Jean-Pierre Wintenberger

Extensions of Iwasawa modules (2)

jw with Shekhar Khare

The aim of the talk is show how Leopoldt conjecture is linked with properties of exact sequences of Iwasawa modules arising from ramification at auxiliary primes. The hope is to be able to use modular technics to study these properties.

We restrict to the case of a totally real F. Let $p > 2$ be a prime. Let $\mathcal{F}_\infty = F(\mu_{p^\infty})$ be the cyclotomic extension. The cyclotomic character χ_p identifies $\mathrm{Gal}(\mathcal{F}_\infty/F)$ to an open subgroup of $(\mathbb{Z}_p)^*$, hence the quotient by its torsion is isomorphic to $\mathbb{Z}_p$. To this quotient, corresponds the cyclotomic $\mathbb{Z}_p$-extension we call F_∞.

A formulation of Leopoldt conjecture (LC) is that F_∞ is the only $\mathbb{Z}_p$-extension of F.

Let E_F be the group of units of F. Let U_F be the units in the p-adic completion of O_F, so $U_F = \prod_\wp U_\wp$ where the $\wp$ are the primes of F over p. The group U_F is the product the multiplicative groups $\prod_\wp (k_\wp)^*$ of the residue fileds by the group U_F^1 of units that reduces to 1 in $\prod_\wp k_\wp$. U_F^1 is a $\mathbb{Z}_p$-module of rank r where $r = [F : \mathbb{Q}]$. One has an injection $E_F \hookrightarrow U_F$. Let $\bar{E}_F$ be the closure of the image of E_F in U_F (with its p-adic or congruence topology). Let L_∞ be the maximal abelian p-extension of F that is only ramified at p. Class field theory gives an exact sequence :

$$1 \to U_F/\bar{E}_F \to \mathrm{Gal}(L_\infty/F) \to \mathrm{Cl}(F) \to 1.$$

As a $\mathbb{Z}_p$-extension is unramified outside p, it follows that LC is equivalent to the fact that the $\mathbb{Z}_p$ rank of $\bar{E}_F$ is $r - 1$, *i.e.* the rank of E_F. It is equivalent to the fact that the topology on E_F induced by the topology of U_F is the same as the p-adic topology. On can express this by the fact that a p-adic regulator made from E_F and the p-adic logarithms is non zero. By the p-adic formula of Colmez for the residue of the p-adic L-function $\zeta_{F,p}(s)$ at $s = 1$, it is equivalent to the fact that $\zeta_p(s)$ has a pole at $s = 1$.

Remark LC is known for abelian extensions of $\mathbb{Q}$ and imaginary quadratic fields by Brumer using independence of logarithms technics and Galois properties of units.

One has another formulation by Iwasawa. Let q be a primes of F prime to p. If L is a finite abelian p-extension of F, the inertia subroup $I_q(L/F)$ of $\mathrm{Gal}(L/F)$ is a quotient of $(k_q)^*$ killed by a power of p, hence it is cyclic of order divisible by the p-part $e(q)$ of $N(q) - 1$. Iwasawa call L fully ramified if $I_q(L/F)$ has order $e(q)$. Iwasawa proved that the Leopoldt conjecture is true for F and p if and only if , for each q prime of F prime to p, F

has a finite abelian p-extension L_q which is unramified outside pq and fully ramified at q.

Remark. It is easy to see that we have sometimes to ramifiy at p to get fullness of q inertia.

One can see the Iwasawa criteria as a property of an exact sequence of Iwasawa modules.

As if LC is true for $F' \supset F$, then it is true for F. We suppose that $\mathcal{F} = F(\mu_p)$ is of degree 2 over F. $+$ and $-$ are relative to the action of complex conjugation $c \in \mathrm{Gal}(\mathcal{F}/F)$.

Let Q be a finite set of primes of F prime to p. We suppose that for $q \in Q$, p divides $N(q) - 1$, so that q splits if $\mathcal{F}$.

