mu_{p^t}$  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  $\text{Gal}(\mathcal{F}_\infty/F)$  acts on  $\text{Gal}(L/\mathcal{F}_\infty)$  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  $\Lambda$ -module with same underlying module  $M$ , and the  $\Lambda$ -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  $\text{Gal}(L/K)$ .

*1.2. Acknowledgements.* We would like to thank Gebhard Böckle, John Coates, Najmuddin Fakhruddin, David Gieseke, Ralph Greenberg, Benedict Gross, Haruzo Hida, Tony Scholl, Chris Skinner, Kevin Ventullo for helpful conversations. The first author thanks the Département de Mathématiques 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 Poincaré - 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 which presumably are well known. They are basic to the work of this paper. For lack of a reference known to us, we provide proofs of these results.

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  $F$  if  $L/F$  is Galois and it is such that  $\text{Gal}(L/\mathcal{F}_\infty) \simeq \mathbb{Z}_p$  is isomorphic to  $\mathbb{Z}_p(1)$  as a  $\text{Gal}(\mathcal{F}_\infty/F)$ -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  $K_{F,n} : F^*/(F^*)^{p^n} \rightarrow H^1(G_F, \mu_{p^n})$ . Taking the projective limits for  $n$ , we get an isomorphism  $K_F : \widehat{F^*} \rightarrow H^1(G_F, \mathbb{Z}_p(1))$ , where the  $H^1$  are continuous  $H^1$ , the topology of  $\mathbb{Z}_p(1)$  being the  $p$ -adic one ([6]).

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  $K_F(\bar{x})$  under the map  $H^1(G_F, \mathbb{Z}_p(1)) \rightarrow \text{Hom}(G_{\mathcal{F}_\infty}, \mathbb{Z}_p(1))^0$ , where the Hom are continuous homomorphisms and  $^0$  means fixed by  $\text{Gal}(\mathcal{F}_\infty/F)$ .

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  $\epsilon$ . 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  $H^1(\text{Gal}(\mathcal{F}_\infty/F), \mu_{p^n}(\overline{F}))$  and  $H^2(\text{Gal}(\mathcal{F}_\infty/F), \mu_{p^n}(\overline{F}))$  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:

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

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 [6]). The lemma implies that  $H^1(\text{Gal}(\mathcal{F}_\infty/F), \mathbb{Z}_p(1))$  is torsion. It then follows from the above exact sequence, the fact that  $H^1(G_{\mathcal{F}_\infty}, \mathbb{Z}_p(1)) = \text{Hom}(G_{\mathcal{F}_\infty}, \mathbb{Z}_p(1))$  has no torsion, and the bijectivity of the Kummer map  $K_F$ , that the kernel of the map  $\widehat{F^*} \rightarrow \text{Hom}(G_{\mathcal{F}_\infty}, \mathbb{Z}_p(1))$  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  $G_{\mathcal{F}_\infty} \rightarrow \mathbb{Z}_p(1)$  whose kernel corresponds to  $L$ . Let  $f_n$  be the morphisms  $G_{\mathcal{F}_\infty} \rightarrow \mu_{p^n}(\overline{F})$  defined by  $f$ . As  $H^2(\text{Gal}(\mathcal{F}_\infty/F), \mu_{p^n}(\overline{F}))$  is killed by  $p^a$ ,  $p^a f_n$  is the image of an element  $\bar{x}_n$  of  $F^*/(F^*)^{p^n}$ . As  $H^1(\text{Gal}(\mathcal{F}_\infty/F), \mu_{p^n}(\overline{F}))$  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  $K_F(\bar{x}') = p^{2a}f$ , 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  $\text{Gal}(\mathcal{F}_\infty/F)$  is isomorphic to  $\mathbb{Z}_p$ . Let  $\gamma$  a generator of  $\text{Gal}(\mathcal{F}_\infty/F)$  and  $\chi_p(\gamma)$  its image by the cyclotomic character. The calculation of the cohomology of the procyclic group  $\mathbb{Z}_p$  gives that  $H^1(\text{Gal}(\mathcal{F}_\infty/F), \mu_{p^n}(\overline{F}))$  is isomorphic to  $(\mathbb{Z}/p^n\mathbb{Z})/(\chi_p(\sigma) - 1)$  and  $H^2(\text{Gal}(\mathcal{F}_\infty/F), \mu_{p^n}(\overline{F}))$  is trivial (prop. 1.7.7 of chap. 1 paragraph 7 of [6]). The lemma follows as  $\chi_p(\gamma) \neq 1$ .  $\square$

*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 elements 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 abelian group 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  $\widehat{F_{\mathfrak{q}}^*} \rightarrow \mathbb{Z}_p$  induced by  $v_{\mathfrak{q}}$ . We denote by  $\text{loc}_{\mathfrak{q}}$  the morphism  $\widehat{F^*} \rightarrow \widehat{F_{\mathfrak{q}}^*}$  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  $\text{loc}_{\mathfrak{q}}(\bar{x})$  is torsion.*

*Proof.* Let us note  $E = F_{\mathfrak{q}}$  and  $E_{\text{ur}}$  the maximal unramified extension of  $E$ . The proposition follows from proposition 2.1 and the fact that the kernel of  $\widehat{E^*} \rightarrow \widehat{E_{\text{ur}}^*}$  is torsion. For this fact, let  $\omega$  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  $\widehat{E_{\text{ur}}^*} \simeq \omega^{\mathbb{Z}_p}$ . If  $\mathfrak{q}$  is above  $p$ , we have  $\widehat{E^*} \simeq \omega^{\mathbb{Z}_p} U_E^+$  and  $\widehat{E_{\text{ur}}^*} \simeq \omega^{\mathbb{Z}_p} U_{E_{\text{ur}}}^+$ , where  $U^+$  are units that  $\equiv 1 \pmod{\omega}$  and  $\widehat{E_{\text{ur}}}$  is the completion of  $E_{\text{ur}}$ . The map  $U_F^+ \rightarrow U_{E_{\text{ur}}}^+$ , is injective as  $U_{E_{\text{ur}}}^+$  is separated for the  $p$ -adic topology.  $\square$

*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

$E_Q/E_Q^{p^n} \rightarrow F^*/(F^*)^{p^n}$  are injective, hence also the map  $\widehat{E}_Q \rightarrow \widehat{F}^*$ . 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 2.3.

