Séminaire BOURBAKI Juin 2003
55ème année, 2002-03, n° 919

LA CONJECTURE DE BIRCH ET SWINNERTON-DYER p-ADIQUE

par **Pierre COLMEZ**

Notations

Dans tout l'article, $\overline{\mathbf{Q}}$ désigne la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$ et un plongement de $\overline{\mathbf{Q}}$ dans $\overline{\mathbf{Q}}_p$ est fixé ; en particulier, $\mathscr{G}_{\mathbf{Q}_p} = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ est un sous-groupe bien déterminé de $\mathscr{G}_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. On note χ_{cycl} le caractère cyclotomique. Si $\mathrm{M} \geq 1$ est un entier, on note $\zeta_{\mathrm{M}} \in \overline{\mathbf{Q}}$ la racine de l'unité $\exp(\frac{2i\pi}{\mathrm{M}})$.

0. INTRODUCTION

Si $\mathbb{M}$ est un motif défini sur un corps de nombres, on sait lui associer (au moins conjecturalement) une fonction analytique complexe $\mathrm{L}(\mathbb{M}, s)$ définie par un produit eulérien convergeant dans un demi-plan. La quantité d'information arithmétique contenue dans les valeurs aux entiers de ces fonctions L est absolument fascinante, et on dispose d'un faisceau de conjectures la décrivant (conjectures de Deligne [64], de Beilinson [7, 180, 161], et de Bloch-Kato [27, 76, 77]). Ces conjectures sont de lointaines descendantes de la conjecture de Birch et Swinnerton-Dyer [25, 26, 184], elle-même inspirée par la formule analytique du nombre de classes d'idéaux qui reste le seul cas général que l'on sache traiter. En p-adique, on a plus de mal à définir les fonctions L mais, une fois définies, celles-ci livrent un peu plus facilement l'information qu'elles contiennent comme nous le verrons dans ce texte pour les fonctions L p-adiques de courbes elliptiques définies sur $\mathbf{Q}$ ou, plus généralement, de formes modulaires.

0.1. La formule analytique du nombre de classes

Soit K un corps de nombres d'anneau des entiers $\mathscr{O}_{\mathrm{K}}$. La fonction zêta de Dedekind ζ_{K} de K est définie, pour $\mathrm{Re}(s) > 1$, par le produit eulérien $\zeta_{\mathrm{K}}(s) = \prod_{\mathfrak{p}} \frac{1}{1-\mathrm{N}\mathfrak{p}^{-s}}$, le produit portant sur les idéaux maximaux de $\mathscr{O}_{\mathrm{K}}$, et possède un prolongement à $\mathbf{C}$ tout entier, holomorphe en dehors d'un pôle simple en $s = 1$. On dispose des résultats suivants :

THÉORÈME 0.1. — (i) *Le groupe* $\mathscr{O}_{\mathrm{K}}^*$ *des unités de* $\mathscr{O}_{\mathrm{K}}$ *est de type fini sur* $\mathbf{Z}$. *Son rang* $r(\mathrm{K})$ *est égal à* $r_1 + r_2 - 1$, *où* r_1 *est le nombre de places réelles de* K *et* r_2 *le nombre de ses places complexes.*

(ii) *Le régulateur*[1] $\mathrm{R}_\infty(\mathrm{K})$ *est non nul.*

THÉORÈME 0.2. — *Le groupe* $\mathrm{Pic}(\mathscr{O}_{\mathrm{K}})$ *des classes d'idéaux de* $\mathscr{O}_{\mathrm{K}}$ *est un groupe fini.*

THÉORÈME 0.3. — *La fonction* $\zeta_{\mathrm{K}}(s)$ *a, en* $s = 0$, *un zéro d'ordre* $r(\mathrm{K})$ *et on a*

$$\lim_{s\to 0} s^{-r(\mathrm{K})}\zeta_{\mathrm{K}}(s) = -|\mathrm{Pic}(\mathscr{O}_{\mathrm{K}})| \cdot \mathrm{R}_\infty(\mathrm{K}).$$