Let M_∞ be the maximal abelian p-extension of F_∞ that is unramified outside p. Let $M_{\infty,Q}$ be the maximal abelian p-extension of F_∞ that is unramified outside p and Q. We have an action of $\Lambda = \mathbb{Z}_p[[T]]$ with $T = \gamma - 1$, γ a generator of $\Gamma = \mathrm{Gal}(F_\infty/F)$. We write $\mathrm{Gal}(M_\infty/F_\infty) = Y_\infty$ and $\mathrm{Gal}(M_{\infty,Q}/F_\infty) = Y_{\infty,Q}$. Iwasawa proved that Y_∞ and $Y_{\infty,Q}$ are finitely generated torsion Λ-modules.

We say that a sequence of torsion Λ-modules is split up to isogeny if it splits after $\otimes\mathbb{Q}_p$.

Proposition 0.1. *(Greenberg) We have an exact sequence (1) :*

$$(0) \to \prod_j I_{q'_j}(N_\infty/F_\infty) \to Y_{\infty,Q} \to Y_\infty \to (0)$$

where j runs in the (finite) set of primes of F_∞ that are above the q_i. The inertia groups $I_{q'_j}(N_\infty/F_\infty)$ are free $\mathbb{Z}_p$-modules of rank 1.The product is a direct product. This sequence splits up to isogeny.

The proposition follows from Kummer theory. One considers a Kummer extension $N_\infty = F(\mu_{p^\infty}, \alpha_j^{1/p^\infty})$, where the $\alpha_j \in \mathcal{F}_\infty$, such that, for each j, the ideal (α_j) is a power of $q'_j(q_j")^{-1}$. q'_j and $(q_j")^{-1}$ are the primes over q_j. The α_j are chosen compatibly with the action of $\mathrm{Gal}(\mathcal{F}_\infty/F)$. It is unramified outside the primes above Q and p, and the direct product of the $I_j(N_\infty/F_\infty)$ injects in $\mathrm{Gal}(N_\infty/F_\infty)$ with open image. Each $I_j(N_\infty/F_\infty)$ is isomorphic to $\mathbb{Z}_p$. We have $N_\infty\ M_\infty = M_{\infty,Q}$ and $N_\infty \cap\ M_\infty$ finite over F_∞.

The following proposition follows easily from Iwasawa criteria.

Proposition 0.2. *LC equivalent to the fact that these exact sequences, for all Q, remains exact modulo T.*

To our knowledge, there is no modular construction of Y_∞. We search an analog criteria which is on $\mathcal{X}_\infty^-$, which have a modular construction by Wiles. Recall that $\mathcal{L}_\infty$ is the maximal abelian p-extension of $\mathcal{F}_\infty$ that is unramified everywhere, and $\mathcal{X}_\infty = \mathrm{Gal}(\mathcal{L}_\infty/\mathcal{F}_\infty)$. Iwasawa gives an isomorphism of $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Lambda$ modules based on Kummer pairing :

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

As above, Q be a finite set of primes q of F that are prime to p and such that p divides $N(q)-1$. We suppose that each prime q is such that Frob_q generates $\Gamma = \mathrm{Gal}(F_\infty/F)$. We consider the maximal abelian p-extension of $\mathcal{F}_\infty$ which is unramified outside the primes above the primes in Q and call it $\mathcal{L}_{\infty,Q}$ and we call $\mathcal{X}_{\infty,Q}$ its Galois group over $\mathcal{F}_\infty$. We have the following exact sequence (2) :

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

where m is the cardinal of Q. This follows from the exact sequences of class field theory, where Q_n is the product of the primes of $\mathcal{F}_n$ above Q :

$$(0) \to (O_{\mathcal{F}_n}/Q_n)^*/E_{\mathcal{F}_n} \to \mathrm{Cl}_{\mathcal{F}_n,Q_n} \to \mathrm{Cl}_{\mathcal{F}_n} \to (0).$$

The $m-1$ comes from $E^-_{\mathcal{F}_n} \simeq \mu_{p^{(n+t)}}$ where μ_{p^t} are the p^* roots of unity in $\mathcal{F}$ ($\mathcal{F}_n = \mathcal{F}(\mu_{p^{n+t}})$).

