# Machinerie générale des systèmes d'Euler I

références R. Rubin ("Euler Systems" Ann. Math. Studies 147, appendice de Lang "Cycl. Fields I, II") A1 R2
PR. Perrin-Riou ("Systèmes d'Euler p-adiques et théorie d'Iwasawa", An. institut Fourier 48/5) (1998)
W. Washington ("Introduction to Cycl. Fields")

~84, Mazur et Wiles démontrent la conjecture principale d'Iwasawa en utilisant des congruences entre séries d'Eisenstein et forme paraboliques, généralisant les travaux antérieurs de Ribet sur la réciproque d'un théorème de Herbrand.
~88, Thaine introduit une méthode basée sur les unités cyclotomiques pour étudier le gr. des classes de $\mathbb{Q}(\mu_m)^+$. ~90 (?) En élaborant ses idées, Kolyvagin réussit à déterminer les p-ordres des composantes galoisiennes de $Cl(\mathbb{Q}(\mu_p))$.
Un outil important qu'il introduit est la construction de "classes dérivées" des unités cyclotomiques, produisant des idéaux principaux "explicites".
Peu après Rubin généralise la méth. de Kolyvagin et donne une nouvelle preuve de la conjecture principale (cf. R2). Ces méthodes ont ensuite été axiomatisées et généralisées indépendamment par Rubin, Perrin-Riou et Kato (R1, PR) (aussi Mazur - Rubin)
Ces généralisations seront traitées dans l'exposé II. Ici, on va exposer les preuves de Kolyvagin et Rubin, dans le cas cyclotomique donc. Ces preuves sont le guide nécessaire à la compréhension du cas général.

Théorème I (Mazur-Wiles, Kolyvagin)

$$\#\left(Cl(\mathbb{Q}(\mu_p)^+)[p^\infty]\right)_\chi = \#\left(\frac{(\mathbb{Z}(\mu_p)^+)^\times}{\text{unités cyclotom.}}\otimes\mathbb{Z}_p\right)_\chi$$

$(\chi : Gal(\mathbb{Q}(\mu_p)^+/\mathbb{Q}) \to \mathbb{Z}_p^\times)$

Théorème II (Mazur-Wiles, Rubin)

$\chi(-1)=-1$, $\chi \neq \omega$, $$(L_{p,\chi}) = \mathrm{char}\left(\varprojlim_m Cl(\mathbb{Q}(\mu_{p^m}))[p^\infty]\right)_\chi$$

de torsion sur $\Lambda$ (Iwasawa)

une certaine fonction $\zeta_p$-adique

# I) Le système d'Euler cyclotomique

1. $m \geq 1$, $\zeta_m = e^{\frac{2i\pi}{m}}$, on a les relations

Définition

**SE 1** $\ell$ premier

$$N_{\mathbb{Q}(\mu_{\ell m})/\mathbb{Q}(\mu_m)}(1-\zeta_{m\ell}) = \begin{cases} \ell & \text{si } m=1 \\ 1-\zeta_m & \text{si } \ell \mid m \\ (1-\zeta_m)^{1-F_\ell^{-1}} & \text{si } \ell \nmid m,\ m \neq 1 \end{cases}$$

(voir appendice)

**SE 2** $\ell$ premier, $\ell \nmid m$, $1-\zeta_{m\ell} \equiv 1-\zeta_m^{\ell^{-1}}$ dans $\overline{\mathbb{Q}}_\ell$

Les $(1-\zeta_m)_{m\geq 2}$ forment un "système d'Euler". Si $m$ n'est pas premier, on voit donc que $1-\zeta_m$ est une unité de $\mathbb{Q}(\mu_m)$. Pour chaque premier $p$, on peut en déduire un système d'Euler $p$-adique pour $\mathbb{Z}_p(1)$ grâce au morphisme de Kummer

$$K^\times \longrightarrow H^1(K, \mathbb{Z}_p(1))$$

## II. les unités cyclotomiques

$p$ premier, on peut exhiber un sous-groupe explicite des unités de $\mathbb{Q}(\mu_{p^n})$, grâce à $1-\zeta_{p^n}$. On définit ce groupe $\mathcal{E}_n$ (unités cyclotomiques) par ($G := Gal(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})$)

$$1 \longrightarrow \mathcal{E}_n \longrightarrow \pm\mu_{p^n}\cdot\mathbb{Z}[G]\cdot(1-\zeta_{p^n}) \xrightarrow{v_{1-\zeta_{p^n}}} \mathbb{Z} \to 1$$

On a bien $\mathcal{E}_n \subset \mathbb{Z}(\mu_{p^n})^\times$ d'après le 1. On a $\mathbb{Z}(\mu_{p^n})^\times = \mu_{p^n}\cdot\mathbb{Z}(\mu_{p^n})^{+,\times}$ (CM)

On pose $\mathcal{E}_n^+ = \mathcal{E}_n \cap \mathbb{Q}(\mu_{p^n})^+$.

proposition:

$$\# \mathcal{C}\ell(\mathbb{Q}(\mu_{p^n})^+) = [\mathbb{Z}(\mu_{p^n})^{+,\times}, \mathcal{E}_n^+]$$, en particulier

$\mathcal{E}_n$ est d'indice fini dans $\mathbb{Z}(\mu_{p^n})^\times$.

preuve: (esquisse) . Des générateurs explicites de $\mathcal{E}_n^+$ sont les $\pm\frac{\sin(\pi k/p^n)}{\sin(\pi/p^n)}$, $1<k<\frac{p^n}{2}$

cf. W 8.2 . Leur régulateur est explicite et vaut $\pm\prod_{\substack{\chi\neq 1\\ \text{pair}}}(-\frac{1}{2}\tau(\chi)L(1,\chi^{-1})) \neq 0$ par Dirichlet

. Formule du nb classes pour $\mathbb{Q}(\mu_{p^n})^+ \xRightarrow{} " = hR$ ∎

Pb. $X = \mathbb{Z}(\mu_{p^n})^{+,\times}/\mathcal{E}_n^+$ comme $G$-module? Par exemple décrire les $\chi$-composantes de $X\otimes\mathbb{Z}_p$ sous l'action de $\Delta = (\mathbb{Z}/p\mathbb{Z})^\times_{\pm 1}$. Thm 1 (et 2) $\Rightarrow \exists$ formule analogue à prop. dans ce cas. Elles ne découlent pas de la formule du nb de classes.

<u>Remarques</u> i) • "Conjecture" de Vandiver $p \nmid \# Cl(\mathbb{Q}(\mu_{p^n})^+)$

ii) • $p \neq 2$, $\chi \neq 1$ car. de $\Delta$, $\left(\mathcal{E}_m^+ \otimes \mathbb{Z}_p\right)_\chi = \mathbb{Z}_p[G].e_\chi((1-\zeta_{p^n})(1-\zeta_{p^n}^{-1}))$.

c'est clair avec la suite exacte définissant $\mathcal{E}_m$.

iii) • $K/\mathbb{Q}$ corps de nombres totalement réel Galois de groupe $G$, $\mathcal{O}_K^\times \otimes \mathbb{Q} \simeq \mathbb{Q}[G]_0$ $(\Sigma a_g = 0)$
d'après le théorème de Dirichlet.

