ANNALES DE L'INSTITUT FOURIER

ALEXIS MICHEL

Une formule de Riemann-Hurwitz pour le groupe de Selmer d'une courbe elliptique

Annales de l'institut Fourier, tome 43, n° 1 (1993), p. 57-84

<http://www.numdam.org/item?id=AIF_1993__43_1_57_0>

Ann. Inst. Fourier, Grenoble
43, 1 (1993), 57-84

UNE FORMULE DE RIEMANN-HURWITZ POUR LE GROUPE DE SELMER D'UNE COURBE ELLIPTIQUE

par Alexis MICHEL

INTRODUCTION

En 1981, K. Iwasawa, s'inspirant des idées de Chevalley et Weil ([ChWe]), a déterminé le caractère de la représentation galoisienne associée au p-groupe des classes imaginaires dans une p-extension de corps surcirculaires (i.e. de $\mathbb{Z}_p$-extensions cyclotomiques de corps de nombres, cf. [Iw1]). Les identités dimensionnelles correspondantes ne sont autre que le pendant, pour l'invariant lambda, de la classique formule de Riemann-Hurwitz relative au genre d'une courbe algébrique, connue sous le nom de formule de Kida ([Ki]).

En 1988, K. Wingberg a démontré une formule analogue pour le groupe de Selmer d'une courbe elliptique définie sur un corps de nombres F, avec multiplication complexe par l'anneau des entiers $\mathcal{O}_K$ d'un corps quadratique imaginaire $K \subset F$, laquelle s'énonce comme suit, [Wi2] :

Soit p un premier impair décomposé dans K, disons $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, pour lequel E a bonne réduction. Soit F_∞/F l'unique $\mathbb{Z}_p$-extension de F contenue dans $F(E_{\mathfrak{p}^\infty})$ et L_∞ une p-extension finie de F_∞ à groupe de Galois G, non ramifiée au dessus $\overline{\mathfrak{p}}$. Alors, si S_{L_∞} (resp. S_{F_∞}) désigne le groupe de Selmer de L_∞ (resp. F_∞), et $\check{S}_{L_\infty}$ (resp. $\check{S}_{F_\infty}$) son dual de Pontrjagin[(1)], il vient :

Mots-clés : Corps de nombres – Formes quadratiques entières.
Classification A.M.S. : 11G05 – 11G15 – 11R23 – 11R32 – 14K22 – 20C11.

(1) De façon générale on appelle rang d'un $\mathbb{Z}_p$-module de type fini M, la dimension sur $\mathbb{Q}_p$ de $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. On dit qu'un module N est divisible de cotype fini, si son dual de Pontrjagin $\check{N} = \mathrm{Hom}_{\mathbb{Z}_p}(N, \mathbb{Q}_p/\mathbb{Z}_p)$ est un $\mathbb{Z}_p$-module de type fini. Dans ce cas le corang de N est le rang de $\check{N}$.

THÉORÈME 1. — *Sous la conjecture faible $\mathfrak{p}$-adique de Leopoldt et la nullité de l'invariant μ des différents groupes de Selmer considérés, le caractère χ_{L_∞} de la représentation galoisienne de G associée au $\mathbb{Q}_p$-espace vectoriel $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \check{S}_{L_\infty}$ est donné par la formule :*

$$\chi_{L_\infty} - \epsilon 1_G = (\lambda_{F_\infty} - \epsilon)\mathrm{Reg}_G + \sum_{v \nmid \mathfrak{p}}^{\times} \mathrm{Ind}_{D_v}^G \mathrm{Aug}_{D_v}$$

où Reg_G est le caractère de la représentation régulière de $G = \mathrm{Gal}(L_\infty/F_\infty)$, 1_G le caractère unité, λ_{F_∞} le corang[(1)] de S_{F_∞} et $\mathrm{Ind}_{D_v}^G \mathrm{Aug}_{D_v}$ l'induit à G du caractère d'augmentation de D_v, le groupe de décomposition de v[(2)]. La somme est restreinte aux places v décomposées dans $L(E_\mathfrak{p})/L$ et $\epsilon = 1$ ou 0 suivant que $F(E_\mathfrak{p})$ est égale à F ou non.

Exprimée en termes de dimensions, (ou plus simplement, en évaluant les caractères en $s = 1$), la formule précédente s'écrit :

$$\lambda_{L_\infty} - \epsilon = (\lambda_{F_\infty} - \epsilon)[L_\infty : F_\infty] + \sum_{v \nmid \mathfrak{p}}^{\times} (e_v - 1)$$

e_v étant l'indice de ramification de la place v dans l'extension L_∞/F_∞ et λ_{L_∞} étant le corang de S_{L_∞}.

Dans cette article nous nous proposons de donner une nouvelle démonstration de ce théorème (Partie II) en suivant essentiellement la démarche expliquée dans [JaMi] : tout comme pour les formules de Kuz'min-Kida (ou de Deuring-Shafarevitch) relatives aux corps surcirculaires (ou aux corps de fonctions), nous interprétons l'identité de Wingberg en termes de quotient de Herbrand. Ce point de vue présente l'avantage, d'une part, d'être dans l'esprit de l'inspiration initiale de la théorie d'Iwasawa et des théorèmes de représentations de Chevalley et Weil; d'autre part de donner de façon naturelle au regard de l'appendice de [JaMi], une généralisation du résultat dans un cas non galoisien : cela fait l'objet de la partie III.

Nous terminons (partie IV) en donnant, pour le groupe de Selmer, les analogues des classiques formules de Kani ([Ka] et [Ac]) sur le genre (ou l'invariant de Hasse-Witt) de certaines familles de revêtements algébriques : les preuves sont essentiellement contenues dans [MaZi] article relatif au cas surcirculaire.

---

(2) Le caractère $\mathrm{Ind}_{D_v}^G \mathrm{Aug}_{D_v}$ ne dépend pas du choix d'une place w de L_∞ au-dessus de v contrairement à D_v. Par abus, nous parlons ici du groupe de décomposition de v.

I. NOTATIONS ET DÉFINITIONS

Dans cette partie nous donnons les définitions et les principales propriétés utilisées par la suite et nous fixons les notations.

1. Courbe elliptique.

E désigne une courbe elliptique définie sur un corps de nombres F. K est un corps imaginaire quadratique contenu dans F, fixé une fois pour toutes. On suppose que E a multiplication complexe par $\mathcal{O}_K$ l'anneau des entiers de K. Dans ce qui suit E est toujours supposée définie sur les corps de nombres considérés qui, de plus, contiennent toujours K.

On se donne un premier p impair vérifiant les propriétés suivantes :

(i) $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ (p est décomposé dans $K/\mathbb{Q}$)

(ii) E a bonne réduction en tout premier de F au dessus de p.

Soit N une extension algébrique de F, puis $E(N)$ le groupe des points rationnels de E sur N. Si L est une extension galoisienne de N, $\mathrm{Gal}(L/N)$ est son groupe de Galois. Enfin $\overline{N}$ est une clôture algébrique de N fixée une fois pour toutes.

Soit G un groupe quelconque opérant sur un module M. On note M^G le sous-module des points fixes et M_G le plus grand quotient de M sur lequel G opère trivialement.

Si M et N sont deux G-modules on fait opérer G sur $\mathrm{Hom}(M, N)$ de la façon suivante :

$$\sigma f(a) = \sigma f(\sigma^{-1}a) \text{ pour } a \in M, \text{ et } \sigma \in G.$$

Si A est un $\mathrm{Gal}(\overline{N}/N)$-module discret, $H^i(N, A)$ désigne le i-ième groupe de cohomologie pour cette action : si $A = E(\overline{N})$ on note juste $H^i(N, E)$. Pour tout $\mathcal{O}_K$-module M on note M_α le noyau de la multiplication par α (considéré comme élément de $\mathcal{O}_K$), et pour tout idéal entier $\mathfrak{A}$ de $\mathcal{O}_K$ $M_\mathfrak{A} = \bigcap_{\alpha \in \mathfrak{A}} M_\alpha$.

Remarque. — On notera de la même façon l'extension ou la restriction d'une place d'un corps de nombres, afin d'alléger les notations.

2. Eléments de calcul infinitésimal (cf [Ja1]).

Soit L un corps de nombres (contenant K) et L_v son complété en une place v. Au corps L nous associons deux $\mathbb{Z}_p$-modules topologiques multiplicatifs :

– à partir du groupe $L^\times$ en formant le tensorisé $\mathcal{R}_L = \mathbb{Z}_p \otimes_{\mathbf{Z}} L^\times$ équipé de la topologie limite inductive des topologies des tensorisés de ses sous-groupes de type fini.

– à partir de l'algèbre semi-locale $L_\mathfrak{p} = \prod_{v|\mathfrak{p}} L_v$, en prenant le complété profini $\widehat{L}_\mathfrak{p}^\times$ du groupe des éléments inversibles :

$$\widehat{L}_\mathfrak{p}^\times = \varprojlim_m L_\mathfrak{p}^\times/(L_\mathfrak{p}^\times)^{p^m} = \prod_{v|\mathfrak{p}} \varprojlim_m L_v^\times/(L_v^\times)^{p^m}.$$

Dans ce dernier cas nous obtenons un $\mathbb{Z}_p$-module de type fini donc compact pour sa topologie naturelle.

L'application naturelle $L^\times \to \prod_{v|\mathfrak{p}} L_v^\times$ induit un épimorphisme continu de $\mathcal{R}_L$ sur $\widehat{L}_\mathfrak{p}^\times$ noté $s_\mathfrak{p}$ et appelé application de semi-localisation.

On pose

$$\mathcal{U}_\mathfrak{p}^m = \prod_{v|\mathfrak{p}}(1+v^m), \quad \mathcal{R}_{L,\mathfrak{p}}^m = s_\mathfrak{p}^{-1}(\mathcal{U}_\mathfrak{p}^m), \text{ et } \mathcal{R}_{L,\mathfrak{p}}^\infty = \bigcap_{m\geq 0} \mathcal{R}_{L,\mathfrak{p}}^m.$$

Le groupe $\mathcal{R}_{L,\mathfrak{p}}^\infty$ est donc constitué des éléments globaux qui sont localement au-dessus de $\mathfrak{p}$ arbitrairement proches de 1. On l'appelle le groupe des éléments infinitésimaux. C'est aussi le noyau de $s_\mathfrak{p}$.

Soit $\mathcal{E}_L = \mathbb{Z}_p \otimes_{\mathbf{Z}} E_L$ où E_L est le groupe des unités de L et $\mathcal{E}_{L,\mathfrak{p}}^\infty = \mathcal{E}_L \cap \mathcal{R}_{L,\mathfrak{p}}^\infty$ le noyau de la restriction de $s_\mathfrak{p}$ à $\mathcal{E}_L$. Nous l'appellerons aussi groupe de défaut de la conjecture $\mathfrak{p}$-adique de Leopoldt. Lorsque la conjugaison complexe opère sur les unités, la conjecture de Leopoldt usuelle n'affirme rien d'autre que la trivialité de ce groupe.