Proposition 0.3. *The exact sequence (2) splits up to isogeny if and only if Leopoldt conjecture is true.*

We call the conjecture that (2) splits up to isogeny the splitting conjecture. In fact, for LC, it suffices to verify splitting conjecture for $m = 2$.

Before we sketch a proof of the proposition, we give an equivalent formulation :

Lemma 0.4. *Splitting conjecture for $m = 2$ is equivalent to saying that there is a $\mathbb{Z}_p$-extension $\mathcal{N}_Q$ of $\mathcal{F}_\infty$ that is Galois over F, ramified at the primes of $\mathcal{F}_\infty$ above q_1, q_2 and unramified everywhere else, and on which complex conjugation acts by -1. Note that Γ acts on $\mathrm{Gal}(\mathcal{N}_Q/\mathcal{F}_\infty)$ by the p-adic cyclotomic character as the q_i are inert in F_∞/F.*

For the lemma, we choose $X \subset \mathcal{X}^-_{\infty,Q}$ a Λ-submodule with $X \to \mathcal{X}^-_\infty$ having kernel and cokernel killed by a power of p. We define $\mathcal{N}_\infty$ the subfield of $\mathcal{L}_{\infty,Q}$ that is Galois over $\mathcal{F}_\infty$ and such that its Galois group over $\mathcal{F}_\infty$ is the quotient of $\mathcal{X}_{\infty,Q}/X$ by its p^*-torsion.

If Leopoldt is true then the splitting conjecture is true. Leopoldt conjecture is equivalent to the fact that the characteristic polynomial of $Y_\infty \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ has not 0 as a zero. By Iwasawa isomorphism it is equivalent that $\mathcal{X}_\infty$ has characteristic polynomial without $u-1$ as zero (corresponding to the action of Λ by the cyclotomic character). But then (2) splits up to isogeny as the characteristic polynomial of $\mathbb{Q}_p(1)$ and $\mathcal{X}^-_\infty \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ are prime.

Let us give another proof.

Let $\hat{F^*} := \mathrm{limproj}_n F^*/(F^*)^{p^n}$ be the p-adic completion of the multiplicative group of F. Kummer's theory gives an exact sequence :

$$(1) \to \mu_{p^t} \to \hat{F^*} \to \mathrm{Hom}(G_{\mathcal{F}_\infty}, \mathbb{Z}_p(1))^{\mathrm{Gal}(\mathcal{F}_\infty/F)}$$

where the cokernel of the right arrow is killed by p^t. For q prime of F, we let v_q be the valuation normalized by $v_q(F^*) = \mathbb{Z}$. Let $\hat{F^*_p} = \prod_\wp \hat{F^*_\wp}$ where the $\wp$ are the prime of F above p. We have a localization map : $\mathrm{loc}_p : \hat{F^*} \to \hat{F^*_p}$.

For $\hat{\alpha} \in \hat{F}^*$ non torsion, the $\mathbb{Z}_p$-extension $F(\mu_{p^\infty}, \hat{\alpha}^{1/p^\infty})$ of $\mathcal{F}_\infty$ is unramified at q prime to p if and only if $v_q(\hat{\alpha}) \neq 0$ and at primes over p if and only if $\mathrm{loc}_p(\hat{\alpha}) = 0$ is torsion.

Let $\alpha_i \in F^*$, for $i = 1, 2$, be such that $(\alpha_i) = q_i^{a_i}$, $a_i \in \mathbb{N}_{>0}$ and such that α_i reduces to 1 in the residue fields $k_\wp$ for $\wp$ prime of F above p. If LC is true, the rank of $\mathrm{rank}_{\mathbb{Z}_p}(U_F^1/\bar{E_F^1}) = 1$ and there are $b_i \in \mathbb{Z}_p$, $b_i \neq 0$, such that $\mathrm{loc}_p(\hat{\alpha_1}^{b_1}\hat{\alpha_2}^{b_2}) \in \overline{E_F^1}$. It implies that there exist $\hat{\epsilon} \in \mathbb{Z}_p \otimes E_F^1$ such that $\mathrm{loc}_p(\hat{\alpha_1}^{b_1}\hat{\alpha_2}^{b_2}\hat{\epsilon}) = 1$. $\mathcal{N}_Q = F(\mu_{p^\infty}, \hat{\alpha}^{1/p^\infty})$ with $\hat{\alpha} = \hat{\alpha_1}^{b_1}\hat{\alpha_2}^{b_2}\hat{\epsilon}$.