## II) <u>Classes dérivées de Kolyvagin</u> (d'après Kolyvagin)

Dans cette partie $F := \mathbb{Q}(\mu_{p^n})^+$ fixé. Pour $m \geq 1$ premier à $p$, on pose

$$c_m := N_{\mathbb{Q}(\mu_{mp^n})/F(\mu_m)}(1-\zeta_{mp^n}) = (1-\zeta_{mp^n})(1-\zeta_{mp^n}^c), \quad c \in \hat{\mathbb{Z}}^\times, \quad c = \begin{cases} -1 & \text{ds } \mathbb{Z}_p^* \\ +1 & \text{ds } \mathbb{Z}_{p'}^* \end{cases}$$

légère modification du système cyclotomique. Il satisfait encore SE1 et 2, et
$c_1 = (1-\zeta_{p^n})(1-\zeta_{p^n}^{-1})$. Pour des $m$ ss fact. carré bien choisis, on va construire, à la suite de Kolyvagin, et à l'aide de $c_m$, un $\kappa_m \in F^\times$ dont on va contrôler le diviseur. Cette partie n'est pas du tout $p$-adique, plutôt $\ell_1 \ell_2 \cdots$ adique...

① <u>Notations</u> $\mathcal{S} = \{$entiers sans facteur carré, divisibles que par des $\ell \equiv \pm 1 \ (p^n)\}$
i.e. t.déc. ds $F$

$r \in \mathcal{S}$, $G_r := Gal(F(\mu_r)/F) \overset{can}{=} \prod_{\substack{\ell | r \\ \text{premier}}} G_\ell$, et $G_\ell \xrightarrow[can]{\sim} Gal(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ cyclique d'ordre $\ell-1$

on fixe $\sigma_\ell$ générateur de $G_\ell$, et pose $D_\ell := \sum_{i=1}^{\ell-1} i\,\sigma_\ell^i \in \mathbb{Z}[G_\ell]$
ainsi que $N_r = \sum_{\sigma \in G_r} \sigma$ (norme). $D_\ell$ est l'opérateur de "dérivation de Kolyvagin".
Il n'est pas canonique, mais $\mathbb{Z}.D_\ell$ l'est dans $\mathbb{Z}/(\ell-1)\mathbb{Z}[G_\ell]$. Cette image engendre en fait la partie $G_\ell$-invariante de $\mathbb{Z}/(\ell-1)\mathbb{Z}[G_\ell]/(N_\ell)$.

On a $\boxed{(\sigma_\ell - 1) D_\ell = (\ell-1) - N_\ell}$ relation essentielle concernant $D_\ell$, notée $*$ ensuite.

on pose $D_r = \prod_{\substack{\ell | r \\ \text{premier}}} D_\ell$. On a aussi $N_r = \prod_{\substack{\ell | r \\ \text{premier}}} N_\ell$

## ② Construction des classes dérivées de Kolyvagin (d'après Kolyvagin ...)

Fixons $M$ une puissance de $p$ et $S_M = \{ n \in S$ divisibles que par des $\ell \equiv 1\ (M) \}$
$p \neq 2$

Observation si $n \in S_M$, alors $D_n c_n \in \left( F(\mu_n)^\times \otimes \mathbb{Z}/M\mathbb{Z} \right)^{G_n}$

En effet $(\sigma_\ell - 1) D_n c_n = (\ell - 1 - N_\ell) D_{\frac{n}{\ell}} c_n = \left(D_{\frac{n}{\ell}} c_n\right)^{\ell - 1} (F_{r_\ell}^{-1} - 1) D_{\frac{n}{\ell}} c_{\frac{n}{\ell}}$

$$(-N_\ell) c_n = (F_{r_\ell}^{-1} - 1) c_{\frac{n}{\ell}}$$

par récurrence sur $n$, $(F_{r_\ell}^{-1} - 1) D_{\frac{n}{\ell}} c_{\frac{n}{\ell}} \in \left( F(\mu_n)^\times \right)^M$ et on conclut car $\{\sigma_\ell, \ell | n\}$ engendrent $G_n$ □

Mais comme $\mu_M \cap F(\mu_n) = \mu_M \cap F = 1$, car $F$ est réel et $F(\mu_n)/F$ non ram. en $p$, et $p \neq 2$

on a par H90 $F^\times \otimes \mathbb{Z}/M\mathbb{Z} \xrightarrow[\iota]{\sim} \left( F(\mu_n)^\times \otimes \mathbb{Z}/M\mathbb{Z} \right)^{G_n}$ (en terme de $H^1$, c'est l'inflation restriction: $\mu_M^{G_n} = 1$ )

on pose $\boxed{\kappa_n := \iota^{-1}(D_n c_n)}$

Récapitulation: $\left((\sigma - 1) D_n c_n\right)^{\frac{1}{M}} = (\sigma - 1) \beta_n$, $\beta_n \in F(\mu_n)^\times$ par Hilbert 90
$\sigma \in G_n$

et $\underline{\kappa_n = D_n c_n \beta_n^{-M}}$ mod $(F^\times)^M$.

## ③ Propriétés locales des $\kappa_n$

Si $x \in F^\times \otimes \mathbb{Z}/M\mathbb{Z}$, $x$ a un diviseur mod $M$ $[x] \in \bigoplus_{v \in \text{pl.} F} \mathbb{Z}/M\mathbb{Z} \cdot v$

si $\ell$ premier, son $\ell$-diviseur (mod $M$) $[x]_\ell := \sum_{v | \ell} v(x) \cdot v$

Clairement, si $\ell \nmid n$ (et $n \neq 1$), $[\kappa_n]_\ell = 0$ car $c_n$ est une unité et $F_\ell(\mu_n) / F_\ell$ non ram.

Kolyvagin a déterminé $[\kappa_n]_\ell$ si $\ell | n$ en terme de $\kappa_{\frac{n}{\ell}}$.