En effet, définissons de la même façon $\mathcal{E}_{L,p}^\infty = \mathcal{E}_L \cap \mathcal{R}_{L,p}^\infty$ et $\mathcal{E}_{L,\overline{\mathfrak{p}}}^\infty = \mathcal{E}_L \cap \mathcal{R}_{L,\overline{\mathfrak{p}}}^\infty$, avec des notations évidentes. Clairement $\mathcal{E}_{L,\overline{\mathfrak{p}}}^\infty$ est l'image par la conjugaison complexe τ de K de $\mathcal{E}_{L,\mathfrak{p}}^\infty$. Donc on a $\mathcal{E}_{L,p}^\infty = \mathcal{E}_{L,\mathfrak{p}}^\infty \oplus \tau(\mathcal{E}_{L,\mathfrak{p}}^\infty)$. Affirmer la trivialité de $\mathcal{E}_{L,\mathfrak{p}}^\infty$ ou de $\mathcal{E}_{L,p}^\infty$, c'est bien la même chose. Pour alléger les notations on pose $\mathcal{E}_{L,\mathfrak{p}}^\infty = \mathcal{E}_L^\infty$ (resp. $\mathcal{R}_{L,\mathfrak{p}}^\infty = \mathcal{R}_L^\infty$), sans ambiguïté pour la suite.

3. Corps de classes et infinitésimaux.

Nous notons $\mathcal{D}_L = \mathbb{Z}_p \otimes_{\mathbf{Z}} D_L$ le tensorisé p-adique du groupe des diviseurs[3] de L, $\mathcal{P}_L = \mathbb{Z}_p \otimes P_L$ son sous-groupe principal, image canonique de $\mathcal{R}_L$ dans $\mathcal{D}_L$. On dit qu'un diviseur est principal-infinitésimal si c'est un diviseur engendré par un élément infinitésimal, i.e. $\mathcal{P}_L^{\infty} = \{(\alpha); \alpha \in \mathcal{R}_L^{\infty}\}$: c'est aussi l'image canonique de $\mathcal{R}_L^{\infty}$ dans $\mathcal{D}_L$. On note $\mathcal{D}_L^{\infty}$ la racine de $\mathcal{P}_L^{\infty}$ dans $\mathcal{D}_L$, i.e. le groupe des diviseurs dont une puissance est principale-infinitésimale.

La théorie du corps de classes interprète les infinitésimaux comme suit.

LEMME 1. — *Le groupe de Galois de la p-extension abélienne maximale de L, non ramifiée en dehors de $\mathfrak{p}$, s'identifie au groupe $\mathcal{D}_L^0/\mathcal{P}_L^{\infty}$, noté encore $\mathcal{C}\ell_L^0$, des classes infinitésimales du corps L, quotient du groupe des diviseurs étrangers à $\mathfrak{p}$ par le groupe des diviseurs principaux-infinitésimaux.*

La torsion de $\mathcal{C}\ell_L^0$ s'identifie à $\mathcal{C}\ell_L^{\infty} = \mathcal{D}_L^{\infty}/\mathcal{P}_L^{\infty}$.

4. Courbe elliptique et théorie d'Iwasawa.

Au corps de base F du **1**, nous associons une $\mathbb{Z}_p$-extension construite à partir de points de E.

On pose $E_{\mathfrak{p}^{\infty}} = \bigcup_n E_{\mathfrak{p}^n}$, $\mathcal{F}_{\infty} = F(E_{\mathfrak{p}^{\infty}})$, $\mathcal{F} = F(E_{\mathfrak{p}})$ et $\Delta = \mathrm{Gal}(\mathcal{F}/F)$ (en particulier $|\Delta|$ divise $p-1$).

L'action naturelle de $\mathrm{Gal}(\mathcal{F}_{\infty}/F)$ sur $E_{\mathfrak{p}^{\infty}}$ définit une injection χ_{∞} : $\mathrm{Gal}(\mathcal{F}_{\infty}/F) \hookrightarrow \mathbb{Z}_p^{\times}$ à image d'indice fini dans $\mathbb{Z}_p^{\times}$. On écrit $\mathbb{Z}_p^{\times} = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$, où μ_{p-1} est le groupe des racines $(p-1)$-ièmes de l'unité, et $\mathrm{Gal}(\mathcal{F}_{\infty}/F) = \Delta \times \Gamma$, Γ étant le groupe de Galois $\mathrm{Gal}(\mathcal{F}_{\infty}/\mathcal{F})$ isomorphe à $\mathbb{Z}_p$. On a alors $\chi_{\infty}(\Delta) \subset \mu_{p-1}$ et $\chi_{\infty}(\Gamma) \subset 1 + p\mathbb{Z}_p$. On note χ la restriction de χ_{∞} à Δ. Si on pose $F_{\infty} = \mathcal{F}_{\infty}^{\Delta}$, alors F_{∞}/F est une $\mathbb{Z}_p$-extension.

Comme Δ est cyclique d'ordre, disons d, divisant $p-1$, tout $\mathbb{Z}_p[\Delta]$-module M s'écrit :

$$M = \bigoplus_{i \bmod d} M^{\chi^i},$$

(3) Nous employons le langage des diviseurs car le formalisme est valable dans ce cadre. Bien entendu p étant impair il s'agit en fait ici d'idéaux.

où M^{χ^i} est le sous-module de M sur lequel Δ opère via χ^i.

De la même façon on note M_χ le plus grand quotient de M sur lequel Δ opère via χ.

Le groupe $\Gamma = \mathrm{Gal}(F_\infty/F) = \gamma^{\mathbf{Z}_p}$ est identifié à $\mathbb{Z}_p$, après choix d'un générateur topologique γ. Et $\Lambda = \mathbb{Z}_p[[\gamma - 1]]$ est l'algèbre d'Iwasawa associée, isomorphe, non canoniquement, à l'anneau des séries formelles en une variable $\mathbb{Z}_p[[T]]$. On munit ainsi tout Γ-module M compact d'une structure de Λ-module compact avec :

$$(1+T)x = \gamma x \text{ pour } x \in M.$$

Enfin F_n désigne l'unique sous-corps de F_∞ cyclique de degré p^n sur F , Γ_n étant le sous-groupe ouvert qui lui correspond par la théorie de Galois.

Les objets définis au **1**, relatifs à l'étage F_n/F, seront indexés par F_n. Le groupe $\mathcal{D}_{F_\infty} = \varinjlim \mathcal{D}_{F_n}$ est le tensorisé du groupe des diviseurs $D_{F_\infty} \otimes_{\mathbf{Z}} \mathbb{Z}_p$ et, $\mathcal{P}_{F_\infty} = \varinjlim \mathcal{P}_{F_n}$ le sous-groupe des diviseurs principaux de F_∞, image dans $\mathcal{D}_{F_\infty}$ de $\mathcal{R}_{F_\infty} = \mathbb{Z}_p \otimes_{\mathbf{Z}} F_\infty^\times$.

De même pour $\mathcal{F}_\infty/\mathcal{F}$: ce sont ces objets là qui nous intéressent en premier lieu. Les groupes infinitésimaux associés à $\mathcal{F}_\infty$ se définissent de façon identique comme limite inductive de ces mêmes groupes attachés aux sous-corps $\mathcal{F}_n$. Par exemple le groupe de défaut de la conjecture de Leopoldt dans $\mathcal{F}_\infty$ est la réunion $\mathcal{E}^\infty_{\mathcal{F}_\infty} = \bigcup_n \mathcal{E}^\infty_{\mathcal{F}_n}$.

On dit que la tour $\mathcal{F}_\infty/\mathcal{F}$ vérifie "la conjecture faible $\mathfrak{p}$-adique" de Leopoldt si le $\mathbb{Z}_p$-rang $\delta_{\mathcal{F}_n}$ du groupe de défaut à l'étage n est borné. Dans ce cas $\mathcal{E}^\infty_{\mathcal{F}_\infty}$ est un $\mathbb{Z}_p$-module libre de rang fini, disons $\delta_{\mathcal{F}_\infty}$.

Remarquons tout de suite, que cette hypothèse "faible" est nécessaire pour le genre de formule que l'on souhaite établir, (voir ci-après). En revanche cette condition est toujours vérifiée dans le cas cyclotomique (Lemme 13.30 [Wa] par exemple).

5. Groupe de Galois et groupe de Selmer [Co].

Soit S un ensemble fini de places de $\mathcal{F}$. Par $\mathcal{F}_S$ on désigne la p-extension abélienne maximale de $\mathcal{F}$ non ramifiée en dehors de S. On note $S_\mathfrak{p} = \{v \in S; v|\mathfrak{p}\}$: dans ce cas $\mathcal{F}_{S_\mathfrak{p}}$ est notée $\mathfrak{M}_\mathcal{F}$.

La théorie du corps de classes affirme l'existence d'une unique $\mathbb{Z}_p$-extension de K, non ramifiée en dehors de $\mathfrak{p}$, que nous notons K_∞. La

théorie de la multiplication complexe montre que F_∞ est alors la composée de K_∞ et F. En particulier F_∞/F est non ramifiée en dehors de $\mathfrak{p}$. Donc $F_\infty \subset \mathfrak{M}_{\mathcal{F}}$. De même $\mathcal{F}_\infty \subset \mathfrak{M}_{\mathcal{F}}$.

On considère $\mathfrak{M}_{\mathcal{F}_\infty}$ la p-extension maximale de $\mathcal{F}_\infty$ abélienne non ramifiée en dehors de $\mathfrak{p}$, qui n'est autre que la réunion des $\mathfrak{M}_{\mathcal{F}_n}$. On note $X_{\mathcal{F}_\infty} = \mathrm{Gal}(\mathfrak{M}_{\mathcal{F}_\infty}/\mathcal{F}_\infty)$, et on rappelle que $X_{\mathcal{F}_\infty}^{\chi}$ est le sous-module de $X_{\mathcal{F}_\infty}$ sur lequel Δ opère via χ. On sait (Lemme 12 et 13 [Co]) que $X_{\mathcal{F}_\infty}$ est un Λ-module noethérien qui, sous la conjecture faible $\mathfrak{p}$-adique de Leopoldt, est de Λ-torsion (Lemme 14 *loc. cit.*). Sous cette condition on a de plus que $X_{\mathcal{F}_\infty}$ est sans Λ-module fini, ([Gr]).

Nous rappelons maintenant les résultats essentiels sur les groupes de Selmer dont nous avons besoin. Pour plus de détails, nous renvoyons à [Co] et [Si], par exemple.

Soit π tel que $(\pi) = \mathfrak{p}^k$ pour un certain k. Si A est un $\mathcal{O}_K$-module, on note $A(\mathfrak{p}) = \bigcup_{n\geq 1} A_{\pi^n}$.

Comme pour les corps de nombres, on définit le groupe de Tate-Shafarevitch Ш_{F_∞} associé à F_∞ par la suite exacte :

$$0 \to \text{Ш}_{F_\infty} \to H^1(F_\infty, E) \to \prod_{v\nmid\mathfrak{p}} H^1(F_{\infty,v}, E).$$

$F_{\infty,v}$ désigne ici la réunion de toutes les complétions en v des sous-extensions finies de F_∞/F. On notera que $F_{\infty,v}$ n'est peut-être pas complet.

On a la suite exacte suivante :

$$0 \to E_{\pi^n} \to E(\overline{F}_\infty) \to E(\overline{F}_\infty) \to 0$$

(bien sûr $\overline{F}_\infty$ est égale à $\overline{F}$).