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 divisible by  $p^n$  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  $\epsilon_n$  a unit in  $O_Q$  such that  $x_n = y_n^{p^{n-a}} \epsilon_n$ . We see that  $x_n$  and  $\epsilon_n$  have the same image in  $F^*/(F^*)^{p^{n-a}}$ . It follows that the  $\epsilon_n$  define an element  $\epsilon$  of  $\widehat{E}_Q$  with image  $x$  in  $\widehat{F}^*$ . The proposition is proved.  $\square$

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 the subgroup generated by the inertia groups above  $Q$  in  $\text{Gal}(F_T/\mathcal{F}_{\infty})$  is the same as the  $\mathbb{Z}_p$ -rank of the closure of (the diagonal image of)  $T$  in  $\prod_{v \in Q} \widehat{F}_v^*$ .*

*Proof.* For  $v \in Q$ , let  $v'$  be a prime of  $\mathcal{F}_{\infty}$  above  $v$  and let  $I_{v'}$  be the inertia subgroup of  $\text{Gal}(F_T/\mathcal{F}_{\infty})$  at  $v'$ . As the action of  $\text{Gal}(\mathcal{F}_{\infty}/F)$  on  $\text{Gal}(F_T/\mathcal{F}_{\infty})$  is by the cyclotomic character  $\chi_p$ , 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:

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

The lemma follows from the fact that the horizontal arrows have torsion kernels by propositions 2.1 and 2.3.  $\square$

## 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  $\mathcal{X}_\infty = \text{Gal}(\mathcal{L}_\infty/\mathcal{F}_\infty)$ . 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  $\Lambda$ -module.

Let  $M_\infty$  be the maximal abelian  $p$ -extension of  $F_\infty$  that is unramified outside  $p$ . We set  $Y_\infty = \text{Gal}(M_\infty/F_\infty)$ . Again by a theorem of Iwasawa,  $Y_\infty$  is a finitely generated torsion  $\Lambda$ -module. We denote by  $Y'_\infty = \text{Gal}(M_\infty/F)$ , which sits inside an exact sequence

$$(1) \quad 0 \rightarrow Y_\infty \rightarrow Y'_\infty \rightarrow \mathbb{Z}_p \rightarrow 0.$$

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

Recall a couple of facts:

- $Y_\infty, \mathcal{X}_\infty^-$  have no non-zero finite  $\Lambda$ -modules (cf. Propositions 15.36 and 13.28 of [8]). This may also be deduced from 11.4.4 of [6] which states that  $\mathcal{X}_\infty^-$  is the adjoint of a finitely generated torsion  $\Lambda$ -module, and th. 11.4.8 of [6].
- $Y_\infty \otimes \mathbb{Q}_p$  and  $\mathcal{X}_\infty^- \otimes \mathbb{Q}_p$  are finite dimensional  $\mathbb{Q}_p$ -vector spaces. Although the  $\mu$ -invariant of  $F_\infty$  is not known to be zero, and thus we do not know that  $Y_\infty$  is a finitely generated  $\mathbb{Z}_p$ -module, we do know that  $Y_\infty/(\gamma - 1)Y_\infty$  is a finitely generated  $\mathbb{Z}_p$ -module.

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

**Lemma 3.1.** *For a  $\Lambda$ -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  $\text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p) = M^0 \otimes \mathbb{Q}_p$ .*

*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  $\text{GL}_n(K)$ .  $\square$

We denote by  $\tilde{\alpha}(X)$  the Iwasawa dual of the adjoint of a finitely generated, torsion  $\Lambda$ -module  $X$ , see §1 of article 52 of [5], or §15.5 of [8]. Thus the adjoint  $\alpha(X) = \tilde{\alpha}(X)^0$ .

**Lemma 3.2.** (*Iwasawa*) *We have that  $X$  and  $\alpha(X)$  are pseudo-isomorphic, hence  $\tilde{\alpha}(X)$  is pseudo-isomorphic to  $X^0$ .*

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

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

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

*which we call the Iwasawa pairing, equivalently*

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

*which we call the Iwasawa isomorphism.*

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

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

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

*or equivalently*

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

*Proof.* (i) Proposition 13.32 of [8] or Theorem 11.4.3 of [6].

(ii) Proposition 15.34 of [8] and its proof, or Theorem 11.1.8 of [6].