Nous avons besoin, pour exprimer cette comparaison, d'introduire

$\ell \in S$, $\varphi_\ell : \mathcal{O}_{F_\ell}^\times \otimes \mathbb{Z}/M\mathbb{Z} \xrightarrow{G\text{-éq.}} \bigoplus_{v | \ell} \mathbb{Z}/M\mathbb{Z} \cdot v$ "comparaison fini-singulier" $H^1_f(F_\ell, \mu_M) \longrightarrow H^1_s(F_\ell, \mu_M)$

$F_\ell = F \otimes \mathbb{Q}_\ell \simeq \prod_{v | \ell} \mathbb{Q}_\ell$ $\quad \| \quad \{ x \in F_\ell^\times \otimes \mathbb{Z}/M\mathbb{Z},\ [x]_\ell = 0 \}$

Sa $v$-composante est defini par $(v : F \to \mathbb{Q}_\ell)$

$$\begin{tikzcd} \mathbb{Z}_\ell^\times \arrow[r, "\mathrm{can}"] \arrow[dr] & \mathbb{F}_\ell^\times & G_\ell \arrow[l, "\sim"'] \arrow[r] & \mathbb{Z}/M\mathbb{Z}\cdot v \\ & (\mathbb{Z}/\ell\mathbb{Z})^\times \arrow[u, "\wr"'] & \sigma_\ell \arrow[r, mapsto] & 1.v \end{tikzcd}$$

, $\varphi_\ell$ <u>surjective, $G$-équivariante</u>

$\varphi_\ell(x)$ ne <u>depend que de $x^{\frac{\ell-1}{M}}$</u>.

la théorie du corps de classes de $\mathbb{Q}_\ell(\mu_\ell)/\mathbb{Q}_\ell$, élémentaire, montre que

$$\begin{tikzcd} & F_\ell(\mu_\ell)^\times \arrow[dl, "(\sigma_\ell-1)"'] \arrow[dr, "{[N_\ell(\cdot)]}"] & \\ (\mathcal{O}_{F_\ell(\mu_\ell)}/\ell)^\times \arrow[d, "\wr"] & & \bigoplus_{v|\ell} v.\mathbb{Z}/M\mathbb{Z} \\ (\mathcal{O}_{F_\ell}/\ell)^\times \arrow[urr] & & \end{tikzcd}$$

<u>commute</u>. (regarder l'image d'une unif.)

<u>Proposition</u> Si $\ell | r$, $(r \in \mathcal{S}_M)$ $[k_r]_\ell = \varphi_\ell(k_{r/\ell})$

<u>preuve</u> : $\underset{F^\times}{\underset{\cap}{k_r}} = \underbrace{D_r c_r}_{\text{unité}} \beta_r^{-M} \in F(\mu_r)^\times$, mais $F_\ell(\mu_r)/F_\ell$ ramifié d'indice $\underline{\ell-1}$.

$(\tilde{v}(k_r) = \frac{1}{e_1}\tilde{v}(\beta_r) = v(\gamma_\ell))$

Dans $F_\ell(\mu_r)$, $\beta_r = \underset{F_\ell(\mu_\ell)^\times}{\underset{\cap}{\gamma_\ell}}^{\frac{\ell-1}{M}} \times$ unité car $(\beta_r)$ provient de $F$, et $[k_r]_\ell = [N_\ell \gamma_\ell]$

puis $[k_r] = \varphi_\ell((\sigma_\ell-1)\gamma_\ell)$. Il suffit

donc d'identifier $((\sigma_\ell-1)\gamma_\ell)^{\frac{\ell-1}{M}}$. Mais (dans $\mathcal{O}_{F_\ell(\mu_\ell)}/_{1-\zeta_\ell} \subset \mathcal{O}_{F_\ell(\mu_r)}/_{1-\zeta_\ell}$)

$$\underset{(\sigma_\ell \in \text{inertie})}{(\sigma_\ell-1)(\gamma_\ell)^{\frac{\ell-1}{M}}} \equiv (\sigma_\ell-1)(\beta_r) = \underset{(\sigma_\ell-1)D_\ell = \ell-1-N_\ell}{((\sigma_\ell-1)D_r c_r)^{\frac{1}{M}}} = \frac{(D_{r/\ell} c_r)^{\ell-1/M}}{((1-\mathrm{Fr}_\ell^{-1}) D_{\frac{r}{\ell}} c_{\frac{r}{\ell}})^{\frac{1}{M}}} \equiv \frac{(D_{r/\ell} \mathrm{Fr}_\ell^{-1} c_{r/\ell})^{\frac{\ell-1}{M}}}{(1-\mathrm{Fr}_\ell^{-1})\beta_{\frac{r}{\ell}}} \leftarrow SE.2$$

$\leftarrow$ ops $\ell$-unité $\in \mathcal{O}_{F_\ell}^\times$

$$\equiv (\mathrm{Fr}_\ell^{-1} k_{r/\ell})^{\frac{\ell-1}{M}} \equiv (k_{\frac{r}{\ell}})^{\frac{\ell-1}{M}} \quad \blacksquare$$

## (III) <u>Interlude : une conséquence de Cebotarev</u>

Pour obtenir des relations "les plus independants possibles" dans $Cl(F) \otimes \mathbb{Z}/M\mathbb{Z}$ en prenant les images des classes $[k_r]$ de Kolyvagin, on doit verifier l'independance linéaire de certains corps de nombres, et bien choisir les $r \in \mathcal{S}_M$ par Cebotarev. C'est accompli par la proposition suivante (Thaine $F = \mathbb{Q}(\mu_p)^+$, Rubin général).

<u>Proposition</u> Soient $c \in Cl(F)[p^\infty]$, $M$ une puissance de $p$, $W \subset F^\times \otimes \mathbb{Z}/M\mathbb{Z}$ un sous-$G$-module fini, et $\psi : W \longrightarrow \mathbb{Z}/M\mathbb{Z}[G]$ $G$-équivariante (additive).

Il existe une infinité de premiers $\lambda$ de $F$ dans la classe $c$, de degré 1, et tels que

$$\exists\, u \in (\mathbb{Z}/M\mathbb{Z})^\times, \quad \forall w \in W \qquad \psi_\ell(w) = u \cdot \psi(w)(\lambda)$$

(où $\ell$ est le premier divisible par $\lambda$, noter que alors $[w]_\ell = 0$)

<u>Preuve</u>

$$\begin{tikzcd}[column sep=small]
 & F(\mu_M, W^{\frac{1}{M}}) \arrow[d, dash, "\text{groupe } \mathrm{Hom}(W,\mu_M)"] \\
H \arrow[dr, dash, "p\text{-Hilbert de } F\text{, de groupe } Cl(F)[p^\infty]"'] & F(\mu_M) \arrow[d, dash] \\
 & F
\end{tikzcd}$$

$\}$ groupe $\mathrm{Hom}(W, \mu_M)$ par la théorie de Kummer et car $F^\times \otimes \mathbb{Z}/M\mathbb{Z} \hookrightarrow F(\mu_M)^\times \otimes \mathbb{Z}/M\mathbb{Z}$ $\left( \text{noyau} = H^1(F(\mu_M)/F, \mu_M) = 1 \text{ car } \mu_M(F) = 1 \right)$

p-Hilbert → de F, de groupe $Cl(F)[p^\infty]$

. On a $F(\mu_M, W^{\frac{1}{M}}) \cap H = F$ car $F(\mu_M) \cap H = F$ (ram. en $p$)

et si $c \in \mathrm{Gal}(F(\mu_M)/F)$ est une conjugaison complexe,
alors $c$ agit par $+1$ sur $\mathrm{Gal}(H(\mu_M)/F(\mu_M))$, $-1$ sur $\mathrm{Gal}(F(\mu_M, W^{\frac{1}{M}})/F(\mu_M)) = \mathrm{Hom}(W, \mu_M)$