0.2. La conjecture de Birch et Swinnerton-Dyer

Soit E une courbe elliptique définie[2] sur $\mathbf{Q}$ de conducteur $\mathrm{N_E}$. Si p est un nombre premier, on définit l'entier a_p par :

- si $p^2 \mid \mathrm{N_E}$ (i.e. si E a réduction additive en p), alors $a_p = 0$;
- si $p \mid \mathrm{N_E}$ et $p^2 \nmid \mathrm{N_E}$ (i.e. si E a réduction multiplicative en p), alors $a_p = 1$ (resp. $a_p = -1$) si E a réduction multiplicative déployée (resp. non déployée) ;
- si $p \nmid \mathrm{N_E}$ (i.e. si E a bonne réduction en p), alors $a_p = p + 1 - |\mathrm{E}(\mathbf{F}_p)|$.

Ceci nous permet de définir la fonction L complexe $\mathrm{L}(\mathrm{E}, s)$ attachée à E par le produit eulérien (convergeant pour $\mathrm{Re}(s) > \frac{3}{2}$ car $|a_p| \leq 2\sqrt{p}$ d'après le théorème de Hasse) :

$$\mathrm{L}(\mathrm{E}, s) = \prod_{p\nmid \mathrm{N_E}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p\mid \mathrm{N_E}} \frac{1}{1 - a_p p^{-s}} = \sum_{n=1}^{+\infty} a_n n^{-s}.$$

La fonction $\mathrm{L}(\mathrm{E}, s)$ est holomorphe sur le demi-plan $\mathrm{Re}(s) > \frac{3}{2}$ et possède un prolongement analytique à tout le plan complexe (voir cor. 0.18).

Les rôles joués par ζ_{K}, $\mathscr{O}_{\mathrm{K}}^*$ et $\mathrm{Pic}(\mathscr{O}_{\mathrm{K}})$ dans la formule analytique du nombre de classes sont ici joués respectivement par $\mathrm{L}(\mathrm{E}, s)$, le groupe $\mathrm{E}(\mathbf{Q})$ des points de E rationnels sur $\mathbf{Q}$ et le groupe de Tate-Shafarevitch[3] Ш(E) de E, et les théorèmes 0.1, 0.2 et 0.3 deviennent respectivement :

---

[1] Ce régulateur est défini de la manière suivante : on part d'une famille $\varepsilon_1, \ldots, \varepsilon_{r(\mathrm{K})}$ d'éléments de $\mathscr{O}_{\mathrm{K}}^*$ engendrant un sous-groupe d'indice fini U de $\mathscr{O}_{\mathrm{K}}^*$ et de plongements $\sigma_1, \ldots, \sigma_{r(\mathrm{K})}$ de K dans $\mathbf{C}$ induisant des places différentes et on pose $e_i = 1$ si σ_i induit une place réelle et $e_i = 2$ si σ_i induit une place complexe ; alors $\mathrm{R}_\infty(\mathrm{K}) = \frac{1}{[\mathscr{O}_{\mathrm{K}}^* : \mathrm{U}]} |\det(e_i \log|\sigma_i(\varepsilon_j)|)_{1\leq i,j\leq r(\mathrm{K})}|$ ne dépend d'aucun des choix que l'on a faits.

[2] On se restreint aux courbes définies sur $\mathbf{Q}$ car ce sont les seules pour lesquelles on peut démontrer quoi que ce soit grâce à leur modularité (cf. § 0.4).