(iii) Theorem 11.1.8 of [6] gives an isomorphism of  $Y_\infty = \text{Hom}_{\mathbb{Z}_p}(\mathcal{A}_\infty^-, \mathbb{Q}_p/\mathbb{Z}_p(1))$  to  $\alpha(\mathcal{X}'_\infty)(1)$  where  $\mathcal{X}'_\infty$  is a sub  $\Lambda$ -module of  $\mathcal{X}_\infty$  of finite index. The natural map  $\alpha(\mathcal{X}_\infty)(1) \rightarrow \alpha(\mathcal{X}'_\infty)(1)$  is an isomorphism after  $\otimes \mathbb{Q}_p$ . It is the same for the natural map  $\alpha(\mathcal{X}_\infty/p^* - \text{tors})(1) \rightarrow \alpha(\mathcal{X}'_\infty)(1)$ . As for  $X$  finitely generated torsion  $\Lambda$ -module without  $p$ -torsion,  $\alpha(X)$  is isomorphic to  $\text{Hom}_{\mathbb{Z}_p}(X, \mathbb{Z}_p)$  (corollary 1.5.7. of [6]), we get an isomorphism of  $\alpha(\mathcal{X}_\infty/p^* - \text{tors})(1)$  to  $\text{Hom}_{\mathbb{Z}_p}(\mathcal{X}_\infty, \mathbb{Z}_p(1))$ . This concludes the proof of the proposition. □

#### 4. DEGREE 0 DIVISORS ON FROBENIUS ELEMENTS

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

We have an exact sequence of  $\mathbb{Z}_p$ -modules deduced from (1) that will also be of importance to us:

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

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

**Definition 4.1.** Let  $M'_Q$  be the  $\mathbb{Z}_p$ -submodule of  $Y'_\infty/(\gamma-1)Y_\infty$  generated by the  $\text{Frob}_q$ 's for  $q \in Q$ , and  $M_Q$  the  $\mathbb{Z}_p$ -submodule of  $M'_Q$  that is mapped to 0 under the map  $Y'_\infty/(\gamma-1)Y_\infty \rightarrow \mathbb{Z}_p$  of (2). 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  $\text{Frob}_q, \text{Frob}_{q'}$  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  $\text{Frob}_{q'}$  in  $\Gamma$  contains that generated by  $\text{Frob}_q$  for all  $q \in Q$ .

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

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  $\text{Frob}_q$ '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  $\text{Frob}_q$  in  $\Gamma$  is a generator for all  $q \in Q$ .

*Proof.* It is enough to choose a finite set of  $q$ 's so that the  $\text{Frob}_q$ 's generate the (finite extension given by the) maximal abelian  $(p, \dots, p)$  extension of  $F$  that is unramified outside  $p$ , and such that  $q$  is inert in  $F_\infty/F$ . By Burnside's theorem such  $\text{Frob}_q$ '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  $Y'_\infty/(\gamma-1)Y_\infty$ .  $\square$

In the next lemma, we consider compact groups  $M$  with a continuous action of  $\Gamma$  that comes from a structure of  $\Lambda$ -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  $\Lambda$ . 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  $\Gamma$ -module  $M$ , we define  $H^1(\Gamma, M)$  by  $M/(\gamma-1)M$  for  $\gamma$  any topological generator of  $\Gamma$ . It is independent of choice of the generator  $\gamma$ .

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

We have the following lemma :

**Lemma 4.5.** From an exact sequence of  $\Gamma$ -modules

$$0 \rightarrow M_1 \rightarrow M \rightarrow M_2 \rightarrow 0$$

we get an exact sequence of abelian groups

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

*Proof.* It follows from the exact sequence of continuous cohomology groups. This exact sequence is available as by compactness the topology of  $M_1$  is induced by the topology of  $M$  and the map  $M \rightarrow M_2$  has a continuous section (in the category of sets). To get a continuous section apply Mittag-Leffler to the projective system of sections of  $M/\mathfrak{m}^n M \rightarrow M_2/\mathfrak{m}^n M_2$ .  $\square$

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  $M/p$ -tors its topology. By compactness of  $\Lambda$  and flatness of  $\mathbb{Q}_p$  over  $\mathbb{Z}_p$ , it is isomorphic to  $H^1(\Gamma, M) \otimes \mathbb{Q}_p$ .

**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  $p$ .  $\square$

Thus, via Proposition 4.6, Leopoldt's conjecture is equivalent to the finiteness of  $M_Q$ 's of the proposition. It is also equivalent to the finiteness of the degree 0 submodule generated by  $\text{Frob}_q, \text{Frob}_{q'}$  for any two places  $q, q'$  not dividing  $p$  by Lemma 4.2 above.

For later use we note:

**Corollary 4.7.** *The  $M_Q$ 's for  $Q = \{q_1, q_2\}$ 's that are inert in  $F_\infty/F$  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  $\text{Frob}_q$  for  $q \in Q$  generates  $\Gamma$ . 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  $\in \text{Gal}(\mathcal{F}_n/F)$  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  $\text{Gal}(\mathcal{F}_n/F)$ -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  $F_\infty/F$  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  $\text{Gal}(\mathcal{F}_n/F)$  if  $q$  is inert in  $\mathcal{F}$ , and with the action of  $\text{Gal}(\mathcal{F}_n/\mathcal{F})$  if  $q$  split in  $\mathcal{F}$ .  $\square$

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

$$(3) \quad 0 \rightarrow \mathcal{K}_{n,Q}^- \rightarrow \mathcal{A}_{n,Q}^- \rightarrow \mathcal{A}_n^- \rightarrow 0$$

*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  $\mathcal{F}_{n+1} \rightarrow \mathcal{F}_n$ :*

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

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

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

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

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

**Corollary 5.4.** *Consider the exact sequence (3).*

(1) *Taking direct limits of the exact sequence (3) as  $n$  varies, we get an exact sequence of discrete  $\Lambda$ -modules:*

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

*Note further that as the first non-zero term of the sequence (4) is divisible, we have a  $\mathbb{Z}_p$ -linear section  $f : \mathcal{A}_{\infty}^- \rightarrow \mathcal{A}_{\infty, Q}^-$ .*