$\uparrow$ réel $\quad \uparrow -1$

Soit $\sigma \in \mathrm{Gal}(H(\mu_M, W^{\frac{1}{M}})/F)$ – d'image $c$ dans $\mathrm{Gal}(H/F)$
– qui dans $\mathrm{Gal}(F(\mu_M, W^{\frac{1}{M}})/F(\mu_M)) = \mathrm{Hom}(W, \mu_M)$
vaut

l'élément $\quad W \xrightarrow{\psi} \mathbb{Z}/M\mathbb{Z}[G] \xrightarrow{i} \mu_M$

"projection sur le neutre"

$1 \mapsto \zeta_M$ (choix), $g \neq 1 \mapsto 1$

<u>Chebotarev</u> $\Rightarrow$

$\exists \infty\ \lambda$ degré 1 tels que $\sigma = \mathrm{Frob}_\lambda$, on vérifie aisément qu'ils conviennent. $\square$

## (IV) $\#_p \, \underline{Cl(\mathbb{Q}(\mu_p)^+)_\chi} = \underline{\#(E/\mathcal{E})_\chi}$ d'après Kolyvagin

$F = \mathbb{Q}(\mu_p)^+$, $p \neq 2$, $E = \mathbb{Z}(\mu_p)^{+,\times}$, $\mathcal{E}$ = unités cyclotomiques

$\chi \in \mathrm{Hom}(\underset{\Delta}{\underset{\shortparallel}{\mathrm{Gal}(F/\mathbb{Q})}}, \mathbb{Z}_p^\times)$, $e_\chi = \frac{2}{p-1} \sum \chi(\sigma)^{-1}\sigma \in \mathbb{Z}_p[\Delta]$ idempotent

$C = Cl(\mathbb{Q}(\mu_p)^+)[p^\infty]$, $C_\chi := e_\chi C$, $(E/\mathcal{E})_\chi := e_\chi(E/\mathcal{E} \otimes \mathbb{Z}_p)$.

<u>théorème</u> (MW - Kolyvagin) $\forall \chi$, $\# C_\chi = \#(E/\mathcal{E})_\chi$

<u>preuve</u>. • D'après la proposition (I).11, $\prod_\chi \# C_\chi = \prod_\chi \#(E/\mathcal{E})_\chi$. il suffit de montrer une divisibilité. M-W montre $\Leftarrow$, Kolyvagin l'inverse, ie $\# C_\chi \mid \#(E/\mathcal{E})_\chi$.

• Si $\chi = 1$, $C_\chi \subset Cl(F)^\Delta$, mais on a une suite exacte

$$\text{Idéaux}(\mathcal{O}_F)^\Delta \xrightarrow[\uparrow \text{ 0 ici}]{} Cl(F)^\Delta \longrightarrow H^1(\Delta, \text{Princ.}(F)) \underset{H.90}{\overset{\delta}{\hookrightarrow}} H^2(\Delta, E) \xrightarrow{\ s\ (\Delta \text{ cyclique})} \{\pm 1\}/N(E)$$

donc si $p \neq 2$, $Cl(F)^\Delta \otimes \mathbb{Z}_p = \{0\}$. <u>On peut donc supposer $\chi \neq 1$</u>.

• Si $x \in F^\times \otimes \mathbb{Z}/M\mathbb{Z}$, on pose $t(x) = \mathrm{Max}\{d \mid M,\ x \in d.F^\times \otimes \mathbb{Z}/M\mathbb{Z}\}$, ie. le plus grand $d \mid n$ tels que les representants de $x$ dans $F^\times$ sont des puissances d'ièmes. si $M$ est une puissance de $p$, alors l'ordre de $x$ dans $F^\times \otimes \mathbb{Z}/M\mathbb{Z}$ est $M/t(x)$, car $\mu_M(F) = \{1\}$.

• J'affirme que $t(e_\chi(k_1)) = \#(E/\mathcal{E})_\chi$. Soit $E[\frac{1}{p}]$ les $p$-unités de $F$, alors (rappel : $c_1 = k_1 = (1-\zeta_p)(1-\zeta_p^{-1})$)

$$1 \to E[\tfrac{1}{p}] \to F^\times \to F^\times/E[\tfrac{1}{p}] \to 1 \qquad \approx \text{plat} / \mathbb{Z}$$

d'où $1 \to (E[\frac{1}{p}] \otimes \mathbb{Z}/M\mathbb{Z})_\chi \to (F^\times \otimes \mathbb{Z}/M\mathbb{Z})_\chi \to$ plat sur $\mathbb{Z}/M\mathbb{Z} \to 1$

et $\uparrow$ libre rg 1 / $\mathbb{Z}/M\mathbb{Z}$ par Dirichlet et $e_\chi(k_1)$ engendre $e_\chi(\mathcal{E})$ par definition.

On conclut par platitude du quotient $(\mathbb{Z}/M\mathbb{Z} \otimes E[\frac{1}{p}] \cap d.F^\times \otimes \mathbb{Z}/M\mathbb{Z} = d\, E[\frac{1}{p}] \otimes \mathbb{Z}/M\mathbb{Z})$.

• On pose $M = \# C_\chi \cdot \#(E/\mathcal{E})_\chi \cdot p$, $C_\chi = \langle c_1, \dots, c_r \rangle$

• On regarde $\mathbb{Z} e_\chi(k_1) =: W_1$, et on considère $\varphi_1 : W_1 \to \mathbb{Z}/M\mathbb{Z}[G]$, $e_\chi(k_1) \mapsto t_1 e_\chi$ bien défini, $t_1 := t(e_\chi(k_1))$

<u>proposition III + proposition II</u> $\Rightarrow \exists\, \ell_1 \mid \lambda_1$, $\lambda_1 \in c_1$, $[\kappa_{\ell_1}] = \varphi_{\ell_1}(e(\chi), k_1) = u_1 t_1 e_\chi(\lambda_1) \pmod M$

On projette dans $C_\chi$, il vient $t_1 c_1 = 0$. $(e_\chi = id)$

Comme on aurait pu prendre $c_2 \dots$ à la place de $c_1$, en fait $\#(E/\mathcal{E})_\chi \cdot C_\chi = 0$

(c'est le Théorème de Thaine). Mais on peut raffiner :

• Soit $t_2 = t(e_\chi(k_{\ell_1}))$, $t_2 \mid t_1 \mid \frac{M}{\#C_\chi}$ donc on peut diviser par $t_2$ avant de projeter dans $C_\chi$. Il vient que $\frac{t_1}{t_2}\cdot c_1 = 0$.