On obtient la suite de cohomologie pour l'action de $\mathrm{Gal}(\overline{F}_\infty/F_\infty)$:

$$0 \to E(F_\infty)/\pi^n\, E(F_\infty) \to H^1(F_\infty, E_{\pi^n}) \to H^1(F_\infty, E)_{\pi^n} \to 0.$$

Alors, le groupe de Selmer de E sur F_∞ relatif à π^n est défini comme l'image réciproque de $(\text{Ш}_{F_\infty})_{\pi^n}$ dans $H^1(F_\infty, E_{\pi^n})$ par le morphisme de droite. Le groupe de Selmer associé à F_∞ est $S_{F_\infty} = \varinjlim_n S_{F_\infty}^{(\pi^n)}$, la limite inductive étant prise sur les morphismes induits par l'injection canonique de E_{π^n} dans $E_{\pi^{n+1}}$. En particulier, les morphismes de restriction conduisent à la suite exacte :

$$0 \to S_{F_\infty} \to H^1(F_\infty, E_{\mathfrak{p}^\infty}) \to \prod_{v\nmid\mathfrak{p}} H^1(F_{\infty,v}, E)(\mathfrak{p}).$$

Remarquons que la restriction aux seules places ne divisant pas $\mathfrak{p}$, dans le terme de droite, ne change, ni la définition de la $\mathfrak{p}$-composante du groupe de Tate-Shafarevitch, ni celle du groupe de Selmer en haut de la tour (Lemme 8 [Co]). C'est ce point de vue que nous utiliserons. Il en va autrement pour un corps de nombres, i.e. pour les extensions algébriques finies de $\mathbb{Q}$.

La démonstration de la formule de Wingberg repose sur le résultat suivant (cf. par exemple [Co] Th. 12).

THÉORÈME 2. — *On a* $S_{F_\infty} \simeq \mathrm{Hom}_\Delta(X_{\mathcal{F}_\infty}, E_{\mathfrak{p}^\infty}) \simeq \mathrm{Hom}_{\mathbb{Z}_p}(X^\chi_{\mathcal{F}_\infty}, E_{\mathfrak{p}^\infty})$, *comme* $\mathrm{Gal}(F_\infty/F)$*-modules.*

Cela signifie que le groupe de Selmer peut être regardé comme le reflet d'un certain groupe de Galois, dans un miroir convenable.

Sous la conjecture "faible", si l'invariant $\mu_{\mathcal{F}_\infty}$ d'Iwasawa associé à $X_{\mathcal{F}_\infty}$ est nul alors, $X^\chi_{\mathcal{F}_\infty}$ est un $\mathbb{Z}_p$-module libre de type fini de rang disons λ_{F_∞}. En fait la nullité du mu de la χ-composante suffit. De plus, comme groupe, $E_{\mathfrak{p}^\infty}$ est isomorphe à $\mathbb{Q}_p/\mathbb{Z}_p$, S_{F_∞} est isomorphe à $(\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_{F_\infty}}$: cela justifie la notation relative à F_∞.

L'un des intérêts de l'étude de S_{F_∞} est le suivant : la conjecture "faible" implique que $E(F_\infty)$ modulo son groupe de torsion est un groupe abélien libre de type fini (Th. 16 *loc. cit.*). Si de plus λ_{F_∞} est nul, alors $E(F)$ est de torsion.

II. LA FORMULE DE WINGBERG

1. Le cadre du problème.

Soit N un corps de nombres (au sens de I. 1). On lui associe les corps $\mathcal{N}$, $\mathcal{N}_\infty$ et N_∞, avec les notations de I. La conjecture faible $\mathfrak{p}$-adique de Leopoldt est vraie, pour une classe de courbes elliptiques à multiplication complexe relativement grande; en effet il suffit que $N(E_\mathfrak{p})$ soit abélienne sur K, (cf. Prop. 15 [Co]), ce qui est le cas par exemple si $N(E_{\mathrm{tor}})/K$ est abélienne sur K ou si $F = K$. Il n'est pas trop restrictif de supposer que la tour $\mathcal{N}_\infty/\mathcal{N}$ satisfait la conjecture.

Soit une p-extension finie galoisienne de F_∞ , à groupe G, non ramifiée au-dessus de $\overline{\mathfrak{p}}$. Compte tenu de ce qu'on souhaite montrer, on peut toujours

se ramener au cas où l'extension est du type L_∞/F_∞, provenant d'une p-extension L/F, à groupe G et non ramifiée au dessus de $\overline{\mathfrak{p}}$.

On énonce (et prouve succinctement) un lemme, afin de donner un sens à certains objets.

LEMME 2. — *Si $\mathcal{L}_\infty/\mathcal{F}_\infty$ est une p-extension non ramifiée au-dessus de $\overline{\mathfrak{p}}$, la nullité de $\mu_{\mathcal{F}_\infty}$ invariant mu associé à $X_{\mathcal{F}_\infty}$, implique celle de $\mu_{\mathcal{L}_\infty}$.*

Démonstration. — Un p-groupe étant nilpotent on peut toujours supposer que $\mathcal{L}_\infty/\mathcal{F}_\infty$ est cyclique d'ordre p. Soit T un ensemble fini de places telles que $T \cap S_p = S_{\mathfrak{p}}$ et $\mathcal{L}_\infty \subset \mathcal{F}_T$ (compte tenu de la ramification cela est toujours possible). Alors (cf. Th. [8] [Wi1]), le groupe de Galois $\mathrm{Gal}(\mathcal{F}_T/\mathcal{L}_\infty)$ est un pro p-groupe libre de rang fini. Pour le quotient $\mathrm{Gal}(\mathfrak{M}_{\mathcal{L}_\infty}/\mathcal{L}_\infty)$ on obtient alors $\mu(\mathrm{Gal}(\mathfrak{M}_{\mathcal{L}_\infty}/\mathcal{L}_\infty)) = 0$. D'où le lemme. □

Remarque. — Bien entendu, pour notre problème, la nullité de μ^χ associé à la χ-composante de chaque module suffit, mais on montre facilement que ces deux conditions sont équivalentes; il suffit par exemple d'adapter la démonstration analogue relative à l'invariant μ^- des $\mathbb{Z}_p$-extensions cyclotomiques à conjugaison complexe. Le lemme signifie donc que, si $\mu_{\mathcal{F}_\infty}$ est nul, alors le groupe de Selmer S_{N_∞} d'une extension de F_∞, disons N_∞ contenue dans L_∞ est de type fini. Il en est de même pour $\mathrm{E}(N_\infty)$.

Nous supposons une fois pour toutes que $\mu_{\mathcal{F}_\infty} = 0$. D'après [Gi] ceci est vrai dès que F est abélienne sur K, par exemple si $F = K$.

Au groupe de Selmer S_{N_∞}, on associe canoniquement un $\mathbb{Q}_p$-espace vectoriel V_{N_∞} de dimension λ_{N_∞}, et un réseau Y_{N_∞} de cet espace. Il suffit de prendre pour Y_{N_∞} le module $\mathrm{Hom}_{\mathbf{Z}_p}(\check{S}_{N_\infty}, \mathbb{Z}_p)$ des formes linéaires entières sur le dual de Pontrjagin de S_{N_∞}. Puis on pose $V_{N_\infty} = Y_{N_\infty} \otimes_{\mathbf{Z}_p} \mathbb{Q}_p$. On a ainsi défini la suite exacte suivante :

$$0 \to Y_{N_\infty} \to V_{N_\infty} \to S_{N_\infty} \to 0.$$

Si on considère la p-extension L_∞/F_∞, à groupe G, V_{L_∞} hérite, canoniquement de S_{L_∞}, une structure de G-module. On souhaite déterminer le caractère associé à cette représention de G. C'est la formule de Wingberg.

Remarque. — Si $\check{S}_{L_\infty} \simeq X_{L_\infty}^\chi$ comme groupe, il n'en est pas de même lorsqu'on regarde l'action de G.

2. Réduction au cas cyclique d'ordre p. Calcul de rang.

On suit pas à pas la démarche expliquée dans [JaMi], (pour une étude détaillée voir [Mi]). Les lemmes suivants permettent de se ramener, d'une part à un calcul de rang, d'autre part au cas où G est cyclique d' ordre p (Chap.2 [Mi])

On a le résultat suivant :

LEMME 3. — *$H^i(G, S_{L_\infty})$ est un p-groupe fini pour $i \geq 1$.*

Démonstration. — On montre en fait le résultat suivant, l'argument étant essentiel pour la suite :

Si M est un G-module $\mathbb{Z}_p$-divisible et de cotype fini, alors $H^i(G, M)$ est un p-groupe fini. En effet, M est défini par une suite exacte :

$$0 \to Y \to V \to M \to 0$$

où V est un $\mathbb{Q}_p$-espace vectoriel de dimension finie, Y un réseau de V, munis chacun d'une structure de G-module. Il vient que $H^i(G, V) = 1$ et, $H^i(G, M) \simeq H^{i+1}(G, Y)$ par décalage . On conclut en sachant que Y est $\mathbb{Z}_p$-libre, de type fini et que $H^{i+1}(G, Y)$ de torsion. □

On considère maintenant une extension L_∞/F_∞ finie galoisienne (non ramifiée au dessus de $\overline{\mathfrak{p}}$), de degré quelconque, de groupe G qui admet un unique p-Sylow. Le cadre du problème se limite à la situation d'un p-groupe, mais le lemme énoncé ci-dessous est vrai sans hypothèse sur l'ordre de G.

LEMME 4. — *Avec les notations précédentes, la restriction induit un morphisme à noyau et conoyau finis, i.e. un pseudo-isomorphisme, de S_{F_∞} dans le module des points fixes par G de S_{L_∞}. En particulier cela signifie que les espaces V ci-dessus vérifient la théorie de Galois, i.e. pour tout sous-groupe H de G on a : $V_{L_\infty}^H = V_{L_\infty^H}$.*

Démonstration.

• *point 1 :*

Comme Δ est d'ordre étranger à p, $H^i(\Delta, M)(\mathfrak{p})$ est trivial pour tout Δ-module M. Les suites d'inflation-restriction donnent l'isomorphisme suivant : $S_{F_\infty} \simeq S_{\mathcal{F}_\infty}^{\Delta}$. De même on a $S_{L_\infty} \simeq S_{\mathcal{L}_\infty}^{\Delta}$. On se ramène donc au cas où $E_\mathfrak{p} \subset E(F)$.

Les mêmes arguments montrent que $S_{L_\infty}^H$ est isomorphe à $S_{L_\infty^H}$ pour H sous-groupe de G d'ordre étranger à p.

En prenant le p-Sylow de G, on se ramène au cas d'une p-extension galoisienne. De plus, un p-groupe étant résoluble il admet une suite de résolution de Jordan-Hölder à quotients cycliques d'ordre p. On peut donc supposer G cyclique d'ordre p.

• *point 2 :*

A nouveau les morphismes Inf et Res conduisent au diagramme suivant :

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \mathrm{Ker}\imath & & H^1(G, E_{\mathfrak{p}^\infty}) & & \mathcal{K}(\mathfrak{p}) \\
 & & \downarrow & & \mathrm{Inf}\downarrow & & \mathrm{Inf}\downarrow \\
0 & \longrightarrow & S_{F_\infty} & \longrightarrow & H^1(F_\infty, E_{\mathfrak{p}^\infty}) & \longrightarrow & \prod_{v\dagger\mathfrak{p}} H^1(F_{\infty,v}, E)(\mathfrak{p}) \\
 & & \imath\downarrow & & \mathrm{Res}\downarrow & & \mathrm{Res}\downarrow \\
0 & \longrightarrow & S_{F_\infty}^G & \longrightarrow & H^1(L_\infty, E_{\mathfrak{p}^\infty})^G & \longrightarrow & \prod_{v\dagger\mathfrak{p}} H^1(L_{\infty,v}, E)(\mathfrak{p})^G \\
 & & \downarrow & & \downarrow & & \\
 & & \mathrm{Coker}\imath & & H^2(G, E_{\mathfrak{p}^\infty}) & & \\
 & & \downarrow & & & & \\
 & & 0 & & & &
\end{array}$$

avec $\mathcal{K}(\mathfrak{p}) = \prod_{v\dagger\mathfrak{p}} H^1(\mathrm{Gal}(L_{\infty,v}/F_{\infty,v}), E(L_{\infty,v}))(\mathfrak{p})$.