(2) Taking inverse limits of terms of the exact sequence (3) with respect to norm maps we get the exact sequence of compact  $\Gamma$ -modules:

$$(5) \quad 0 \rightarrow \lim_{\leftarrow} \mathcal{K}_{n,Q}^- \simeq \mathbb{Z}_p(1)^{m-1} \rightarrow \lim_{\leftarrow} \mathcal{A}_{n,Q}^- \rightarrow \lim_{\leftarrow} \mathcal{A}_n^- \rightarrow 0.$$

which by class field theory is isomorphic to the exact sequence

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

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  $\Lambda$ -modules

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

*Proof.* The exactness in part (2) follows using Mittag-Leffler criterion Prop. 2.7.3 of [6].  $\square$

5.1. *Cohomology classes:* We consider  $m = 2$  (recall that  $m$  is the number of elements of  $Q$ ). The exact sequence (4), 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  $\mathcal{A}_{\infty}^- \rightarrow \mathcal{A}_{\infty,Q}^-$  which we know exists by Cor. 5.4. 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 (4), 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

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

and then taking  $\Gamma$ -invariants, Lemma 4.5 gives

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

The cohomology class  $[c_{\gamma}]$  is  $\delta(\mathrm{id})$ . We see that (4) splits as a sequence of  $\Lambda$ -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)

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

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  $\Gamma$ . The conjecture predicts that these lines are preserved 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 (6) made using the pairing  $Y_\infty \times X_\infty^- \rightarrow \mathbb{Q}_p(1)$ , is the same as the  $M_Q \otimes \mathbb{Q}_p$ . (Of course assuming the Leopoldt conjecture this is 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 5.5 for function fields. Assume that  $X$  is a smooth projective defined over a finite field  $k$ ,  $P, Q \in X(k)$ , with  $J, J_{P,Q}$  as before. Let  $\ell$  be a prime different from the characteristic of  $k$ . Consider the exact sequences of  $\Gamma = \hat{\mathbb{Z}} = \text{Gal}(\bar{k}/k)$  modules

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

which splits as abelian groups. It is easily seen that it splits up to isogeny as  $\Gamma$ -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

$$\begin{aligned} H^1(\Gamma, \text{Hom}_{\mathbb{Z}_\ell}(J(\bar{k})[\ell^\infty], \mathbb{Q}_\ell(1)/\mathbb{Z}_\ell(1))) &\simeq H^1(\Gamma, \text{Hom}_{\mathbb{Z}_\ell}(\text{Ta}_\ell(J), \mathbb{Z}_\ell(1))) \\ &\simeq H^1(\Gamma, \text{Ta}_\ell(J)) = J(k)[\ell^\infty]. \end{aligned}$$

Then just as we did in a similar situation earlier we can form a cyclic subgroup of  $H^1(\Gamma, \text{Ta}_\ell(J)) = J(k)[\ell^\infty]$  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  $\ell$ -part of  $J(k)$ , in perfect analogy with our Conjecture 5.5. One may allow  $K$  to be any field in the above considerations, by using the Kummer map  $\widehat{J(K)} \rightarrow H^1(G_K, \text{Ta}_\ell(J))$  where  $\widehat{J(K)}$  is the pro- $\ell$  completion of  $J(K)$ , instead of the isomorphism  $H^1(\Gamma, \text{Ta}_\ell(J)) = J(k)[\ell^\infty]$  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 (6)  $\otimes \mathbb{Q}_p$ , i.e.,*

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

of  $\Gamma$ -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  $\wp'_1, \dots, \wp'_{s'}$  be the places above  $p$  of  $\mathcal{F}_\infty$ , and  $\wp_1, \dots, \wp_s$  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  $i = 1, \dots, s'$ . Let  $G_{\wp_j}$  be decomposition subgroups of  $G = \text{Gal}(\mathcal{F}_\infty/F)$  at the places  $\wp_j$  of  $F$ .

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

*Proof.* This follows easily from Theorem 11.2.4 of [6]. □

**Corollary 5.8.** Recall that  $s$  is the number of places above  $p$  of  $F$ .

– 1. The  $\mathbb{Z}_p$ -rank of the group generated by inertia groups at the places above  $p$  of  $\mathcal{F}_\infty$  in the Galois group of the maximal odd abelian  $p$ -extension  $N_\infty$  of  $\mathcal{F}_\infty$  on which  $\Gamma$  acts by the  $p$ -adic cyclotomic character  $\chi$  on the inertia above  $p$ , say  $I_p$ , is  $[F:\mathbb{Q}] + s$ .

– 2. The  $\mathbb{Z}_p$ -rank of the group generated by the inertia groups at the places above  $p$  of  $\mathcal{F}_\infty$ , in the Galois group that we denote by  $\mathcal{X}_{\infty,p}^-$ , of the maximal odd abelian  $p$ -extension  $N'_\infty$  of  $\mathcal{F}_\infty$  that is unramified outside  $p$ , and on which  $\Gamma$  acts by the  $p$ -adic cyclotomic character  $\chi$  on the inertia above  $p$ , say  $I'_p$ , 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  $U_{\mathcal{F}_n}^1$ . The first part of the corollary then follows from the last lemma and the fact that the image of inertia above  $p$  in  $\text{Gal}(N_\infty/\mathcal{F}_\infty)$  is isomorphic to  $\mathcal{U}/(\gamma' - \chi(\gamma'))$  where  $\gamma'$  is a generator of  $\text{Gal}(\mathcal{F}_\infty/F)$ . Similarly the image of inertia above  $p$  in  $\text{Gal}(N'_\infty/\mathcal{F}_\infty)$  is isomorphic by class field theory to  $\frac{\mathcal{U}/(\gamma' - \chi(\gamma'))}{\mathbb{Z}_p(1)}$ . □