If LC is not true, $\mathrm{rank}_{\mathbb{Z}_p}(U_F^1/\bar{E_F^1}) \geq 2$. We have prove that for a choice of $Q = \{q_1, q_2\}$, the sequence (2) does not split up to isogeny.

By the Cebotarev density theorem, we can find primes of F q_1, q_2, not above p, and α_1 α_2 in O_F such that

– α_i generate some power of q_i ;

– α_i reduce to 1 in the residue fields $k_\wp$, for $\wp$ prime of F above p ;

– q_i are inert in F_∞ ;

– p divides $N(q_i) - 1$;

– the images of the α_i in $U_F^1/\overline{E_F^1}$ are independent over $\mathbb{Z}_p$.

Let $Q = \{q_1, q_2\}$. If the extension $\mathcal{N}_Q$ were to exist, it would be of the type $F(\mu_{p^\infty}, \hat{\alpha}^{1/p^\infty})$ with $\hat{\alpha}$ of the form $\alpha_1{}^{b_1}\alpha_2{}^{b_2}\hat{\epsilon}$ with $\mathrm{loc}_p(\hat{\alpha})$ torsion and b_i and $b_i \neq 0$. It contradicts that the α_i in $U_F^1/\overline{E_F^1}$ are independent over $\mathbb{Z}_p$.

Motivation. Can we construct $\mathcal{N}_Q$ by modular methods, using Λ-adic modular forms new of level q_1q_2 ?

Let $u = \chi_p(\gamma)$. It seems likely that one can construct $\mathcal{L}_Q$ by modular methods. Let $\zeta_p(s)$ the p-adic zeta function for F. We have $\zeta_p(s) = W(u^s - 1)/(u^{1-s} - 1)$ with $W(T) \in \mathbb{Z}_p[[T]]$. Let a be the order of $u - 1$ as a zero of W ($a = 0$ if and only if $\zeta_p(s)$ has a pole of order 1 at 1 *i.e.* LC is true). Main conjecture, proved by Wiles, implies that the multiplicity of $u - 1$ in the characteristic polynomial of $\mathcal{X}_\infty^-$ is a. It seems that one can find a Λ-adic Eisentstein series of level q_1q_2 and whose constant terms are divisible by $(T - u + 1)^{a+1}$. The method of Ribet and Wiles should give a $(\mathbb{Z}_p)^{a+1}$ extension of $\mathcal{F}_\infty$ which is Galois over F, unramified outside q_1 q_2, c acting by -1 , characteristic polynomial of γ equal to $(T - u + 1)^{a+1}$. This extension is $\mathcal{L}_{\infty,Q}$, in particular it is ramified at q_1 and q_2 (it is ramified at q_1 and q_2 by main conjecture).

Nevertheless, it seems not clear how to prove that the method of Ribet Wiles applied to new forms of level q_1q_2 give $\mathbb{Z}_p$-extensions that are ramified at q_1 and q_2.

We have another exact sequence which gives an analog criteria for ramified at p extensions.

Consider $\mathcal{X}_{\infty,p}^-$, the Galois group of the maximal odd abelian p-extension N'_∞ of $\mathcal{F}_\infty$ that is unramified outside p, and on which $\mathrm{Gal}(\mathcal{F}_\infty/F)$ acts on the subgroup I_p generated by the inertia groups at places above p via the p-adic

cyclotomic character χ_p. Then we have an exact sequence of Λ-modules

$$0 \to I_p \to \mathcal{X}_{\infty,p}^- \to \mathcal{X}_\infty^- \to 0.$$

I_p is isomorphic to $\mathbb{Z}_p(1)^{[F:\mathbb{Q}]+s-1}$ as Λ-module, where s is the number of primes of F above p. It is not difficult to see that LC is equivalent to the splitting up to isogeny of this exact sequence.