La restriction induit un morphisme $\imath$, de S_{F_∞} vers $S_{L_\infty}^G$, à noyau fini en raison du lemme 3 et de la commutativité du carré.

Il s'agit donc de montrer que Coker$\imath$ est un groupe fini.

Le lemme 3, à nouveau, affirme que $H^i(G, E_{\mathfrak{p}^\infty})$ est fini, pour i=1 ou 2. Par le diagramme du serpent , on est ramené à démontrer que $\prod_{v \nmid \mathfrak{p}} H^1(\mathrm{Gal}(L_{\infty,v}/F_{\infty,v}), E(L_{\infty,v}))(\mathfrak{p})$ est fini.

La trivialité de $H^1(\mathrm{Gal}(L_{\infty,v}/F_{\infty,v}), E(L_{\infty,v}))(\mathfrak{p})$ est donnée, par passage à la limite, par les résultats de [Mz], (pp 203 et 204) lorsque v est non ramifiée.

Compte tenu des règles de ramifications dans une $\mathbb{Z}_p$-extension, v est ramifiée dans L_∞/F_∞ si et seulement si elle l'est dans L_n/F_n pour n suffisamment grand (ou du moins la restriction de v). En conséquence il n'y a qu'un nombre fini de telles places au-dessus de $\mathfrak{p}$ dans L_∞/F_∞. Dans ce cas $\mathrm{Gal}(L_{\infty,v}/F_{\infty,v})$ s'identifie à G. Il suffit donc de montrer que $H^1(G, E(L_{\infty,v}))(\mathfrak{p})$ est fini, avec v (totalement) ramifiée. En particulier, on a $(v,p) = 1$. De la suite exacte :

$$0 \to E(L_{\infty,v})_{\pi^n} \to E(L_{\infty,v}) \to \mathrm{Im}\pi^n \to 0$$

on tire la suite de cohomologie

$$0 \to E(F_{\infty,v})/\pi^n E(F_{\infty,v}) \to H^1(G, E(L_{\infty,v})_{\pi^n}) \to H^1(G, E(L_{\infty,v}))_{\pi^n} \to 0.$$

On a donc une flèche surjective de $H^1(G, E(L_{\infty,v}) \cap E_{\mathfrak{p}^\infty})$ vers $H^1(G, E(L_{\infty,v}))(\mathfrak{p})$. Il suffit donc de montrer que ce premier goupe est fini.

Comme E a bonne réduction sur F ([Co] Lemme 5), $E(L_{\infty,v}) \cap E_{\mathfrak{p}^\infty}$ s'injecte dans $E(f_{\infty,v})$, où $f_{\infty,v}$ est la $\mathbb{Z}_p$-extension du corps résiduel de F_v, disons $f_v \simeq \mathbb{F}_q$, où $q = \ell^n$ et $\ell \neq p$ (car v est non ramifiée). En particulier on a $E(L_{\infty,v}) \cap E_{\mathfrak{p}^\infty} \hookrightarrow E(\overline{\mathbb{F}_\ell})$.

Comme $E(L_{\infty,v}) \cap E_{\mathfrak{p}^\infty}$ est un p-groupe, il s'identifie à un sous-groupe du $\mathbb{Z}_p$-module divisible de cotype fini $(\mathbb{Q}_p/\mathbb{Z}_p)^2$. On conclut en utilisant les arguments du lemme 3.

On a donc établi la première partie du lemme, i.e. l'existence d'un pseudo-isomorphisme de S_{F_∞} vers $S^G_{L_\infty}$.

• *point 3 :*

Maintenant, on considère la suite exacte :

$$0 \longrightarrow \mathrm{Ker}\imath \longrightarrow S_{F_\infty} \longrightarrow S^G_{L_\infty} \longrightarrow \mathrm{Coker}\imath \longrightarrow 0.$$

On obtient au moyen de la dualité de Pontrjagin, la suite exacte suivante ($\mathbb{Q}_p/\mathbb{Z}_p$ étant $\mathbb{Z}_p$-injectif) :

$$0 \longrightarrow \check{\text{Coker}}\imath \longrightarrow (\check{S}_{L_\infty})_G \xrightarrow{f} \check{S}_{F_\infty} \longrightarrow \check{\text{Ker}}\imath \longrightarrow 0.$$

On constate que $\text{Im}f$ est un sous-réseau de $\check{S}_{F_\infty}$. Donc $\text{Hom}_{\mathbf{Z}_p}(\check{S}_{F_\infty}, \mathbb{Z}_p)$ est un sous-réseau de $\text{Hom}_{\mathbf{Z}_p}(\text{Im}f, \mathbb{Z}_p)$. Il vient alors l'isomorphisme suivant :

$$\text{Hom}_{\mathbf{Z}_p}(\text{Im}f, \mathbb{Z}_p) \otimes_{\mathbf{Z}_p} \mathbb{Q}_p \simeq V_{F_\infty}.$$

On a aussi la suite suivante :

$$0 \longrightarrow \check{\text{Coker}}\imath \longrightarrow (\check{S}_{L_\infty})_G \xrightarrow{f} \text{Im}f \longrightarrow 0.$$

Le noyau de f étant fini, en prenant les formes linéaires entières de ces $\mathbb{Z}_p$-modules on a :

$$\text{Hom}_{\mathbf{Z}_p}((\check{S}_{L_\infty})_G, \mathbb{Z}_p) \simeq \text{Hom}_{\mathbf{Z}_p}(\text{Im}f, \mathbb{Z}_p).$$

Comme de plus

$$\text{Hom}_{\mathbf{Z}_p}((\check{S}_{L_\infty})_G, \mathbb{Z}_p) \simeq \text{Hom}_{\mathbf{Z}_p}(\check{S}_{L_\infty}, \mathbb{Z}_p)^G,$$

il suffit pour démontrer le lemme de savoir que

$$\text{Hom}_{\mathbf{Z}_p}(\check{S}_{L_\infty}, \mathbb{Z}_p)^G \otimes_{\mathbf{Z}_p} \mathbb{Q}_p \simeq (\text{Hom}_{\mathbf{Z}_p}(\check{S}_{L_\infty}, \mathbb{Z}_p) \otimes_{\mathbf{Z}_p} \mathbb{Q}_p)^G.$$

Ce dernier point est clair. D'où le lemme. □

Ces deux derniers lemmes, compte tenu des résultats de [JaMi], permettent de ramener le problème d'une part, au cas où G est cyclique d'ordre p (le cas général se faisant par induction), et d'autre part, à un calcul de rang. Moyennant ce dévissage, la formule de Wingberg est un cas particulier du résultat suivant (loc. cit.) : pour tout $\mathbb{Z}_p[G]$-module M, $\mathbb{Z}_p$-divisible et de cotype fini on a

$$\text{corang}_{\mathbf{Z}_p} M = p \times \text{corang}_{\mathbf{Z}_p} M^G + q(G, M)(p-1)$$

où $q(G, M)$ est le quotient de Herbrand dimensionnel :

$$q(G, S_{L_\infty}) = \dim_{\mathbb{F}_p} H^2(G, S_{L_\infty}) - \dim_{\mathbb{F}_p} H^1(G, S_{L_\infty}).$$

Ceci a un sens au regard du lemme 3.

Au paragraphe suivant, nous calculons donc le quotient $q(G, S_{L_\infty})$ de S_{L_∞} pour l'action de $G = \text{Gal}(L_\infty/F_\infty)$, groupe associé à l'extension galoisienne L_∞/F_∞ de degré p et non ramifiée au dessus de $\overline{\mathfrak{p}}$.

3. Arithmétique du cas cyclique élémentaire : calculs de quotient de Herbrand.

Commençons par rappeler deux propriétés essentielles du quotient de Herbrand :

(i) $q(G,M)=0$ pour tout $\mathbb{Z}_p[G]$-module M fini.

(ii) Pour une suite exacte courte

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

de $\mathbb{Z}_p[G]$-modules, les quotients des trois termes sont définis dès que deux quelconques le sont, auquel cas on a $q(G,N)=q(G,P)+q(G,M)$.

En particulier cela permet de remplacer un $\mathbb{Z}_p[G]$-module par un autre qui lui est pseudo-isomorphe.

Nous avons besoin aussi du résultat dual sur le corang d'un module divisible ci-dessus, pour le rang d'un $\mathbb{Z}_p[G]$-module libre et de type fini :

$$\text{rang}_{\mathbb{Z}_p} M = p \times \text{rang}_{\mathbb{Z}_p} M^G - q(G,M)(p-1). \tag{2}$$

Nous faisons la convention suivante pour alléger les notations : on omettra de considérer, dans les calculs, les χ-composantes des modules considérés. En effet, χ étant un caractère asssocié à Δ d'ordre étranger à p, sur une suite de $\mathbb{Z}_p$-module le foncteur "χ-composante" est exact. Les résultats en revanche sont énoncés dans le cadre du problème.

Sous les conditions arithmétiques de l'énoncé (nullité de l'invariant μ et conjecture faible $\mathfrak{p}$-adique de Leopoldt) on rappelle que $X_{\mathcal{L}_\infty}=\text{Gal}(\mathfrak{M}_{\mathcal{L}_\infty}/\mathcal{L}_\infty)$, où $\mathfrak{M}_{\mathcal{L}_\infty}$ est la p-extension abélienne maximale de $\mathcal{L}_\infty$, non ramifiée en dehors de $\mathfrak{p}$, est un $\mathbb{Z}_p$-module de type fini, projectif (i.e. libre , $\mathbb{Z}_p$ étant un anneau local), de dimension $\lambda_{\mathcal{L}_\infty}$. Remarquons que les hypothèses signifient, en fait, que le p-rang de $\mathcal{C}\ell^0_{\mathcal{L}_n}$, soit $\dim_{\mathbb{F}_p}(\mathcal{C}\ell^0_{\mathcal{L}_n})/(\mathcal{C}\ell^0_{\mathcal{L}_n})^p$, est borné à chaque étage. Enoncées ainsi, on voit que les contraintes arithmétiques sont identiques au cas cyclotomique (alors qu'a priori elles semblaient plus forte dans le cas elliptique).