Consider  $\mathcal{X}_{\infty,p}^-$ , the Galois group of the maximal odd abelian  $p$ -extension, denoted  $N'_\infty$  above, of  $\mathcal{F}_\infty$  that is unramified outside  $p$ , and on which  $\text{Gal}(\mathcal{F}_\infty/F)$  acts on the subgroup  $I'_p$  generated by the inertia groups at places above  $p$  via the  $p$ -adic cyclotomic character  $\chi$ . Then we have an exact sequence of  $\Lambda$ -modules

$$(7) \quad 0 \rightarrow I'_p \otimes \mathbb{Q}_p \rightarrow \mathcal{X}_{\infty,p}^- \otimes \mathbb{Q}_p \rightarrow \mathcal{X}_\infty^- \otimes \mathbb{Q}_p \rightarrow 0,$$

We know by Cor. 5.8 that  $I'_p \otimes \mathbb{Q}_p$  is isomorphic to  $\mathbb{Q}_p(1)^{[F:\mathbb{Q}] + s - 1}$  as  $\Lambda$ -module.

We make in the situation another splitting conjecture.

**Conjecture 5.9.** *The exact sequence (7) of  $\Lambda$ -modules splits.*

## 6. RELATION TO LEOPOLDT'S CONJECTURE

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  $\Lambda$  map  $M \rightarrow N$  of compact finitely generated torsion  $\Lambda$ -modules is an isogeny if the kernel and cokernel are torsion abelian groups (necessarily of bounded exponent and finitely generated as  $\Lambda$ -modules).*

– *If*

$$0 \rightarrow K \rightarrow M \rightarrow N \rightarrow 0$$

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

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

*splits.*

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

**Lemma 6.2.** *Consider an exact sequence*

$$0 \rightarrow K \rightarrow M \rightarrow N \rightarrow 0$$

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

The following lemma is easily proved.

**Lemma 6.3.** *Conjecture 5.6, in the case  $Q = \{q_1, q_2\}$  with  $q_i$  inert in  $F_\infty/F$ , 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  $\Gamma$  acts on  $\text{Gal}(L_Q/\mathcal{F}_\infty)$  by the  $p$ -adic cyclotomic character as the  $q_i$  are inert in  $F_\infty/F$ , and thus  $L_Q$  is a  $\mathbb{Z}_p$ -Kummer extension of  $F$ , 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  $\Lambda$ -submodule with  $X \rightarrow \mathcal{X}_\infty^-$  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.  $\square$

**Theorem 6.4.** *Consider  $Q = \{q_1, q_2\}$  a tuple of primes of  $F$ , inert in  $F_\infty/F$ . Then the exact sequence in Conjecture 5.6 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  $\prod_{v|p} F_v^*$ , 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:

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

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 [8]).

By Lemma 6.3 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  $\text{loc}_p : \widehat{F}^* \rightarrow \widehat{F}_p^*$ . By the results of §2, 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  $\alpha$  of  $\widehat{E}_Q \subset \widehat{F}^*$  such that  $v_t(\alpha) \neq 0$  for  $t = q_1, q_2$ , and  $\text{loc}_p(\alpha)$  is torsion. By replacing  $\alpha$  by a power of  $\alpha$ , we can suppose that  $\text{loc}_p(\alpha)$  is trivial.

Suppose that the exact sequence of Conjecture 5.9. splits. Then we get an  $\alpha$  as above. Its image by the map  $\widehat{E}_Q \rightarrow U_F^1/\overline{E_F^1} \rightarrow Y'_\infty/(\gamma-1)Y_\infty$  is  $\text{Frob}_{q_1}^{a_1} \text{Frob}_{q_2}^{a_2}$  for  $a_i \in \mathbb{Z}_p$ . It is trivial as  $\text{loc}_p(\alpha)$  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  $\text{Frob}_{q_1}$  and  $\text{Frob}_{q_2}$ , hence  $M_Q$  is finite.

Conversely suppose that  $M_Q$  is finite. Let, for  $i = 1, 2$ ,  $\alpha_i$  be elements of  $F^*$  which generates a power of the ideal  $q_i$ . As  $M_Q$  is finite, the images of  $\alpha_1$  and  $\alpha_2$  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  $\alpha_3$  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  $\text{loc}_p(\alpha) = 1$ . The theorem follows.  $\square$

**Corollary 6.5.** *Conjecture 5.6 is true for all tuples of primes  $Q = \{q_1, q_2\}$  which are inert in  $F_\infty/F$  if and only if Leopoldt's conjecture is true.*

*Proof.* We need only prove that the truth of Conjecture 5.6 for tuples  $Q = \{q_1, q_2\}$  inert in  $F_\infty/F$  implies Leopoldt's conjecture. For this we note (cf. Cor. 4.7) 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 5.6 implies that  $M_Q$  is of finite order.  $\square$

*Remark.* The fact that Leopoldt's conjecture implies the splitting of the exact sequence of conjecture 5.6 also follows as then the  $\Lambda$ -modules  $\mathbb{Q}_p(1)^{m-1}$  and  $X_\infty^- \otimes \mathbb{Q}_p$  have characteristic polynomials which are prime to each other.