[3] $Ш(\mathrm{E}) = \mathrm{Ker}\big(\mathrm{H}^1(\mathscr{G}_{\mathbf{Q}}, \mathrm{E}(\overline{\mathbf{Q}})) \to \prod_p \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}_p}, \mathrm{E}(\overline{\mathbf{Q}}_p))\big)$ est un groupe de torsion qui représente en quelque sorte l'obstruction à la détermination du groupe $\mathrm{E}(\mathbf{Q})$: si m est un entier $m \geq 1$, le sous-groupe de m-torsion $Ш_m(\mathrm{E})$ de Ш(E) vit dans une suite exacte $0 \to \mathrm{E}(\mathbf{Q})/m\mathrm{E}(\mathbf{Q}) \to \mathrm{S}_m(\mathrm{E}) \to Ш_m(\mathrm{E}) \to 0$, où le m-groupe de Selmer $\mathrm{S}_m(\mathrm{E})$ est un groupe fini « effectivement calculable ».

Théorème 0.4. — (i) *Le groupe* $\mathrm{E}(\mathbf{Q})$ *est un groupe abélien de type fini.*

(ii) *Le régulateur*[4] $\mathrm{R}_\infty(\mathrm{E})$ *est non nul.*

Conjecture 0.5. — *Le groupe* $Ш(\mathrm{E})$ *est un groupe fini. Plus généralement, si* K *est une extension finie de* $\mathbf{Q}$*, alors* $Ш(\mathrm{E}/\mathrm{K})$ *est un groupe fini.*

On note $r(\mathrm{E})$ le rang de $\mathrm{E}(\mathbf{Q})$ et $r_\infty(\mathrm{E})$ l'ordre du zéro de $\mathrm{L}(\mathrm{E}, s)$ en $s = 1$.

Conjecture 0.6 (Birch et Swinnerton-Dyer). — *On a* $r_\infty(\mathrm{E}) = r(\mathrm{E})$ *et*[5]

$$\lim_{s\to 1}(s-1)^{-r(\mathrm{E})}\mathrm{L}(\mathrm{E}, s) = \Omega_{\mathrm{E}}^+ \cdot |Ш(\mathrm{E})| \cdot \mathrm{R}_\infty(\mathrm{E}) \cdot \prod_v m_v.$$

Les résultats concernant les conjectures 0.5 et 0.6 sont très partiels ; ce sont les suivants :

- $(\Omega_{\mathrm{E}}^+)^{-1}\mathrm{L}(\mathrm{E}, 1)$ est un nombre rationnel (c'est une conséquence du théorème de Manin-Drinfeld) ;
- si $\mathrm{L}(\mathrm{E}, 1) = 0$, alors $\lim_{s\to 1}(s-1)^{-1}\mathrm{L}(\mathrm{E}, s)$ est un multiple rationnel de $\Omega_{\mathrm{E}}^+ \cdot \mathrm{R}_\infty(\mathrm{E})$ (cela suit du théorème de Gross-Zagier [86, 40]) ;
- si $r_\infty(\mathrm{E}) \leq 1$, alors $Ш(\mathrm{E})$ est fini et $r(\mathrm{E}) = r_\infty(\mathrm{E})$ (théorème de Kolyvagin ; la démonstration utilise le théorème de Gross-Zagier et la technique des dérivées de Kolyvagin introduite à cette occasion [107, 138]).

Remarque 0.7. — (i) En ce qui concerne le dernier point, on n'a pas de résultat dans l'autre sens : on ne sait pas démontrer que $r(\mathrm{E}) = 0$ implique $r_\infty(\mathrm{E}) = 0$ (de manière