La théorie d'Iwasawa permet d'écrire $X_{\mathcal{L}_\infty} \simeq Y_{\mathcal{L}_\infty} \oplus Z_{\mathcal{L}_\infty}$, où $Z_{\mathcal{L}_\infty}$ est un Λ-module de torsion, dont la série caractéristique est un produit de polynômes du type :

$$\omega_k = (1+T)^{p^k} - 1,$$

et $Y_{\mathcal{L}_\infty}$ de série caractéristique étranger à ces derniers. Cela signifie, en particulier que $Y_{\mathcal{L}_\infty}/\omega_k Y_{\mathcal{L}_\infty}$ est fini. Notons que $\mathfrak{M}_{\mathcal{L}_n}$ est la p-extension abélienne maximale de $\mathcal{L}_n$, contenue dans $\mathfrak{M}_{\mathcal{L}_\infty}$. On a donc

$$\mathrm{Gal}(\mathfrak{M}_{\mathcal{L}_n}/\mathcal{L}_\infty) \simeq X_{\mathcal{L}_\infty}/\omega_n X_{\mathcal{L}_\infty}.$$

De plus à l'étage n on a la suite exacte :

$$0 \longrightarrow \mathrm{Gal}(\mathfrak{M}_{\mathcal{L}_n}/\mathcal{L}_\infty) \longrightarrow \mathcal{C}\ell^0_{\mathcal{L}_n} \longrightarrow \mathrm{Gal}(\mathcal{L}_\infty/\mathcal{L}_n) \longrightarrow 0.$$

Le membre de droite étant $\mathbb{Z}_p$-projectif, cette suite est scindée, et on a :

$$\mathcal{C}\ell^0_{\mathcal{L}_n} \simeq X_{\mathcal{L}_\infty}/\omega_n X_{\mathcal{L}_\infty} \oplus \mathbb{Z}_p \qquad \text{où } \mathbb{Z}_p \text{ s'identifie à } \mathrm{Gal}(\mathcal{L}_\infty/\mathcal{L}_n).$$

Ce dernier module disparaît par passage à la limite projective, pour les morphismes induits par la norme arithmétique. La théorie du corps de classe interprète $\delta_{\mathcal{L}_\infty}$ comme le rang pour n suffisamment grand de $X_{\mathcal{L}_\infty}/\omega_n X_{\mathcal{L}_\infty}$ modulo sa torsion. La $\mathbb{Z}_p$-torsion de $\mathcal{C}\ell^0_{\mathcal{L}_n}$, $\mathcal{C}\ell^\infty_{\mathcal{L}_n}$, s'identifie à $Y_{\mathcal{L}_\infty}/\omega_n Y_{\mathcal{L}_\infty}$. Il vient donc :

$$\varprojlim_n \mathcal{C}\ell^\infty_{\mathcal{L}_n} \simeq \mathbb{Z}_p{}^{\lambda_{\mathcal{L}_\infty} - \delta_{\mathcal{L}_\infty}}.$$

On note $X^\infty_{\mathcal{L}_\infty}$ ce module.

La limite inductive s'étudie comme suit : pour n suffisamment grand on a le diagramme suivant :

$$\begin{array}{ccccccc}
\mathcal{C}\ell^0_{\mathcal{L}_n} & \simeq & \mathrm{Gal}(\mathcal{L}_\infty/\mathcal{L}_n) & \oplus & Z_{\mathcal{L}_\infty}/\omega_n Z_{\mathcal{L}_\infty} & \oplus & \mathcal{C}\ell^\infty_{\mathcal{L}_n} \\
{\scriptstyle N_{\frac{n+1}{n}}}\downarrow & & \downarrow {\scriptstyle j_{\frac{n+1}{n}}} & & \downarrow {\scriptstyle i_{\frac{n+1}{n}}} & & \downarrow {\scriptstyle k_{\frac{n+1}{n}}} \\
\mathcal{C}\ell^0_{\mathcal{L}_{n+1}} & \simeq & \mathrm{Gal}(\mathcal{L}_\infty/\mathcal{L}_{n+1}) & \oplus & Z_{\mathcal{L}_\infty}/\omega_{n+1} Z_{\mathcal{L}_\infty} & \oplus & \mathcal{C}\ell^\infty_{\mathcal{L}_{n+1}}
\end{array}$$

où $j_{\frac{n+1}{n}}$ est induite par l'extension des diviseurs, et $N_{\frac{n+1}{n}}$ par la norme arithmétique. Le morphisme $i_{\frac{n+1}{n}}$, restriction de $j_{\frac{n+1}{n}}$ au terme de gauche, est clairement surjectif. Le morphisme $k_{\frac{n+1}{n}}$, restriction de $j_{\frac{n+1}{n}}$ au terme de droite, est défini comme suit : à une classe $x \bmod \omega_n$, on associe la classe de $\dfrac{\omega_{n+1}}{\omega_n} x \bmod \omega_{n+1}$. Par un lemme classique de théorie d'Iwasawa (voir par exemple [Wa] Ch XIII § 8), $\dfrac{\omega_{n+1}}{\omega_n}$ opère, à un inversible de l'algèbre $\mathbb{Z}_p[\gamma - 1]$ près, comme la multiplication par p. Donc, pour la limite inductive prise pour les $j_{\frac{n+1}{n}}$, on a

$$\mathcal{C}\ell^0_{\mathcal{L}_\infty} \simeq \mathcal{C}\ell^\infty_{\mathcal{L}_\infty} \oplus \mathbb{Z}_p. \tag{3}$$

De plus, les ω_n étant étrangers au polynôme caractéristique de $Y_{\mathcal{L}_\infty}$, ils forment, pour ce module, un système admissible (au sens d' Iwasawa). Il vient donc ([Iw2] p. 250) :

$$Y_{\mathcal{L}_\infty} \sim \mathrm{Hom}_{\mathbf{Z}_p}(\varinjlim_n Y_{\mathcal{L}_\infty}/\omega_n Y_{\mathcal{L}_\infty}, \mathbb{Q}_p/\mathbb{Z}_p). \tag{4}$$

Soit encore :

$$\mathcal{C}\ell^\infty_{\mathcal{L}_\infty} \simeq \varinjlim_n Y_{\mathcal{L}_\infty}/\omega_n Y_{\mathcal{L}_\infty} \sim (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_{L_\infty}-\delta_{\mathcal{L}_\infty}}. \tag{5}$$

De ce qui précède, il vient : $\mathcal{C}\ell^\infty_{\mathcal{L}_\infty}$, comme $\mathbb{Z}_p[G]$-module pseudo-isomorphe à un $\mathbb{Z}_p$-module divisible et de cotype fini, d'après (1) vérifie :

$$\lambda_{\mathcal{L}_\infty} - \delta_{\mathcal{L}_\infty} = (\lambda_{\mathcal{F}_\infty} - \delta_{\mathcal{F}_\infty})p + (p-1)q(G, \mathcal{C}\ell^\infty_{\mathcal{L}_\infty}). \tag{6}$$

De (3) il vient :

$$q(G, \mathcal{C}\ell^\infty_{\mathcal{L}_\infty}) = q(G, \mathcal{C}\ell^0_{\mathcal{L}_\infty}) - 1. \tag{7}$$

Comme $\mathcal{E}^\infty_{\mathcal{L}_\infty}$ est un $\mathbb{Z}_p$-module libre, de type fini et de rang $\delta_{\mathcal{L}_\infty}$, d'après (2) on a :

$$\delta_{\mathcal{L}_\infty} = p\delta_{\mathcal{F}_\infty} - (p-1)q(G, \mathcal{E}^\infty_{\mathcal{L}_\infty}). \tag{8}$$

En sommant membre à membre (6), (7) et (8), on obtient :

$$\lambda_{\mathcal{L}_\infty} = p\lambda_{\mathcal{F}_\infty} + (p-1)(q(G, \mathcal{C}\ell^0_{\mathcal{L}_\infty}) - q(G, \mathcal{E}^\infty_{\mathcal{L}_\infty}) - 1). \tag{9}$$

Revenons à la situation du problème : regardons les χ-composantes.

On a $X^\chi_{\mathcal{L}_\infty} \simeq \mathbb{Z}_p^{\lambda_{L_\infty}}$ et $(X^\infty_{\mathcal{L}_\infty})^\chi \simeq \mathbb{Z}_p^{\lambda_{L_\infty}-\delta_{L_\infty}}$.

On a montré ci-dessus que $X^\infty_{\mathcal{L}_\infty}$ est pseudo-dual de $\mathcal{C}\ell^\infty_{\mathcal{L}_\infty}$.

Le caractère χ étant étranger à p, les arguments précédents conduisent au pseudo-isomorphisme de $\mathbb{Z}_p$-modules suivant :

$$(X^\infty_{\mathcal{L}_\infty})^\chi \sim \mathrm{Hom}_{\mathbf{Z}_p}\left((\mathcal{C}\ell^\infty_{\mathcal{L}_\infty})^\chi, \mathbb{Q}_p/\mathbb{Z}_p\right).$$

Il vient donc :

$$(\mathcal{C}\ell^\infty_{\mathcal{L}_\infty})^\chi \sim (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_{L_\infty}-\delta_{L_\infty}},$$

où δ_{L_∞} est le rang de la χ-composante de $\mathcal{E}^\infty_{\mathcal{L}_\infty}$. De la même façon on montre que le corang de $(\mathcal{C}\ell^\infty_{\mathcal{F}_\infty})^\chi$ est $\lambda_{F_\infty} - \delta_{F_\infty}$.

On remarquera qu'on ne cherche pas à comparer les structures de G-modules des différents objets considérés. Cela est d'une part inutile pour établir des égalités entre dimensions (voir II.3), et d'autre part plus délicat, la dualité de Pontrjagin tordant l'action galoisienne.

En conclusion on a encore :

$$\lambda_{L_\infty} = p\lambda_{F_\infty} + (p-1)(q(G,(\mathcal{C}\ell^0_{\mathcal{L}_\infty})^\chi) - q(G,(\mathcal{E}^\infty_{\mathcal{L}_\infty})^\chi) - 1). \tag{9bis}$$

Il faut donc calculer $q(G,(\mathcal{C}\ell^0_{\mathcal{L}_\infty})^\chi) - q(G,(\mathcal{E}^\infty_{\mathcal{L}_\infty})^\chi)$. La suite exacte

$$0 \longrightarrow \mathcal{E}^\infty_{\mathcal{L}_\infty} \longrightarrow \mathcal{R}^\infty_{\mathcal{L}_\infty} \longrightarrow \mathcal{D}^0_{\mathcal{L}_\infty} \longrightarrow \mathcal{C}\ell^0_{\mathcal{L}_\infty} \longrightarrow 0$$

donne :

$$q(G,(\mathcal{C}\ell^0_{L_\infty})^\chi) - q(G,(\mathcal{E}^\infty_{\mathcal{L}_\infty})^\chi) = q(G,(\mathcal{D}^0_{\mathcal{L}_\infty})^\chi) - q(G,(\mathcal{R}^\infty_{\mathcal{L}_\infty})^\chi).$$

On a les lemmes suivants :

LEMME 5. — $q(G,(\mathcal{D}^0_{\mathcal{L}_\infty})^\chi) = t^\chi$, *où* t^χ *est le nombre de premiers de* $\mathcal{F}_\infty$ *étrangers à* $\mathfrak{p}$, *ramifiés dans* $\mathcal{L}_\infty/\mathcal{F}_\infty$ *et décomposés dans* $\mathcal{F}_\infty/F_\infty$.

Démonstration

• *point 1 :* $H^1(G,\mathcal{D}^0_{\mathcal{L}_\infty}) = 1$. En effet, on a

$$\mathcal{D}^0_{\mathcal{L}_\infty} = \bigoplus_{\mathfrak{P}_\infty \dagger \mathfrak{p}} \mathfrak{P}_\infty^{\mathbf{Z}_p},$$

la somme étant prise sur les premiers de $\mathcal{L}_\infty$ étrangers à $\mathfrak{p}$. Ou bien le groupe de décomposition, $G_{\mathfrak{P}_\infty}$, de $\mathfrak{P}_\infty$ dans $\mathcal{L}_\infty/\mathcal{F}_\infty$ est trivial, ou bien c'est G. Dans les deux cas on a, par le lemme de Shapiro

$$H^1(G,\mathcal{D}^0_{\mathcal{L}_\infty}) = \bigoplus_{\mathfrak{P}_\infty \dagger \mathfrak{p}} H^1(G_{\mathfrak{P}_\infty}, \mathfrak{P}_\infty^{\mathbf{Z}_p}) = 1,$$

la somme directe dans le terme central étant prise sur un système de représentants des orbites des diviseurs, pour l'action de G.