**Proposition 6.6.** *Conjecture 5.9 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  $[F : \mathbb{Q}] + s - 1$ . We claim that (7) splits if and only if the  $p^\infty$ -Kummer extension  $\mathcal{L} = \mathcal{F}_\infty(E'_F{}^{1/p^\infty})$  of  $\mathcal{F}_\infty$ , whose Galois group has  $\mathbb{Z}_p$ -rank  $[F : \mathbb{Q}] + s - 1$  (see the results of §2 for instance), is almost totally ramified at  $p$ . If Leopoldt's conjecture is true, which is equivalent to  $\mathcal{X}_\infty^-/(\gamma - \chi(\gamma))$  being finite, then as the action of  $\Gamma$  on  $\text{Gal}(\mathcal{L}/\mathcal{F}_\infty)$  is via the  $p$ -adic cyclotomic character,  $\mathcal{L}$  is almost linearly disjoint from  $\mathcal{L}_\infty^-$  over  $\mathcal{F}_\infty$ , which implies that  $\mathcal{L}/\mathcal{F}_\infty$  is almost totally ramified above  $p$ . On the other hand if  $\mathcal{L}/\mathcal{F}_\infty$  is almost totally ramified at  $p$ , we may deduce that the  $p$ -adic completion of the units  $E_F$  of  $F$  in  $U_F^1$  has rank  $[F : \mathbb{Q}] - 1$ . This is another form of the Leopoldt conjecture. For the deduction we use Proposition 2.3 and Lemma 2.5. Namely we see that the  $\mathbb{Z}_p$ -rank of the subgroup generated by the inertia groups above  $p$  in  $\text{Gal}(\mathcal{L}/\mathcal{F}_\infty) = (\mathbb{Z}_p\text{-rank of the submodule } \overline{E_F^1} \text{ of } U_F^1) + s$ .  $\square$

## 7. SOME EVIDENCE FOR THE RECIPROCITY CONJECTURE

Using the Kummer theory of §2, when (6) splits after tensoring with  $\mathbb{Q}_p$  as  $\Lambda$ -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 (8) becomes :

$$(9) \quad 0 \rightarrow U_F^1/\overline{E_F^1} \rightarrow G \rightarrow C \rightarrow 0,$$

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  $\mu$ , 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  $F_\infty/F$ .

**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  $L_Q/F$  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 6.3 and Theorem 6.4). 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 §2, 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 the triviality of  $H^1(\text{Gal}(\mathcal{F}_\infty/F), \mu_p) = 0$ . This triviality follows from the triviality of  $\mu_p(F)$ .

Consider the map  $\widehat{F}^* \rightarrow \widehat{\mathbb{Q}}^* \rightarrow \widehat{\mathbb{Q}}_p^*$ , where the first arrow is induced by the norm and the second one by the localisation map  $\text{loc}_p$ . It sends  $\alpha$  to  $N(q_1)^{v_{p_1}(\alpha)} N(q_2)^{v_{p_2}(\alpha)}$ . Its image in  $U_{\mathbb{Z}_p}^1$  is trivial as  $\text{loc}_p(\alpha)$  is torsion. As  $q_1$  and  $q_2$  are inert in  $F_\infty$ , the norms  $N(q_1)$  and  $N(q_2)$  have images in  $U_{\mathbb{Z}_p}^1$  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.  $\square$

By the Kummer theory in §2 we deduce that  $\alpha \in \widehat{E}_Q$  of the first paragraph of the proof has the properties:

- $\text{loc}_p(\alpha)$  is torsion, and hence the natural norm map  $\widehat{E}_Q \rightarrow \widehat{\mathbb{Q}}_p^*$  evaluates  $\alpha$  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  $\text{Frob}_{q_1}^{a_1} \text{Frob}_{q_2}^{a_2}$  with  $a_i \in \mathbb{Z}_p^*$ , such that its image in  $\text{Gal}(F_\infty/F)$  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  $\Gamma$  in the decomposition  $\mathbb{Z}_p^* = \mathbb{Z}/(p-1)\mathbb{Z} \times \Gamma$ .

Consider the image of such an  $\alpha$  in the Galois group  $G'$  by the map  $\widehat{E}_Q \rightarrow U_F^1 \rightarrow G \rightarrow G'$ . On the one hand it is trivial as  $\text{loc}_p(\alpha)$  is torsion. But on the other hand, as  $\text{loc}_p(N(\alpha)) = 1$ , it is also of the form  $(\text{Frob}_{q_1}^{a_1} \text{Frob}_{q_2}^{a_2})^m$  with  $\text{Frob}_{q_i}$  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 7.2 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*

- $\text{loc}_p(\alpha)$  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*

- $\text{loc}_p(\alpha) = 1$
- $v_t(\alpha) = 0$  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  $\alpha$  as in the first part of the lemma. By §2 we get that  $L_\alpha$  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 7.2,  $[L_\alpha \cap \mathcal{L}_\infty^- : \mathcal{F}_\infty] = m_Q$ .

Thus we only need to prove the lemma. We recall the fundamental exact sequence (2) from earlier:

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

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  $\text{Frob}_{q_1}^{a_1} \text{Frob}_{q_2}^{a_2}$  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  $F_\infty/F$ . 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  $\alpha'$  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  $(\text{Frob}_{q_1}^{a_1} \text{Frob}_{q_2}^{a_2})^{nm_Q}$  is trivial in  $G'$ , and thus gives rise to a well-defined element  $\beta$  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 (2). Furthermore  $(q_1^{np^m c_1} q_2^{np^m c_2})^{m_Q}$  gives rise to a well-defined element  $\beta'$  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  $\alpha'$  of  $\widehat{E}_Q/\widehat{E}_F$  independent of choice of  $m$ . Furthermore, the natural map  $\widehat{E}_Q/\widehat{E}_F \rightarrow U_F^1/\overline{E}_F^1\mu$  sends  $\alpha'$  to 1.