On pose
$$\begin{aligned} \varphi_2 : \mathbb{Z}\cdot e_\chi(k_{\ell_1}) &\longrightarrow \mathbb{Z}/M\mathbb{Z}[G] \\ e_\chi(k_{\ell_1}) &\longmapsto t_2 e_{(\chi)} \end{aligned}$$
bien définie.

proposition II et III $\underset{\lambda_2 \in c_2}{\overset{\exists \ell_2 \mid \lambda_2}{\Rightarrow}}$ $[e_\chi(k_{\ell_1\ell_2})] = u_2\, \varphi_{\ell_2}(e_\chi(k_{\ell_1})) + [e_\chi(k_{\ell_1\ell_2})]_{\ell_1}$

$t_3 = t(e_\chi(k_{\ell_1\ell_2})) \mid t_2$, on projette dans $C_\chi/c_1$ après avoir divisé par $t_3$ : $\frac{t_2}{t_3}\cdot c_2 = 0$ dans ce quotient

• Par récurrence, $r_i = \ell_1 \dots \ell_i$, $t_{i+1} = t(e_\chi(k_{r_i}))$, $\frac{t_i}{t_{i+1}}\cdot c_i = 0$ dans $C_\chi/_{c_1\dots c_{i-1}}$. D'où $\#C_\chi \mid \frac{t_1}{t_2}\dots\frac{t_n}{t_{n+1}} = \frac{\#(E/\mathcal{E})_\chi}{t_{n+1}}$. ■

## (V) Point de vue groupes de Selmer

$F$ corps de nombres, $T$ rep. $p$-adique de $G_F$ non ram. hors d'un ens. fini, $W = \mathrm{Hom}_{\mathbb{Z}_p}(T, \mathbb{Q}_p/\mathbb{Z}_p)$ dual Pontryagin

une version de Poitou-Tate (cf R1 1.7.3)

$$\begin{tikzcd}[column sep=small] 0 \arrow[r] & H^1_f(F,T) \arrow[r] & H^1_{f\text{ hors }\Sigma}(F,T) \arrow[r] & \bigoplus_{v\in\Sigma} H^1_s(F_v,T) \arrow[r] & H^1_f(F,W^*(1))^\vee \arrow[r] & H^1_{\substack{f\text{ hors }\Sigma\\ 0 \text{ en } \Sigma}}(F,W^*(1))^\vee \arrow[r] & 0 \\ 0 \arrow[r] & \mathcal{O}_F^\times \otimes \mathbb{Z}/M\mathbb{Z} \arrow[r] \arrow[u, "\text{Kummer}", "s"'] & \mathcal{O}_F[\frac{1}{\Sigma}]^\times \otimes \mathbb{Z}/M\mathbb{Z} \arrow[r, "\text{div}\,[\cdot]"] \arrow[u, "s"'] & \bigoplus_{v\in\Sigma} \mathbb{Z}/M\mathbb{Z}\cdot v \arrow[r] \arrow[u, "s"'] & Cl(F)_p[M] \arrow[r] \arrow[u, "s\ \text{c.d. classe}"'] & \mathrm{Pic}(\mathcal{O}_F[\frac{1}{\Sigma}])_p^{[M]} \arrow[r] \arrow[u, "s"'] & 0 \end{tikzcd}$$

si $T = \mu_M$ $\qquad v \longmapsto \overline{P_v}$

cas étudié : $F = \mathbb{Q}(\mu_p)^+$, $\chi$-partie de la suite.
On choisit récursivement $\Sigma$ de manière à tuer $\mathrm{Pic}(\mathcal{O}_F[\frac{1}{\Sigma}])_p$, pour obtenir à la fin une présentation de $Cl(F)_{p,\chi}$ en terme des diviseurs des éléments construits dans $\mathcal{O}_F[\frac{1}{\Sigma}]^\times \otimes \mathbb{Z}/M\mathbb{Z}$, i.e les $k_\ell$. Cela dicte le cas général. (cf. Exposé II)
La méthode permet de majorer $\# Cl(F)_p[M]$ par l'indice de l'élément de base du système d'Euler.

NB. • $\varphi_\ell$ peut être vue comme $H^1_f(F_\ell,\mu_M) \longrightarrow H^1_s(F_\ell,\mu_M)$ sendet

• par la théorie de Kummer $\quad 1 \to \mathcal{O}_{F_\ell}^\times \longrightarrow F_\ell^\times \xrightarrow{\sim} \bigoplus_{\lambda \mid \ell} \mathbb{Z}\cdot\lambda \to 1$

$-\otimes \mathbb{Z}/M\mathbb{Z}$ s'identifie à $\quad 1 \to H^1_f(F_\ell,\mu_M) \to H^1(F_\ell,\mu_M) \longrightarrow H^1_s(F_\ell,\mu_M) \to 1$.

# VI La conjecture principale d'Iwasawa

$p>2$

$$\begin{tikzcd}[row sep=small] & M_n \arrow[dd, dash, "\substack{p\text{-ext ab max}\\ \text{non ram.}\\ \text{hors } p}"'] \arrow[dr, dash] & \\ n\geq 0 & & L_n \arrow[dl, dash, "\substack{p\text{-ext. ab max.}\\ \text{non ramifiée}}"] \\ \mathbb{Q}(\mu_{p^{n+1}}) =: & K_n \arrow[d, dash] & \\ & \mathbb{Q} & \end{tikzcd}$$

$C_n := \mathrm{Gal}(L_n/K_n) \xrightarrow[\sim]{\text{can}} Cl(K_n)[p^\infty]$

$X_n := \mathrm{Gal}(M_n/K_n)$

$U_n :=$ unités de $\mathbb{Q}_p(\mu_{p^{n+1}}) \equiv 1$ modulo $(1-\zeta_{p^{n+1}})$

$E_n :=$ adhérence de $\mathbb{Z}(\mu_{p^{n+1}})^\times \cap U_n$ dans $U_n$

$\mathcal{E}_n :=$ ——— $\mathcal{E}_n \cap U_n$ ———

On pose $\mathcal{X}_\infty := \varprojlim_{n\geq 0} \mathcal{X}_n$

$\mathcal{X} = C, X, U, E, \mathcal{E} \dots$ ce sont des $\Lambda[\Delta]$-modules, $\mathcal{X}(\chi) := e_\chi(\mathcal{X})$, $\chi$ caractère de $\Delta$ dans $\mathbb{Z}_p^\times$

<u>problème</u> déterminer ces $\Lambda$-modules. Contrôle : $\mathcal{X}_{\infty\,\Gamma_n} \xrightarrow{\text{isom?}} \mathcal{X}_n$

où $\mathcal{X}_{\Gamma_n} := \mathcal{X}/(\gamma^{p^n}-1)\mathcal{X} = \mathcal{X} \otimes \Lambda_n$, $\Lambda_n = \mathbb{Z}_p[\mathrm{Gal}(K_n/K_0)] = \Lambda/(\gamma^{p^n}-1)$

<u>On a les propriétés suivantes :</u>

(i) $C_{\infty\,\Gamma_n} \longrightarrow C_n$ est un isomorphisme $\forall n\geq 0$, ainsi que $X_\infty(\chi)_{\Gamma_n} \longrightarrow X_n(\chi)$ si $\chi\neq 1$.
(Théorème d'Iwasawa) cf. appendice. En particulier, $C_\infty$ et $X_\infty(\chi)$ sont de torsion, t.f, et $C_{\infty\,\Gamma_n}$ fini $\forall n$.