•*point 2 :* $H^2(G,\mathcal{D}^0_{\mathcal{L}_\infty}) \simeq \bigoplus_{\mathfrak{P}_\infty \dagger \mathfrak{p}} \mathbb{Z}/e_\infty\mathbb{Z}$, la somme portant sur les premiers de $\mathcal{F}_\infty$ ramifiés dans $\mathcal{L}_\infty/\mathcal{F}_\infty$ et e_∞ étant l'indice de ramification. Les règles de ramification dans une $\mathbb{Z}_p$-extension assurent que la somme précédente est bien finie.

En effet, G étant cyclique, engendré par, disons σ, on a l'isomorphisme suivant :

$$H^2(G, \mathcal{D}^0_{\mathcal{L}_\infty}) \simeq \frac{(\mathcal{D}^0_{\mathcal{L}_\infty})^G}{\nu_{\mathcal{L}_\infty/\mathcal{F}_\infty}(\mathcal{D}^0_{\mathcal{L}_\infty})} \tag{10}$$

où $\nu_{\mathcal{L}_\infty/\mathcal{F}_\infty} = \sum_{i=0}^{p-1} \sigma^i$ est la norme algébrique.

Cette dernière peut être remplacée par la norme arithmétique, en identifiant les diviseurs de $\mathcal{F}_\infty$ avec leurs étendus à $\mathcal{L}_\infty$, tout diviseur de $\mathcal{F}_\infty$ étant norme, (car sans inertie), le dénominateur dans (10) est $\mathcal{D}^0_{\mathcal{F}_\infty}$. Comme les diviseurs ambiges, étrangers à $\mathfrak{p}$, sont engendrés par les étendus et les ramifiés on a le deuxième point.

• *point 3 :* Les hypothèses de bonne réduction imposent à $\mathcal{L}/L$ d'être non ramifiée en dehors de $\mathfrak{p}$. Il en est de même pour $\mathcal{L}_\infty/L_\infty$. Donc le nombre de ramifiés étrangers à $\mathfrak{p}$ dans $\mathcal{L}_\infty/\mathcal{F}_\infty$ est égal au nombre de ramifiés étrangers à $\mathfrak{p}$ dans L_∞/F_∞. D'où le lemme en prenant les χ-composantes. □

LEMME 6. — *On a* $q(G, (\mathcal{R}_{\mathcal{L}_\infty})^\chi) = 0$.

Démonstration. — On montre en fait $q(G, (\mathcal{R}_{\mathcal{L}_\infty})) = 0$. Le premier groupe de cohomologie $H^1(G, \mathcal{R}_{\mathcal{L}_\infty})$ est nul ; c'est une conséquence facile du théorème 90 de Hilbert, par passage à la limite inductive. La trivialité de $H^2(G, \mathcal{R}_{\mathcal{L}_\infty})$ signifie, G étant cyclique, que la norme est surjective : on vérifie qu'un élément global est norme locale partout, à l'aide des symboles de Hasse ([Ja2]). D'où le lemme. □

Le lemme précédent et la suite exacte :

$$0 \longrightarrow \mathcal{R}^\infty_{\mathcal{L}_\infty} \longrightarrow \mathcal{R}_{\mathcal{L}_\infty} \longrightarrow \varinjlim_n \widehat{\mathcal{L}}^\times_{n,\mathfrak{p}} \longrightarrow 0,$$

donnent : $q(G, (\mathcal{R}^\infty_{\mathcal{L}_\infty})^\chi) = -q(G, (\varinjlim_n \widehat{\mathcal{L}}^\times_{n,\mathfrak{p}})^\chi)$.

Ceci permet d'énoncer le lemme suivant :

LEMME 7. — *On a* $q(G, (\mathcal{R}^\infty_{\mathcal{L}_\infty})^\chi) = \begin{cases} 0 & \text{si } L_\infty(E_\mathfrak{p}) = L_\infty \\ 1 & \text{sinon.} \end{cases}$

Démonstration. — Pour tout n, $\mathrm{Gal}(\mathcal{L}_n/\mathcal{F}_n)$ s'identifie à G, et opère sur l'algèbre semi-locale $\widehat{\mathcal{L}}^\times_{n,\mathfrak{p}} = \prod_{v|\mathfrak{p}} \widehat{\mathcal{L}}^\times_{n,v}$. Par le lemme de Shapiro, on a :

Pour $i = 1, 2$ $H^i(G, \widehat{\mathcal{L}}^\times_{n,\mathfrak{p}}) \simeq H^i(G, \widehat{\mathcal{L}}^\times_{n,v})$ pour un v divisant $\mathfrak{p}$ quelconque.

On a par le théorème 90 de Hilbert $H^1(G, \widehat{\mathcal{L}}^\times_{n,v}) = 1$.

Pour $i = 2$ on a :

$$H^2(G, \widehat{\mathcal{L}}^\times_{n,v}) \simeq \frac{\widehat{\mathcal{F}}^\times_{n,v}}{\nu_{\mathcal{L}_{n,v}/\mathcal{F}_{n,v}}(\widehat{\mathcal{L}}^\times_{n,\mathfrak{p}})}$$

où $\nu_{\mathcal{L}_{n,v}/\mathcal{F}_{n,v}}$ est l'opérateur norme algébrique.

Ce dernier quotient s'interprète, par la théorie du corps de classes, comme le groupe de l'extension locale $\mathcal{L}_{n,v}/\mathcal{F}_{n,v}$; elle est triviale ou de degré p. Par restriction à la χ-composante on obtient le lemme. □

Démonstration du théorème 1. — On pose $\epsilon = 1$ si $E_\mathfrak{p} \subset E(F), 0$ sinon. Les lemmes 5, 6 et 7, et l'égalité (9) donnent le théorème 1. □

Remarque. — L'extension L/F est une p-extension et $\mathcal{F}/F$ est de degré premier à p. La condition $E_\mathfrak{p} \subset E(F)$ peut donc identiquement se lire aussi : $E_\mathfrak{p} \subset E(L)$, $E_\mathfrak{p} \subset E(L_\infty)$ ou encore $E_\mathfrak{p} \subset E(F_\infty), E_{\mathfrak{p}^\infty} \subset E(L_\infty), E_{\mathfrak{p}^\infty} \subset E(F_\infty)$. De même, la totale décomposition d'une place s'exprime indifféremment pour $\mathcal{L}/L$ ou $\mathcal{F}/F$.

III. UNE SITUATION NON GALOISIENNE

On dit qu'un groupe G d'ordre pn est métacyclique, s'il s'écrit comme le produit direct de son p-groupe de Sylow, disons S, d'ordre p, par un groupe cyclique T, d'ordre n divisant $p - 1$. La loi de G détermine un homomorphisme de T dans $\mathrm{Aut}S$ qui se factorise via un caractère p-adique ψ de T, qui vérifie l'identité suivante :

$$\tau\sigma\tau^{-1} = \sigma^{\psi(\tau)} \text{ pour tout } \tau \in T, \text{ où } \sigma \text{ est un générateur de } S.$$

L'extension considérée, L_∞/F_∞, est toujours de degré p. En revanche, on ne la suppose plus nécessairement galoisienne. Cependant, on demande que la clôture normale N_∞ de L_∞/F_∞ soit à groupe de Galois $G = \mathrm{Gal}(N_\infty/F_\infty)$ métacyclique. Avec les notations précédentes, on a $T =$

$\mathrm{Gal}(N_\infty/L_\infty)$. On note H_∞, l'unique sous-extension de N_∞ fixée par S, et communément appelée arête métacyclique.

Le groupe des caractères irréductibles p-adiques de T sera noté T^*, 1_T étant le caractère unité.

En outre, E désigne toujours une courbe elliptique satisfaisant les hypothèses de I.1. On associe à N_∞ (*resp.* H_∞), les corps $\mathcal{N}, \mathcal{N}_\infty$ et N, (*resp.* $\mathcal{H}, \mathcal{H}_\infty$ et H).

Les $\mathbb{Z}_p$-extensions considérées satisfont l'hypothèse faible $\mathfrak{p}$-adique de Leopoldt. De plus, N_∞/H_∞ est non ramifiée au-dessus de $\overline{\mathfrak{p}}$.

LEMME 8. — *Si $\mu_{\mathcal{H}_\infty}$ est nul, alors $\mu_{\mathcal{N}_\infty}, \mu_{\mathcal{F}_\infty}$ et $\mu_{\mathcal{L}_\infty}$ le sont aussi.*

Remarque. — Ce résultat assure que le groupe de Selmer d'un quelconque sous-corps considéré est un $\mathbb{Z}_p$-module divisible et de cotype fini, dès que celui associé à H_∞ l'est.

Démonstration. — On oublie, comme précédemment, d'écrire la χ-composante des modules considérés.

Soit $\varphi \in T^*$. On lui associe l'idempotent $e_\varphi = \dfrac{1}{n} \sum_{\tau \in T} \varphi(\tau^{-1})\tau$. Comme n divise $p-1$, tout $\mathbb{Z}_p[T]$-module M s'écrit comme la somme directe (orthogonale) de ses φ-composantes $M^\varphi = e_\varphi M$, image de M par le projecteur e_φ. Si on applique cela à $X_{\mathcal{N}_\infty}$, on a, avec des notations claires :

$$\mu_{\mathcal{N}_\infty} = \sum_{\varphi \in T^*} \mu^\varphi_{\mathcal{N}_\infty}. \tag{11}$$

Soit $\mathcal{N}'_n$ un sous-corps de $\mathcal{N}_n$ contenant $\mathcal{L}_n$. On note T' le sous-groupe de T qui lui correspond par la théorie de Galois. Posons $|T'| = n'$ et φ' l'induit à T du caractère unité de T'. Alors $C\ell^0_{\mathcal{N}'_n}$ s'identifie à la φ'-partie de $C\ell^0_{\mathcal{N}_n}$. En effet, la norme $\nu_{\mathcal{N}_n/\mathcal{N}'_n}$ est, à un inversible près de $\mathbb{Z}_p[T]$, le projecteur $e' = \dfrac{1}{n} \sum_{\tau \in T'} \tau$, qui induit l'identité sur $C\ell^0_{\mathcal{N}'_n}$. En particulier, on a :

$$C\ell^0_{\mathcal{L}_n} \simeq (C\ell^0_{\mathcal{N}_n})^{1_T}.$$

Pour tous $m \geqslant n$ et pour tout $\varphi \in T^*$, il est facile de voir que e_φ et $\nu_{\mathcal{N}_m/\mathcal{N}_n}$ commutent. On en déduit :

$$\varprojlim_n (C\ell^0_{\mathcal{N}_n})^\varphi \simeq (\varprojlim_n C\ell^0_{\mathcal{N}_n})^\varphi \simeq \mathrm{Gal}(\mathfrak{M}_{\mathcal{N}_\mathfrak{p}}/\mathcal{N}_\infty) \simeq (X_{\mathcal{N}_\infty})^\varphi.$$

D'où, en spécialisant en $\varphi = 1_T$, on obtient :

$$(X_{\mathcal{N}_\infty})^{1_T} \simeq X_{\mathcal{L}_\infty}.$$

Il vient donc, en particulier,

$$(\mu_{\mathcal{N}_\infty})^{1_T} = \mu_{\mathcal{L}_\infty}, \tag{12}$$

et de la même façon :

$$(\mu_{\mathcal{H}_\infty})^{1_T} = \mu_{\mathcal{F}_\infty}. \tag{13}$$

En appliquant le lemme 2 à l'extension cyclique N_∞/H_∞, on a : $\mu_{\mathcal{H}_\infty} = 0$ implique $\mu_{\mathcal{N}_\infty} = 0$. On conclut au moyen de (11), (12) et (13). □

Dans ce contexte, on énonce une généralisation de la formule de Wingberg, qui est l'analogue de la formule de Gold et Madan donnée dans [GoMa], pour le cas cyclotomique.