Choose  $\alpha'' \in \widehat{E}_Q$  which projects to  $\alpha'$ , and by choice maps to an element of  $\overline{E}_F^1\mu$  under the natural map  $\widehat{E}_Q \rightarrow U_F^1$ . Thus the image of  $\alpha''$  in  $F_p^*/\mu$  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  $\widehat{E}_F \rightarrow \overline{E}_F^1$ . We set  $\alpha = \alpha'' \cdot e^{-1}$ , and see that  $\text{loc}_p(\alpha)$  is torsion,  $\alpha \in \widehat{E}_Q$ , and  $(v_{q_i}(\alpha)) = (m_Q)$ , thus proving the lemma.  $\square$

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

**Corollary 7.4.** (i) *The exact sequence (6) of  $\Lambda$ -modules splits if and only if  $m_Q = 1$ .*

(ii) *For a tuple of primes  $Q = \{q_1, q_2\}$  inert in  $F_\infty/F$ ,  $M_Q$  trivial implies that the exact sequence (4) of  $\Lambda$ -modules splits.*

*Proof.* (i) The sequence (6) 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 7.3 in the proof above, under the assumption that  $M_Q$  is trivial we get an element  $\alpha$  of  $\widehat{E}_Q$  such that  $\text{loc}_p(\alpha) = 1$ , 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 (3), and thus a splitting of (4).  $\square$

*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 [5].

**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*

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

*is surjective.*

*Remark:* Iwasawa stated his criterion as: Leopoldt's conjecture, cf. Conjecture 1.1, is true if and only for every prime  $q$  prime to  $p$  of  $F$ , the image of inertia at the prime  $q$  in  $\text{Gal}(F_{p,q}/F)$ , 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  $F_\infty$  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  $\Gamma$  or  $\Lambda$ -modules:

$$(10) \quad 0 \rightarrow K_Q \rightarrow Y_{\infty, Q} \rightarrow Y_\infty \rightarrow 0$$

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 [3] using Kummer theory, which also shows that the exact sequence (10) splits up to isogeny.

**Lemma 8.2.** *Leopoldt's conjecture is true for  $F, p$  if and only if the exact sequence (10) remains exact on going modulo  $T$  for each choice of  $q$ .*

*Proof.* Note that the sequence (10) remains exact on going modulo  $T$  if and only if the image of an inertia group above  $q$  in  $\text{Gal}(F_{p,q}/F)$  is of order the  $p$ -part of  $N(q) - 1$ , namely  $e(q)$ . Then we are done by the equivalence of Theorem 8.1.  $\square$

It is interesting to note that in the odd case the sequence (6) 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 (10) does split up to isogeny, as shown by Greenberg 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. OUR CRITERION USING POITOU-TATE

The criteria for Leopoldt's conjecture contained in Cor. 6.5 and Prop. 6.6 above may also be derived from formulas of Greenberg and Wiles in Galois cohomology, which are consequences of the Poitou-Tate exact sequence. We apply these formulas to  $\mathbb{Q}_p$ -representations where they are also valid.

For a finite dimensional vector space  $V$  over  $\mathbb{Q}_p$  endowed with a continuous action of  $G_F$  that is everywhere almost unramified, and a set of Selmer conditions  $\mathcal{L} = \{\mathcal{L}_v\}$  for  $\mathcal{L}_v \subset H^1(F_v, V)$  with  $\mathcal{L}_v$  almost everywhere the unramified subgroup we have the formula

$$h_{\mathcal{L}}^1(F, V) - h_{\mathcal{L}^\perp}^1(F, V^*(1)) = h^0(F, V) - h^0(F, V^*(1)) + \sum_v (\dim_{\mathbb{Q}_p} \mathcal{L}_v - h^0(F_v, V)).$$

We apply this formula for  $V = \mathbb{Q}_p(1)$ , and with the Selmer conditions  $\mathcal{L}$  to be unramified everywhere, in particular trivial at places above  $p$ . The Leopoldt conjecture is equivalent to  $h_{\mathcal{L}^\perp}^1(F, \mathbb{Q}_p)$ , which is at least 1-dimensional, having dimension 1. Let  $\delta := h_{\mathcal{L}^\perp}^1(F, \mathbb{Q}_p) - 1$  the defect to Leopoldt conjecture. We easily get the criterion for Leopoldt conjecture contained in Cor. 6.5 by choosing  $Q = \{q_1, q_2\}$  so that  $h_{\mathcal{L}_Q}^1(F, \mathbb{Q}_p) = h_{\mathcal{L}^\perp}^1(F, \mathbb{Q}_p) - 2$  if  $\delta \geq 1$ , and by applying again the formula of Greenberg and Wiles replacing  $\mathcal{L}$  by  $\mathcal{L}_Q$ . Here  $\mathcal{L}_Q$  are the Selmer conditions that arise when we allow ramification at  $Q$ . We get that  $h_{\mathcal{L}}^1(F, \mathbb{Q}(1)) = h_{\mathcal{L}_Q}^1(F, \mathbb{Q}(1))$ , which contradicts the existence of a  $\mathbb{Z}_p$ -extension as in lemma 6.3. To see the criterion for the Leopoldt conjecture contained in Prop. 6.6 we relax the Selmer conditions by allowing ramification at  $p$ .