(ii) $U_\infty(\chi)$ est isomorphe à $\Lambda$ si $\chi\neq 1,\tau$ et satisfait au contrôle si $\chi\neq 1$. Ainsi $E_\infty(\chi) \subset U_\infty(\chi)$ est pseudo isomorphe à $\Lambda$ si $\chi$ pair $\neq 1$ (nul si $\chi$ impair $\neq \tau$). (on utilise Leopoldt dans le premier cas). $\mathcal{E}_\infty(\chi)$ est libre de rang $1$ si $\chi\neq 1$ pair, engendré par $e_\chi(1-\zeta_{p^n})$, il satisfait au contrôle. Ainsi $(E_\infty/\mathcal{E}_\infty)(\chi) \sim \Lambda/h_\chi\Lambda$ pour un certain $h_\chi \neq 0 \in \Lambda$.

(iii) <u>Corps de classes</u> $1 \to U_\infty/E_\infty \to X_\infty \to C_\infty \to 1$. (*)
établit un lien entre ces modules.

<u>Rappel</u>. Soit $\chi\neq 1$ pair, il existe un unique élément $L_p(\chi) \in \Lambda$
tel que $\forall k\geq 1$, $\omega_{cycl}^k(L_p(\chi)) = (1-(\chi\tau)^{-k}(p)\,p^{k-1})\left(-\frac{B_{k,\chi\tau^{-k}}}{k}\right)$

· $\chi$ impair, $L_p(\chi) := i(L_p(\chi^{-1}\tau))$, $i : \Lambda \to \Lambda$ $\gamma \mapsto \omega_{cycl}(\gamma)\gamma$.
$^*\tau$ teichmuller

Théorème (Mazur - Wiles, Rubin)

a) - si $\chi$ est pair, $\mathrm{char}\,(C_\infty(\chi)) = \mathrm{char}\,\left( E_\infty/_{\mathcal{E}_\infty}(\chi) \right)$

b) - si $\chi \neq 1, \tau$ $\qquad L_p(\chi) = \begin{cases} \mathrm{char}\; X_\infty(\chi) & \text{si } \chi \text{ pair} \\ \mathrm{char}\; C_\infty(\chi) & \text{si } \chi \text{ impair} \end{cases}$

Remarques. • a) $\Rightarrow$ b) Si $\chi \neq 1$ pair, un calcul local montre que $L_p(\chi) = \mathrm{char}\; U_\infty/_{\mathcal{E}_\infty}(\chi)$

Mais alors
$$\underset{\substack{\uparrow \\ \text{de torsion} \\ \text{si } \chi\neq 1}}{\mathrm{char}\,(X_\infty(\chi))} = \mathrm{char}\; C_\infty(\chi)\; \underbrace{\mathrm{char}\; U_\infty/_{\mathcal{E}_\infty}(\chi)}_{\mathrm{char}\; U_\infty/_{E_\infty}(\chi)\; \mathrm{char}^{-1}\, E_\infty/_{\mathcal{E}_\infty}(\chi)} = L_p(\chi)\; \mathrm{char}\; C_\infty(\chi)\; \mathrm{char}^{-1}\, E_\infty/_{\mathcal{E}_\infty}(\chi). \qquad \circledast(\chi)$$

Pour le reste on utilise la dualité de Kummer pour $M_n/_{K_n}$ et on passe à la limite sur $n$:

pour un certain $\Delta \in K_\infty^\times \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$, $\quad \underset{X_\infty}{\overset{}{\mathrm{Gal}(M_\infty/_{K_\infty})}} \times \Delta \longrightarrow \mu_{p^\infty}$ accouplement parfait $\Gamma\times\Delta$ équivariant

et on a une suite exacte
$$0 \to \mathcal{O}_{K_\infty}^\times \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \to \Delta \to Cl(K_\infty)[p^\infty] \to 0$$
$$a \otimes p^{-n} \mapsto I$$
$$(a) = I^{p^n} \text{ dans } \mathcal{O}_{K_\infty}$$

Un résultat d'Iwasawa assure que si $\chi \neq \tau$, $\widehat{Cl(K_\infty)[p^\infty]}(\chi) \sim C_\infty(\chi)$

Mais pour un tel $\chi$, $\hat{\Delta}(\chi) \twoheadrightarrow \widehat{Cl(K_\infty)[p^\infty]}(\chi)$ et $\hat{\Delta}(\chi) \simeq X_\infty(\chi^{-1}\tau)$. ■

• Quand $\chi = 1, \tau$ $\;L_p(\chi)$ définie par la même formule est dans $\frac{\Lambda^\times}{\gamma-1}$. L'analogue du théorème est $C_\infty(1) = 0$ (ce qui résulte du contrôle et de $C_0(1)=0$ comme on a déjà vu) et $C_\infty(\tau) = 0$ (idem, Herbrand).

• La suite de Poitou-Tate pour $\mathbb{Z}_p(1)$ s'écrit:

$$\begin{tikzcd}
0 \arrow[r] & H^1_{Iw}(\mathbb{Q}, \mathbb{Z}_p(1)) \arrow[r] & H^1_{Iw}(\mathbb{Q}_p, \mathbb{Z}_p(1)) \arrow[r] & X_\infty \arrow[r] \arrow[dr] & H^2_{Iw}(\mathbb{Q}, \mathbb{Z}_p(1)) \arrow[r] & H^2_{Iw}(\mathbb{Q}_p, \mathbb{Z}_p(1)) \simeq \mathbb{Z}_p \arrow[r] & 0 \\
 & \varprojlim_m \mathbb{Z}[\mu_{p^m}][\tfrac{1}{p}]^\times \otimes \mathbb{Z}_p \arrow[r] \arrow[u, "\wr"] \arrow[d, "v_{1-\zeta_{p^m}}"] & \varprojlim_m \mathbb{Q}_p(\mu_{p^m})^\times \otimes \mathbb{Z}_p \arrow[u, "\wr"] \arrow[d, "v_{1-\zeta_{p^m}}"] & & C_\infty \arrow[u, hook] \arrow[ur, dashed, "0"] & & \\
 & \mathbb{Z}_p \arrow[r, "\sim"] & \mathbb{Z}_p & & & &
\end{tikzcd}$$
(kummer)

elle s'identifie donc à la suite $\circledast$ essentiellement

On voit de suite alors que la conjecture de Perrin-Riou prédit exactement le théorème pour $\mathbb{Z}_p(1)$..