THÉORÈME 3. — *Soit L_∞/F_∞ une extension de degré p. Supposons que $\mathrm{Gal}(N_\infty/F_\infty)$, le groupe de Galois de la clôture normale N_∞, de L_∞ sur F_∞, soit métacyclique. Avec les notations ci-dessus, sous réserve de la nullité de l'invariant $\mu_{\mathcal{H}_\infty}$, les corangs des φ-composantes des groupes de Selmer, associés aux différents sous-corps, pour $\varphi \in T^*$, sont donnés par la formule :*

$$\lambda^{\varphi}_{N_\infty} = \lambda^{\varphi}_{H_\infty} + \frac{p-1}{[N_\infty : L_\infty]}(\lambda_{H_\infty} + t_{N_\infty/H_\infty} - \epsilon)$$

où $\epsilon = 1$ si $E_{\mathfrak{p}} \subset E(H)$ et 0 sinon, t_{N_∞/H_∞} est le nombre de premiers étrangers à p, ramifiés dans N_∞/H_∞ et totalement décomposés dans $H(E_{\mathfrak{p}})/H$.

Remarque. — En regard des arguments du lemme 8 et de l'interprétation du groupe de Selmer comme dual (de la φ-composante) d'un groupe de Galois, la spécialisation en $\varphi = 1_T$ de la formule du théorème donne :

$$\lambda_{L_\infty} = \lambda_{F_\infty} + \frac{p-1}{[N_\infty : L_\infty]}(\lambda_{H_\infty} + t_{N_\infty/H_\infty} - \epsilon).$$

Ceci est bien une formule analogue à celle de [GoMa].

Si, de plus on suppose L_∞ galoisienne sur F_∞, alors $H_\infty = F_\infty$ et on retrouve la formule de Wingberg.

Le corollaire qui suit généralise le résultat au cas où L_∞/F_∞ est de degré une puissance de p. Il s'obtient essentiellement par empilement d'extensions élémentaires.

COROLLAIRE. — *Soit L_∞/F_∞ une extension de degré p^s et N_∞/F_∞ sa clôture normale. On suppose que $\mathrm{Gal}(N_\infty/F_\infty)$ s'écrit comme produit semi-direct de son p-groupe de Sylow S par le sous-groupe $T = \mathrm{Gal}(N_\infty/L_\infty)$, avec action fidèle sur les quotients de Jordan-Hölder d'une suite sous-normale de S (condition de simplicité). Notons $H_\infty = {N_\infty}^S$. Moyennant les hypothèses arithmétiques précédentes, les corangs des φ-composantes des groupes de Selmer sont donnés par :*

$$\lambda^{\varphi}_{N_\infty} = \lambda^{\varphi}_{H_\infty} + \frac{p^s - 1}{[N_\infty : L_\infty]}(\lambda_{H_\infty} - \epsilon) + \sum_{v \nmid \mathfrak{p}}^{\times} \frac{e_v - 1}{[N_\infty : L_\infty]}$$

où ϵ a la signification précédente, e_v étant l'indice de ramification de v dans N_∞/L_∞, et $\times$ signifiant que la somme est restreinte aux seuls premiers totalement décomposés dans $H(E_\mathfrak{p})/H$.

Démonstration du théorème 3. — La preuve est identique à celle du cas cyclotomique, voir l'appendice de [JaMi] ; on explique comment passer du cas cyclique au cas métacyclique de façon purement algébrique, l'arithmétique n'ayant aucune part dans la démonstration. □

Compte tenu des analogies rencontrées avec les formules relatives à l'invariant d'Iwasawa "classique", on peut espérer obtenir une démonstration au moyen de fonctions L p-adiques de ce résultat.

IV. APPENDICE : REMARQUES SUR CERTAINES RELATIONS ENTRE INVARIANTS LAMBDA ASSOCIÉS AUX GROUPES DE SELMER

Dans ce paragraphe, un corps de nombre H vérifie les conditions de I.1. On lui associe toujours les corps $\mathcal{H}, \mathcal{H}_\infty, H_\infty$. L'hypothèse faible de Leopoldt est supposée satisfaite. Sous cette condition X_{H_∞} étant de Λ-torsion et noethérien, S_{H_∞} s'écrit comme la somme directe de $(\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_{H_\infty}}$ et d'un $\mathbb{Z}_p$-module d'exposant borné qui est trivial si et seulement si $\mu_{\mathcal{H}_\infty}$ est nul. Dans un premier temps on n'impose pas la nullité de cet invariant.

Nous énonçons trois propositions. La première est un analogue d'un théorème de Kani ([Ka]) pour les courbes algébriques, où le genre (ou

l'invariant de Hasse-Witt) joue le rôle de l'invariant λ_{H_∞}. Les propositions 2 et 3 sont des analogues de deux résultats de Accola sur les surfaces de Riemann ([Ac]). Madan et Zimmer ont établi le pendant de ces relations pour les invariants lambda classiques d'Iwasawa ([MaZi]).

PROPOSITION 1. — *Soit L_∞/F_∞ une extension galoisienne finie. Notons $N_{\infty,i}$ pour $0 \leqslant i \leqslant t$ les sous-corps intermédiaires et $H_i = \mathrm{Gal}(L_\infty/N_{\infty,i})$. On pose*

$$e_{H_i} = \frac{1}{|H_i|} \sum_{\tau \in H_i} \tau.$$

Si on a $\sum_{i=1}^{t} r_i e_{H_i} = 0$ les r_i étant dans $\mathbb{Q}$, il suit $\sum_{i=1}^{t} r_i \lambda_i = 0$, où λ_i est le corang du groupe de Selmer associé à $N_{\infty,i}$.

On pose $\mathcal{A}_k^t = \{\iota_k = (i_1, ...i_k) | 1 \leqslant i_1 < i_2 < ... < i_k < ... \leqslant t\}$.

PROPOSITION 2. — *Soit L_∞/F_∞ une extension galoisienne finie. Si $H_1, H_2, ..., H_t$ sont des sous-groupes de $G = \mathrm{Gal}(L_\infty/F_\infty)$ satisfaisant $G = \bigcup_{i=1}^{t} H_i$, alors on a :*

$$|G|\lambda_{F_\infty} = \sum_{k=1}^{t} (-1)^{k+1} \sum_{\iota_k \in \mathcal{A}_k^t} |\cap H_{\iota_k}| \lambda_{\iota_k},$$

où λ_{ι_k} est le corang associé au compositum des $\mathcal{N}_{\infty,i_1}, ..., \mathcal{N}_{\infty,i_k}$ avec $\iota_k = (i_1, ..., i_k)$ et $\cap H_{\iota_k} = H_{i_1} \cap ... \cap H_{i_k}$.

PROPOSITION 3. — *Soit L_∞/F_∞ une extension galoisienne finie. Si $H_1, H_2, ..., H_t$ sont des sous-groupes de $G = \mathrm{Gal}(L_\infty/F_\infty)$ satisfaisant :*

(i) *$H_i H_j = H_j H_i$ pour $i \neq j$.*

(ii) *Pour tout caractère φ de G, il existe $i \in \{1, ..., t\}$ tel que $H_i \subset \mathrm{Ker}\varphi$.*

Notons $N_{\infty,i}$ pour $0 \leqslant i \leqslant t$ les sous-corps intermédiaires et $H_i = \mathrm{Gal}(L_\infty/N_{\infty,i})$.

Alors

$$\lambda_{L_\infty} = \sum_{k=1}^{t} (-1)^{k+1} \sum_{\iota_k \in \mathcal{A}_k^t} \lambda_{\cap \iota_k},$$

où $\lambda_{\cap \iota_k}$ est le corang du groupe de Selmer associé à $N_{\infty,i_1} \cap ... \cap N_{\infty,i_k}$ avec $\iota_k = (i_1, ..., i_k)$.

Démonstration. — Nous adaptons et simplifions la méthode de [MaZi]. Ainsi nous mettons en évidence l'aspect "fonctoriel" de ces formules.

En fait ces trois énoncés ne sont que la traduction en terme de dimension de relations de $\mathbb{Q}$-dépendance linéaire entre idempotents. Il s'agit de construire un caractère de G dont la valeur sur un idempotent est relié à l'invariant lambda.

On se donne N_∞ une sous-extension quelconque de L_∞/F_∞, on note $H = \mathrm{Gal}(L_\infty/N_\infty)$.

Soit le foncteur $M \to W(M) = \mathrm{Hom}_{\mathbf{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbf{Z}_p} \mathbb{Q}_p$ de la catégorie des $\mathbb{Z}_p$-modules de torsion dans la catégorie des $\mathbb{Q}_p$-espaces vectoriels. Il est exact et contravariant, nul sur les $\mathbb{Z}_p$-modules d'exposant fini. (p 273 [Iw2]).

Revenons un instant sur le diagramme commutatif du lemme 4. La restriction induit la suite exacte suivante :

$$0 \longrightarrow A_{N_\infty} \longrightarrow S_{N_\infty} \xrightarrow{\imath} S_{L_\infty}^H \longrightarrow B_{N_\infty} \longrightarrow 0,$$

où A_{N_∞} et B_{N_∞} sont des $\mathbb{Z}_p$-modules d'exposant fini. On notera que l'ordre de G étant quelconque $\imath$ n'est plus a priori un pseudo-isomorphisme. En appliquant W on obtient l'isomorphisme $W(S_{N_\infty}) \simeq W(S_{L_\infty}^H)$. Or $\mathbb{Q}_p/\mathbb{Z}_p$ étant $\mathbb{Z}_p$-injectif on a :

$$\mathrm{Hom}_{\mathbf{Z}_p}(S_{L_\infty}^H, \mathbb{Q}_p/\mathbb{Z}_p) \simeq \mathrm{Hom}_{\mathbf{Z}_p}(S_{L_\infty}, \mathbb{Q}_p/\mathbb{Z}_p)_H.$$

En remarquant que :

$$\mathrm{Hom}_{\mathbf{Z}_p}(S_{L_\infty}, \mathbb{Q}_p/\mathbb{Z}_p)_H \otimes_{\mathbf{Z}_p} \mathbb{Q}_p \simeq (\mathrm{Hom}_{\mathbf{Z}_p}(S_{L_\infty}, \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbf{Z}_p} \mathbb{Q}_p)_H$$

et que $\mathbb{Q}_p$ est de caractéristique nulle, le théorème de Maschke donne :

$$W(S_{L_\infty^H}) \simeq W(S_{L_\infty})^H,$$

c'est-à-dire que les espaces W vérifient la théorie de Galois.

On note Ψ le caractère de G associé à $W(S_{L_\infty})$ et $< \ , \ >_H$ le produit scalaire usuel sur les caractères de H. La construction de Ψ est indépendante de H : ceci n'apparaît pas clairement dans [MaZi].

