Jean-Pierre Wintenberger

Extensions of Iwasawa modules

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 techniques 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 and F_∞ the cyclotomic $\mathbb{Z}_p$-extension.

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). Leopoldt conjecture states that the rank of $\bar{E}_F$ is $[F : \mathbb{Q}] - 1$.

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 techniques and Galois structure of units.

One has another formulation by Iwasawa. Let q be a prime 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.

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 write $\mathrm{Gal}(M_\infty/F_\infty) = Y_\infty$ and $\mathrm{Gal}(M_{\infty,Q}/F_\infty) = Y_{\infty,Q}$. We have an action of $\Lambda = \mathbb{Z}_p[[T]]$ with $T = \gamma - 1$, γ a generator of $\Gamma = \mathrm{Gal}(F_\infty/F)$ on Y_∞ and $Y_{\infty,Q}$. 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) :*

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

where j runs in the (finite) set of primes q'_j of F_∞ that are above the q_i. The inertia groups $I_{q'_j}$ 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. 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 M_∞. 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, let Q be a finite set of primes q of F that are prime to p but we do not impose 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 L_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 $\mathrm{Gal}(L_Q/\mathcal{F}_\infty)$ by the p-adic cyclotomic character as the q_i are inert in F_∞/F and $L_Q/\mathcal{F}_\infty$ is ramified at the primes over q_1 and q_2.*

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 L_Q 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 LC is true, the extension L_Q like above is unique.

Let us prove the proposition.

If Leopoldt is true then the splitting conjecture is true. Let $\gamma \in \Gamma$ be a generator and $u = \chi_p(\gamma)$. Leopoldt conjecture is equivalent to the fact that the characteristic polynomial of γ acting on $Y_\infty \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ does not vanish at 0. By Iwasawa isomorphism it is equivalent that $\mathcal{X}_\infty$ has characteristic polynomiial not vanishing at $u - 1$. 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 based on Kummer's theory.

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

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

where the cokernel is killed by a power of p. 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 $\mathrm{loc}_p(\hat{\alpha})$ 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 $\mathrm{loc}_p(\hat{\alpha_1}^{b_1}\hat{\alpha_2}^{b_2}\hat{\epsilon}) = 1$. We define $L_Q = F(\mu_{p^\infty}, \hat{\alpha}^{1/p^\infty})$ 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 to prove that for a choice of $Q = \{q_1, q_2\}$, the sequence (2) does not split up to isogeny.

It is not dificult to see that there exists a such that for every prime q of F prime to p, q^{p^a} has a generator α which reduces to 1 in the residue fields $k_\wp$, for $\wp$

prime of F above p. Then $\mathrm{Frob}_q^{p^a}$ is a well defined element of $U_F^1/\overline{E_F^1}$. By Cebotarev density theorem, it is not difficult to find primes q_1 and q_2 of F, q_1, q_2, not above p, such that

– q_i are inert in F_∞ ;

– $\mathrm{Frob}_{q_i}^{p^a}$ are independent over $\mathbb{Z}_p$.

The second condition is possible as LC is supposed to be false.

Let $Q = \{q_1, q_2\}$. If the extension L_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, α_i generates $\mathrm{Frob}_{q_i}^{p^a}$ and $b_i \neq 0$. It contradicts that the $\mathrm{Frob}_{q_i}^{p^a}$ in $U_F^1/\overline{E_F^1}$ are independent over $\mathbb{Z}_p$.

Motivation. Can we construct L_Q by modular methods, using Λ-adic modular forms of level q_1q_2 ?

Let $u = \chi_p(\gamma)$. 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 we have a critical Eisenstein series $E_{q_1}(z) = E(z) - E(q_1 z)$ which is congruent to a cuspidal eigenform modulo $(T-u+1)^a$. The method of Ribet-Wiles should give a $\mathbb{Z}_p^a$-extension of $\mathcal{F}_\infty$ which is unramified outside q_1 and is Kummer (stable by

γ, odd, and the characteristic polynomial of it is $(T-u+1)^a)$. By class field theory, as we saw, it is unramified at q_1, hence is the $\mathbb{Z}_p^a$ extension which correspond to the Kummer characteristic subspace of $\mathcal{X}_\infty^-$.

Let us apply Ribet-Wiles method for forms for $\Gamma_0(q_1q_2)$. The Eisenstein series $E_{q_1}(z) - E_{q_1}(q_2z)$ should be congruent to a cuspidal eigenform modulo $(T-u+1)^{a+1}$. The method of Ribet-Wiles furnish a Kummer $(\mathbb{Z}_p)^{a+1}$ extension which is unramified outside q_1 and q_2. By main conjecture, It has to be ramifed at q_1 and q_2. It is the extension of $\mathcal{F}_\infty$ that has Galois group $\mathcal{X}_{\infty,Q}^-$ modulo torsion.

Hence there are forms for $\Gamma_0(q_1q_2)$, new at q_2 which are Eisenstein and are responsible of the ramification at q_1 and q_2. Can they allow us to prove the existence of the searched $\mathbb{Z}_p$ extension ?