## VII $\mathrm{Char}(C_\infty(\chi)) \mid \mathrm{Char}\left(\mathcal{E}_\infty/\mathcal{C}_\infty(\chi)\right)$, $\chi$ pair, d'après Rubin



• Cette divisibilité $\forall \chi$ entraîne l'égalité par la formule du nombre de classes, comme dans le cas de $C_0(\chi)$ déjà étudié. On a vu aussi que $C_\infty(1) = 0$. De plus

$$C_n(\chi) \xrightarrow[\text{(norme)}]{\sim} Cl(\mathbb{Q}(\mu_{p^{n+1}})^+)[p^\infty](\chi) \text{ car } \chi \text{ est pair et } p>2. \text{ On suppose donc } \chi \neq 1.$$

• On veut raisonner comme dans la preuve de Kolyvagin, mais sur $\mathbb{Q}(\mu_{p^n})^+$. Le problème est que l'on ne maîtrise que grossièrement $E_m^+$ et $C_n(\chi)$ comme $\Lambda_n$-module.

structure $\exists \quad 0 \to \bigoplus_{i=1}^{k} \Lambda/(f_i) \longrightarrow C_\infty(\chi) \longrightarrow Z_1 \to 0$ ← pseudo-nul, $1_i \mapsto c_i$.

serpent + contrôle $\Rightarrow \quad Z_1^{\Gamma_n} \to \bigoplus_{i=1}^{k} \Lambda_n/f_i \to C_n(\chi) \to Z_{1\,\Gamma_n}$ (*)

donc si $B_1 Z_1 = 0$ ← idéal de cod. finie, $\quad \underline{B_1 \mathrm{Ann}_{c_i} \text{ dans } C_n(\chi)/\sum_{j<i} \Lambda_n c_j \subset f_i \Lambda_n}$

pour $\mathcal{E}_\infty/\mathcal{C}_\infty(\chi)$. $\exists$ idéal $B_2$ cod fini, $\quad \mathcal{E}_\infty(\chi)_{\Gamma_n} \longrightarrow E_n(\chi)$ noyau fini, # ind. $n$, tué par $B_2$

(Contrôle faible, on le déduit du contrôle fait pour tous les autres $\Lambda$ modules et de la suite exacte du cup de classes les reliant.)

Comme $\mathcal{E}_\infty(\chi)$ libre de rang 1 sur $\Lambda$, engendré p. $e_\chi((1-\zeta_{p^n}))$, $\forall n$, $\eta \in B_2$, $\exists\ \theta_{n,\eta} : E_n(\chi) \longrightarrow \Lambda_n$, $\underline{e_\chi(1-\zeta_{p^n}) \longrightarrow \eta h_\chi}$.

et $\mathcal{E}_\infty/\mathcal{C}_\infty(\chi) \sim \Lambda/h_\chi\Lambda$

• On pose $B = B_1 B_2$, on fixe $m \geq 0$ et $\eta \in \overset{\text{bon}}{B}$. Soit $M :=$ une puissance de $p$

$\geq \# C_n(\chi)\, p^{m+(k+1)\alpha}$ ← fini, où $p^\alpha \geq \# \Lambda_n/\eta\Lambda_n\, \# \Lambda_n/h_\chi\Lambda_n$ ← fini si $\eta$ bon ← fini car $\frac{E_n}{C_n}(\chi)$ l'est.

• Soit $\psi_1 : E_n^+(\chi) \otimes \mathbb{Z}/M\mathbb{Z} \xrightarrow{\theta_{n,\eta}} \Lambda_n/M\Lambda_n \xrightarrow{\times e_\chi} \mathbb{Z}/M\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$

$F := \mathbb{Q}(\mu_{p^{n+1}})^+ \qquad e_\chi(\kappa_1) \longmapsto \eta h_\chi \longmapsto \eta h_\chi e_\chi.$

On applique la prop. Ceb $\Rightarrow \lambda_1 \mid \ell_1$ etc et on regarde $\kappa_{\ell_1}$ défini en II.
$\lambda_1 \in c_1$

$[e_\chi(k_{\ell_1})] = u_1 \eta h_\chi e_\chi(\lambda_1)$, on projette dans $C_n(\chi)$ $(\# C_n(\chi) \mid M)$

et il vient $\eta h_\chi c_1 = 0$, puis $\eta^2 h_\chi \in f_1 \Lambda_n$.

Remarque $c_1$ étant arbitraire, $\mathcal{B}^2 h_\chi C_n(\chi) = 0$, puis $\mathrm{char}\, C_\infty(\chi) \mid h_\chi^{k+1}$.
C'est l'analogue du résultat de Thaine, que l'on raffine comme suit :

- J'affirme qu'il existe $\Psi_2 : \Lambda_n \cdot e_\chi(k_{\ell_1}) \longrightarrow \frac{\Lambda_n}{M\Lambda_n}$, $f_1 e_\chi(k_{\ell_1}) \longmapsto \eta^2 h_\chi$.

Comme $\frac{\Lambda_n}{f_1}$ fini, $f_1$ non div. de $0$ dans $\Lambda_n$, et $\delta := \frac{\eta^2 h_\chi}{f_1}$ a un sens dans $\Lambda_n$.

On va vérifier que si $g \in \mathbb{Z}[\mathrm{Gal}(K_n/K_0)]$ satisfait $g(e_\chi(k_{\ell_1})) = 0$ dans $F^\times \otimes \mathbb{Z}/M\mathbb{Z}$ alors $\eta^2 h_\chi g \in M f_1 \Lambda_n$, ce qui définira $\Psi_2$ par $g\, e_\chi(k_{\ell_1}) \mapsto g\delta$.