This method allows us to get a refinement of Prop. 6.6 as follows. Consider the Galois group  $M_{\infty, p}$  of the maximal odd, abelian  $p$ -extension of  $\mathcal{F}_\infty$  which is unramified outside  $p$ . Then we have an exact sequence

$$0 \rightarrow T_p \otimes \mathbb{Q}_p \rightarrow M_{\infty, p} \otimes \mathbb{Q}_p \rightarrow X_\infty^- \otimes \mathbb{Q}_p \rightarrow 0.$$

Here  $T_p$  is the group generated by inertia at primes above  $p$ . Consider any odd character  $\psi : \text{Gal}(\mathcal{F}_\infty/F) \rightarrow \overline{\mathbb{Q}_p}^*$ , and assume that the Selmer group

$H_{\mathcal{L}}^1(G_F, \chi\psi^{-1}) = 0$  with the Selmer conditions being that of unramified everywhere. The vanishing would follow from Greenberg's conjecture that the Sylow  $p$ -subgroup of the class group of  $F_{\infty}$  is finite as  $\chi\psi^{-1}$  is an even character. (For the case  $\psi = \chi$  which corresponds to Prop. 6.6 this just follows from finiteness of class numbers of number fields.) The character  $\psi$  gives rise to a prime ideal  $P_{\psi}$  of height one of  $\Lambda_{\mathcal{O}}$  where  $\Lambda \otimes_{\mathbb{Z}_p} \mathcal{O}$  for the ring of integers  $\mathcal{O}$  of a  $p$ -adic field that contains values of  $\psi$ . Then again using the Greenberg-Wiles formula one sees that the localisation of the above exact sequence (tensorised with  $\Lambda_{\mathcal{O}}$ ) at  $P_{\psi}$  is split as  $(\Lambda_{\mathcal{O}})_{(P_{\psi})}$ -modules if and only if  $(X_{\infty}^-)_{(P_{\psi})} = 0$ . Thus every eigenspace of  $X_{\infty}^- \otimes \mathbb{Q}_p$ , assuming Greenberg's conjecture, intertwines with ramification at  $p$ .

## 10. 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 [7] and [2], 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. [4])

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

with  $\chi$  running through the irreducible  $p$ -adic representations of  $\text{Gal}(F/\mathbb{Q})$ . Note that for  $\chi$  a non-trivial representation,  $L_{F,p}(s, \chi)$  is entire by the  $p$ -adic form of the Artin conjecture which is proved in [4] to follow from the main conjecture. The factor for  $\chi$  the trivial representation has a simple pole at  $s = 1$ , and for other non-trivial abelian characters  $\chi$ , the corresponding factor does not vanish at  $s = 1$ , by the known case of the Leopoldt conjecture for abelian extensions of  $\mathbb{Q}$  (cf. [1]). Thus if the Leopoldt conjecture is false for  $F, p$ , for a representation  $\chi$  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. This could well be known to the experts. 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-semisimplicity of Leopoldt zeros"). It will be nice to remove the assumption that  $F/\mathbb{Q}$  is Galois; this will require other methods.

**Proposition 10.1.** *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  $L = \text{Gal}(N/F) : L$  is a free  $\mathbb{Z}_p$ -module of rank 2. The inclusion  $F_{\infty} \subset N$  gives a surjective morphism  $L \rightarrow \Gamma$ . 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 through

the character  $\eta$  giving the action of  $H_1$  on  $\mathbb{Q}_p \otimes (L/\Gamma)$ . Hence the action of  $H_1$  on  $L$  factors through  $\eta$ . Let  $H$  be the kernel of  $\eta$  and  $F_\eta$  the field corresponding to  $H$ . The next lemma implies the existence of an extension  $N'$  of  $F_\eta$  of Galois group a free  $\mathbb{Z}_p$ -module of rank 2 such that  $N = N'F$ . This is impossible as  $F_\eta$  is abelian over  $\mathbb{Q}$  and we know Leopoldt conjecture for  $F_\eta$  and  $p$ .

**Lemma 10.2.** *Let  $1 \rightarrow L \rightarrow G \rightarrow H \rightarrow 1$  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  $G \rightarrow L'$ .*

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  $1 \rightarrow L' \rightarrow G' \rightarrow H \rightarrow 1$  has a trivialisation  $G' \rightarrow L'$ . If we compose it with the morphism  $G \rightarrow G'$  we get a morphism  $G \rightarrow L'$  that coincide on  $L$  with the inclusion  $L \hookrightarrow L'$ .

Conversely, if we have a surjection  $G \rightarrow L'$ , its restriction to  $L$  has a finite index image as  $H$  is finite. This implies that this restriction is injective. The morphism  $G \rightarrow L'$  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  $1 \rightarrow G'' \rightarrow G \rightarrow H/H' \rightarrow 1$  to get a surjective morphism of  $G$  in  $(\mathbb{Z}_p)^d$ . If  $G''$  has torsion  $T$ ,  $T$  is cyclic of order  $p$  and  $G \rightarrow H$  induces an isomorphism of  $T$  to  $H'$ . We apply the induction hypothesis to the exact sequence  $1 \rightarrow L \rightarrow G/T \rightarrow H/H' \rightarrow 1$ . 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  $H^2(H, L') \rightarrow H^2(H_p, L')$  is injective. This follows from the injectivity of the maps  $H^2(H, L'/p^n L') \rightarrow H^2(H_p, L'/p^n L')$  and Mittag-Leffler. We see that  $o'$  is trivial and this proves the lemma.  $\square$

## REFERENCES

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

- [2] Pierre Colmez. Résidu en  $s=1$  des fonctions zeta  $p$ -adiques. *Invent. Math.* 91 (1988), no. 2, 371389.
- [3] Ralph Greenberg. On  $p$ -adic  $L$ -functions and Cyclotomic fields II. *Nagoya Math. J.*, 67, 1977, p. 139-158.
- [4] Ralph Greenberg. On  $p$ -adic Artin  $L$ -functions. *Nagoya Math. J.* 89 (1983), 77–87.
- [5] Kenkichi Iwasawa. *Collected Papers I and II*. Springer-Verlag.
- [6] J. Neukirch, A. Schmidt, K. Wingberg. *Cohomology of number fields*. Springer-Verlag.
- [7] 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.
- [8] Larry Washington. *Introduction to Cyclotomic Fields* (2nd edition). Springer-Verlag.
- [9] 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