Soit e_H l'idempotent associé à H. On a clairement que $\Psi(e_H) = < 1_H, \Psi_{|H} >_H$. Ceci n'est autre que la dimension sur $\mathbb{Q}_p$ du sous-espace des points fixes par H de $W(S_{L_\infty})$ soit, d'après ce qui précède, λ_{N_∞}.

Pour obtenir les différentes propositions, il suffit, pour chacune d'elles, d'appliquer le caractère Ψ à une relation de dépendance $\mathbb{Q}$-linéaire entre idempotents, donnée par les hypothèses. Nous expliquons rapidement pour chacune d'elles, comment on les obtient ; pour plus de détails le lecteur peut consulter [Ka] par exemple.

Pour la première formule c'est clair.

Pour la seconde on considère la norme algébrique $\sum_{h\in H} h = |H|e_H$, associée à un sous-groupe H de G.

On a alors :

$$\sum_{g\in G} g = \sum_{k=1}^{t}(-1)^{k+1} \sum_{g\in \cap H_{\iota_k}} g.$$

Il suffit de faire une sommation partielle sur les éléments de G qui sont contenus exactement dans k sous-groupes parmi les t. D'où la relation :

$$|G|e_G = \sum_{k=1}^{t}(-1)^{k+1} \sum_{\iota_k\in\mathcal{A}_k^t} |\cap H_{\iota_k}|e_{\cap H_{\iota_k}}.$$

Pour la dernière proposition on traduit les hypothèses. Le (i) signifie que pour tous $i, j \in \{1...t\}$ e_{H_i} et e_{H_j} commutent, et que par conséquent un nombre quelconque de ces idempotents commutent.

Le (ii) signifie que tout caractère de G s'annule sur $(1-e_{H_1})...(1-e_{H_t})$, i.e. que ce produit est nul. En développant on obtient une relation de dépendance linéaire sur les idempotents, en remarquant que $e_{H_i}e_{H_j} = e_{H_iH_j}$. □

Maintenant on se place sous la condition de nullité de l'invariant mu, pour chacune des tours considérées. On reprend les notations précédentes.

On considère maintenant :

$$W'_{\mathcal{L}_\infty} = \mathrm{Hom}_{\mathbf{Z}_p}(\mathcal{C}\ell^\infty_{\mathcal{L}_\infty}, \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbf{Z}_p} \mathbb{Q}_p.$$

C'est un $\mathbb{Q}_p[G]$-module de dimension $\lambda_{L_\infty} - \delta_{L_\infty}$ sur $\mathbb{Q}_p$ (II.3) . On définit ainsi un nouveau caractère de G.

L'extension des diviseurs de $\mathcal{N}_\infty$ vers $\mathcal{L}_\infty$ induit un morphisme à noyau et conoyau d'exposant borné de $(\mathcal{C}\ell^\infty_{\mathcal{N}_\infty})^\chi$ vers $\left((\mathcal{C}\ell^\infty_{\mathcal{L}_\infty})^\chi\right)^H$. Les $\mathbb{Q}_p$-espaces W' vérifient aussi la théorie de Galois. En reprenant, point par point, la démonstration précédente on obtient les résultats suivants :

PROPOSITION 1 bis. — *Soit L_∞/F_∞ une extension galoisienne finie. Notons $N_{\infty,i}$ les sous-corps intermédiaires pour $0 \leqslant i \leqslant t$, et $H_i = \mathrm{Gal}(L_\infty/N_{\infty,i})$. On pose*

$$e_{H_i} = \frac{1}{|H_i|} \sum_{\tau \in H_i} \tau.$$

$$\text{Si on a } \sum_{i=1}^{t} r_i e_{H_i} = 0 \text{ avec } r_i \in \mathbb{Q}, \text{ alors } \sum_{i=1}^{t} r_i(\lambda_i - \delta_i) = 0,$$

où λ_i est le corang du groupe de Selmer associé à $N_{\infty,i}$ et δ_i est le $\mathbb{Z}_p$-rang de la la χ-composante du groupe de défaut de Leopoldt dans la tour $\mathcal{N}_{\infty,i}/\mathcal{N}_i$.

PROPOSITION 2 bis. — *Soit L_∞/F_∞ une extension galoisienne finie. Si $H_1, H_2, ..., H_t$ sont des sous-groupes de $G = \mathrm{Gal}(L_\infty/F_\infty)$ satisfaisant $G = \bigcup_{i=1}^{t} H_i$, alors on a :*

$$|G|(\lambda_{F_\infty} - \delta_{F_\infty}) = \sum_{k=1}^{t} (-1)^{k+1} \sum_{\iota_k \in \mathcal{A}_k^t} |\cap H_{\iota_k}|(\lambda_{\iota_k} - \delta_{\iota_k}),$$

avec les notations de la proposition 2.

PROPOSITION 3 bis. — *Soit L_∞/F_∞ une extension galoisienne finie. Si $H_1, H_2, ..., H_t$ sont des sous-groupes de $G = \mathrm{Gal}(L_\infty/F_\infty)$ satisfaisant :*

(i) *$H_i H_j = H_j H_i$ pour $i \neq j$.*

(ii) *Pour tout caractère φ de G, il existe $i \in \{1, ..., t\}$ tel que $H_i \subset \mathrm{Ker}\varphi$.*

Notons $N_{\infty,i}$ pour $i \geqslant t$ les sous-corps intermédiaires et $H_i = \mathrm{Gal}(L_\infty/N_{\infty,i})$.

Alors

$$(\lambda_{L_\infty} - \delta_{L_\infty}) = \sum_{k=1}^{t} (-1)^{k+1} \sum_{\iota_k \in \mathcal{A}_k^t} (\lambda_{\cap \iota_k} - \delta_{\cap \iota_k}),$$

avec les notations de la proposition 3.

En prenant deux à deux les théorèmes précédents, on déduit les assertions suivantes relatives au rang du défaut de Leopoldt.

PROPOSITION 1 ter. — *Soit L_∞/F_∞ une extension galoisienne finie. Notons $N_{\infty,i}$ pour $i \geqslant t$ les sous-corps intermédiaires et $H_i = \mathrm{Gal}(L_\infty/N_{\infty,i})$. On pose*

$$e_{H_i} = \frac{1}{|H_i|} \sum_{\tau \in H_i} \tau.$$

Si on a $\sum_{i=1}^{t} r_i e_i = 0$ avec $r_i \in \mathbb{Q}$, alors $\sum_{i=1}^{t} r_i \delta_i = 0$, *avec les notations de la proposition 1 bis.*

PROPOSITION 2 ter. — *Soit L_∞/F_∞ une extension galoisienne finie. Si $H_1, H_2, ..., H_t$ sont des sous-groupes de $G = \mathrm{Gal}(L_\infty/F_\infty)$ satisfaisant $G = \bigcup_{i=1}^{t} H_i$, alors on a :*

$$|G|\delta_{\mathcal{F}_\infty} = \sum_{k=1}^{t} (-1)^{k+1} \sum_{\iota_k \in \mathcal{A}_k^t} |\cap H_{\iota_k}| \delta_{\iota_k},$$

avec les notations de la proposition 2.

PROPOSITION 3 ter. — *Soit L_∞/F_∞ une extension galoisienne finie. Si $H_1, H_2, ..., H_t$ sont des sous-groupes de $G = \mathrm{Gal}(L_\infty/F_\infty)$ satisfaisant :*

(i) *$H_i H_j = H_j H_i$ pour $i \neq j$.*

(ii) *Pour tout caractère φ de G, il existe $i \in \{1, ..., t\}$ tel que $H_i \subset \mathrm{Ker}\varphi$.*

Notons $N_{\infty,i}$ pour $i \geqslant t$ les sous-corps intermédiaires et $H_i = \mathrm{Gal}(L_\infty/N_{\infty,i})$.

Alors

$$\delta_{\mathcal{L}_\infty} = \sum_{k=1}^{t} (-1)^{k+1} \sum_{\iota_k \in \mathcal{A}_k^t} \delta_{\cap \iota_k},$$

avec les notations de la proposition 3.

BIBLIOGRAPHIE

[ChWe] C. CHEVALLEY et A. WEIL, Über das Verhalten der Integrale Erster Gattung bei Automorphismen des Functionenkörpers, Hamb. Abh., 10 (1934), 358-361.

[Co] J. COATES, Infinite descent on elliptic curves, in Arithmetic and Geometry, papers dedicated to I. Shafarevitch, vol. 35, Progress in Math., Birkhäuser, 1983, pp. 107-137.

[Gi] R. GILLARD, Fonctions L p-adiques des corps quadratiques imaginaires et de leurs extensions abéliennes, J. reine angew. Math., 358 (1985), 76-91.

[GoMa] R. GOLD et M. MADAN, Kida's theorem for a class of non-normal extensions, Proc. Am. Math. Soc., 104 (1988), 55-59.

[Gr] R. GREENBERG, On the structure of certain Galois groups, Invent. Math., 47 (1978), 85-99.

[Iw1] K. IWASAWA, Riemann-Hurwitz formula and p-adic Galois representation for number fields, Tôhoku Math. J., 33 (1984), 263-288.

[Iw2] K. IWASAWA, On $\mathbb{Z}_p$-extensions of algebraic number fields, Ann. of Math., 98 (1973), 243-326.

[Ja1] J.-F. JAULENT, Dualité dans les corps surcirculaires, Sém. Th. Nbres Paris 1986-87, 85 (1988), 183-220, Progress in Math., Birkhäuser.

[Ja2] J.-F. JAULENT, Genres des corps surcirculaires, Pub. Math. Fac. Sci. Besançon, 1985-1986 (1986).

[JaMi] J.-F. JAULENT et A. MICHEL, Classes des corps surcirculaires et des corps de fonctions, Sém. Th. Nbres Paris 1989-90 (1991) (to appear).

[Ka] E. KANI, Relations between the Hasse-Witt invariants of Galois covering of curves, Canad. Math. Bull., 28 (1985), 321-327.

[Ki] Y. KIDA, ℓ-extension of C.M. fields and Iwasawa invariants, J. Numb. Th., 12 (1980), 519-528.

[MaZi] M. MADAN et H. ZIMMER, Relations among Iwasawa invariants, J. Numb. Th., 25 (1987), 213-219.

[Mi] A. MICHEL, Ubiquité de la formule de Riemann-Hurwitz, Thèse, Pub. Ec. Doc. Math. Univ. Bordeaux 1, 1992.

[Mz] B. MAZUR, Rational points of abelian varieties with values in towers of number fields, Invent. Math., 18 (1972), 183-266.

[Si] J. SILVERMAN, Arithmetic of elliptic curves, GTM 106, Springer-Verlag, New-York, 1986.

[Wa] L. C. WASHINGTON, Introduction to cyclotomic field, GTM 83, Springer-Verlag, New-York, 1982.

[Wi1] K. WINGBERG, Galois groups of numbers fields generated by torsion points of elliptic curves, Nagoya Math. J., 104 (1986), 43-53.

[Wi2] K. WINGBERG, A Riemann-Hurwitz formula for the Selmer group of an elliptic curve with complex multiplication, Comment. Math. Helvetica, 63 (1988), 587-592.

Manuscrit reçu le 3 décembre 1991.

Alexis MICHEL,
Centre de Recherche en Mathématiques de Bordeaux
Université de Bordeaux 1
C.N.R.S. U.A. 226
351, cours de la Libération
33405 Talence Cedex (France).