(i) $e_\chi(\bigoplus_{v \mid \ell} \mathbb{Z}/M\mathbb{Z} \cdot v)$ est libre de rang 1 sur $\Lambda_n (\Lambda_n e_\chi(\lambda_1))$ l'indice de $\Lambda_n [e_\chi(k_{\ell_1})]_{\ell_1}$ dedans est $\leq p^{2\alpha} \mid \frac{M}{\# C_n(\chi)}$, donc $g\, [e_\chi(k_{\ell_1})]_{\ell_1} = 0 \Rightarrow \underline{g \in \# C_n(\chi) \frac{\Lambda_n}{M\Lambda_n}}$. $\quad [e_\chi(k_{\ell_1})]_{\ell_1} = (\eta h_\chi) \cdot e_\chi(\lambda_1)$

(ii) Soit $\beta \in F^\times$ relevant $e_\chi(k_{\ell_1})$ et $g \in \mathbb{Z}[\mathrm{Gal}(K_n/K_0)]$ tel que $g\beta = x^M$ dans $F^\times$.
Si $\ell$ premier $\mathrm{div}_\ell(x) = \frac{g}{M} \mathrm{div}_\ell(\beta)$. Si $\ell \neq \ell_1$, on sait que $M \mid \mathrm{div}_\ell(\beta)$, donc d'après i) $\# C_n(\chi) \mid \mathrm{div}_\ell(x)$ pour un tel $\ell$. En projetant $e_\chi(x)$ dans $C_n(\chi)$, il vient donc

$$0 = \frac{g \eta h_\chi}{M} c_1 \text{, puis } g\eta^2 h_\chi \in M f_1 \Lambda_n \text{, } \underline{\text{QED}}.$$

- Par le même procédé (cef + kol.), et en projetant dans $\frac{C_n(\chi)}{\sum_{j<i} \Lambda_n c_j}$, on construit $\ell_1 \dots \ell_i$

et $\Psi_{i+1} : \Lambda_n e_\chi(k_{\ell_1 \dots \ell_i}) \longrightarrow \frac{\Lambda_n}{M\Lambda_n}$, $e_\chi(k_{\ell_1 \dots \ell_i}) \times f_1 \dots f_i \longmapsto \eta^{i+1} h_\chi$

jusqu'à $\underline{i = k}$ (prendre $c_{k+1} = 0$), (ça utilisera que $p^{(k+1)\alpha} \mid \frac{M}{\# C_n(\chi)}$)

- $\underline{\text{Ainsi}}$ $f_1 \cdots f_k \mid \eta^{k+1} h_\chi$ dans $\frac{\Lambda_n}{p^n \Lambda_n}$ $(p^n \mid M)$, et ce $\forall n$.

compacité de $\Lambda \Rightarrow f_1 \cdots f_k \mid h_\chi \eta^{k+1}$ dans $\Lambda$, $\forall \eta$ bon $\Rightarrow \underbrace{f_1 \cdots f_k}_{\mathrm{char}(C_\infty(\chi))} \mid h_\chi$ ∎

# Appendice

## vérification de ES 1

$N(\mathbb{Q}(\mu_\ell)/\mathbb{Q})(1-\zeta_\ell) = \phi_\ell(1) = \ell$

$\ell | m$, $N_{\mathbb{Q}(\mu_{\ell m})/\mathbb{Q}(\mu_m)}(1-\zeta_{\ell m}) = \prod_{i=0}^{\ell-1}(1-\zeta_{\ell m}\zeta_\ell^i) = 1-\zeta_m$ car c'est $1-X^\ell$ evalué en $\zeta_{m\ell}$

$m>1$, $\ell \nmid m$, $a\ell + bm = 1$, $N_{\mathbb{Q}(\mu_{\ell m})/\mathbb{Q}(\mu_m)}(1-\zeta_{\ell m}) = \prod_{i=1}^{\ell-1}(1-\zeta_m^a\zeta_\ell^{bi}) = \left(\frac{1-X^\ell}{1-X}\right)_{X=\zeta_m^a} = \frac{1-\zeta_m}{1-\zeta_m^a}$

$\underline{ES\ 2}$ $\quad \zeta_{m\ell} = \zeta_{m\ell}^{a\ell}\zeta_{m\ell}^{bm} = \zeta_m^a \underbrace{\zeta_\ell^b}_{\equiv 1 \text{ dans } \overline{\mathbb{Q}}_\ell} \equiv \zeta_m^{\ell^{-1}}$ car $a\ell \equiv 1\ (m)$ et $a \equiv \ell^{-1}\ (m)$

## Fin de la preuve de la proposition III (d'après Rubin R2)

(existence de $u \in (\mathbb{Z}/M\mathbb{Z})^\times$ comme dans l'énoncé). Tout d'abord, si $\lambda$ premier de $F$ (tel que $F_\lambda$, $W \to \mu_M$ comme dans la preuve)

les applications $W \to \bigoplus_{v | \ell} \mathbb{Z}/M\mathbb{Z} \cdot v \to \mathbb{Z}/M\mathbb{Z} \cdot \lambda$.

$(\varphi_\ell(\cdot))_\lambda$ et $(\Psi(\cdot)(\lambda))_\lambda$ sont $(\mathbb{Z}/M\mathbb{Z})^\times$ - proportionnelles car elles ont pour même noyau $\{w \in W,\ w \text{ puissance } M\text{ième mod } \lambda\}$. On l'a déjà vu pour $\varphi_\ell$, et pour $\Psi(\cdot)(\lambda)_\lambda$ c'est l'affirmation $i \circ \Psi(w) = 1 \Leftrightarrow \mathrm{Frob}_\lambda(w^{1/M})/w^{1/M} = 1$.

Par $G$-équivariance de $\varphi_\ell$ et $\Psi$, le $u \in (\mathbb{Z}/M\mathbb{Z})^\times$ tel que $\varphi_\ell(\cdot)_\lambda = u\,\Psi(\cdot)(\lambda)_\lambda$ satisfait $\varphi_\ell(\cdot)_v = u\,\Psi(\cdot)(\lambda)_v \quad \forall v | \ell$. ∎

## Preuve de la propriété V.(1)

(thm. Iwasawa)

$$\begin{array}{l} L_\infty \\ \mid \ C_\infty \\ K_\infty \\ \mid \ \Gamma_m \\ K_m \end{array}$$

$G$ est produit semi-direct de $\Gamma_m$ par $C_\infty$ donc $\overline{DG} = (\gamma^{p^m}-1)C_\infty$

Ainsi, si $I$ designe l'inertie en une place de $L_\infty$ divisant $p$,

$G = C_\infty \cdot I$ et $\mathrm{Gal}(L_\infty/L_m) = \overline{DG}\cdot I \Rightarrow C_{\infty\,\Gamma_m} \xrightarrow{\sim} C_m$.

De même,

$$\begin{array}{l} M_\infty \\ \mid \ X_\infty \\ K_\infty \\ \mid \ \Gamma_m \\ K_m \end{array}$$

$G' = X_\infty \rtimes \Gamma_m$, $\overline{DG'} = (\gamma^{p^m}-1)X_\infty$

et donc $1 \to X_{\infty\,\Gamma_m} \to G'/\overline{DG'} \to \Gamma_m \to 1$, et $G'/\overline{DG'} \xrightarrow{\sim} \mathrm{Gal}(M_m/K_m)$.

si $\underline{\chi \neq 1}$, $\quad X_{\infty\,\Gamma_m} \xrightarrow{\sim} \mathrm{Gal}(M_m/K_m) =: X_m$ □