[4]Ce régulateur est défini à partir de l'accouplement *hauteur de Néron-Tate* $\langle\ ,\ \rangle_\infty$ sur l'espace vectoriel $\mathbf{R}\otimes_{\mathbf{Z}}\mathrm{E}(\mathbf{Q})$. Si $y^2 = 4x^3 + ax + b$ est une équation de Weiestrass de E, alors la fonction $\mathrm{P} = (x(\mathrm{P}), y(\mathrm{P})) \mapsto h(\mathrm{P}) = \frac{1}{2}\log d(\mathrm{P})$, où $d(\mathrm{P})$ est le dénominateur de $x(\mathrm{P})$, est presque quadratique, et la hauteur de Néron-Tate est l'unique forme bilinéaire symétrique $\langle\ ,\ \rangle_\infty$ sur $\mathrm{E}(\mathbf{Q})$ telle que $\mathrm{P} \mapsto h(\mathrm{P}) - \langle \mathrm{P}, \mathrm{P}\rangle_\infty$ soit bornée sur $\mathrm{E}(\mathbf{Q})$. Tate a remarqué que l'on pouvait définir $\langle \mathrm{P}, \mathrm{P}\rangle_\infty$ comme la limite de la suite de terme général $4^{-n}h(2^n\mathrm{P})$. Par ailleurs, Néron [129, 110], a démontré que l'accouplement $\langle\ ,\ \rangle_\infty$ pouvait s'exprimer comme une somme, sur toutes les places de $\mathbf{Q}$, de symboles locaux, les contributions aux places finies étant fournies par la théorie de l'intersection et celle à l'infini par la théorie du potentiel (fonctions de Green). Cette décomposition en somme de symboles locaux est fondamentale d'un point de vue théorique (elle est par exemple cruciale dans la démonstration du théorème de Gross-Zagier [86]), et sert de modèle pour la construction des hauteurs p-adiques (note 14). Si $\mathrm{P}_1, \dots, \mathrm{P}_r$, $r = r(\mathrm{E})$ sont des éléments de $\mathrm{E}(\mathbf{Q})$ formant une base de $\mathbf{Q}\otimes_{\mathbf{Z}}\mathrm{E}(\mathbf{Q})$ sur $\mathbf{Q}$, alors $\mathrm{R}_\infty(\mathrm{E}) = e^{-2}\det(\langle \mathrm{P}_i, \mathrm{P}_j\rangle_\infty)_{1\leq i,j\leq r}$, où e est l'indice du sous-groupe engendré par $\mathrm{P}_1, \dots, \mathrm{P}_r$ dans $\mathrm{E}(\mathbf{Q})$. La non nullité de $\mathrm{R}_\infty(\mathrm{E})$ suit de ce que l'accouplement $\langle\ ,\ \rangle_\infty$ est non dégénéré car $\langle \mathrm{P}, \mathrm{P}\rangle_\infty > 0$ si P n'est pas de torsion comme on le constate en utilisant la formule de Tate.

[5]Les termes non encore définis dans cette formule sont :

- Le nombre m_v de composantes connexes de $\mathrm{E}(\mathbf{Q}_v)$ si v est une place de $\mathbf{Q}$: si $v = \infty$, alors m_v est le nombre de composantes connexes de $\mathrm{E}(\mathbf{R})$ au sens habituel, et si $v = p$ est un nombre premier, alors m_v est le nombre de composantes connexes sur $\mathbf{F}_p$ de la réduction du modèle de Néron de E.
- La période réelle Ω_{E}^+ d'une différentielle de Néron (ou de Kähler ?, [171, p.101]) ω_{E} ; on a donc $m_\infty\Omega_{\mathrm{E}}^+ = |\int_{\mathrm{E}(\mathbf{R})}\omega_{\mathrm{E}}|$.

équivalente, on ne sait pas prouver que $L(E,1)=0$ entraîne l'existence d'un point d'ordre infini).

(ii) On ne dispose d'aucun résultat concernant le lien entre $r(E)$ et $r_\infty(E)$ ou la finitude de Ш(E) dans le cas $r_\infty(E)\geq 2$.

(iii) Une des difficultés est que l'on ne connaît pas la valeur de $r(E)$ a priori ; on pense que si on prend une courbe E au hasard, alors $r(E)\leq 1$ avec une probabilité tendant vers 1 quand N_E tend vers $+\infty$, mais on connaît des courbes de rang ≥ 24, et il y a tout lieu de croire que $r(E)$ n'est pas majoré.

(iv) Par contraste, on ne connaît pas de courbe elliptique E pour laquelle on peut prouver que[6] $r_\infty(E)\geq 4$; le problème est qu'il est impossible de prouver qu'un réel est nul[7] sauf si c'est un entier. C'est un peu dommage, car l'existence de telles courbes permettrait d'améliorer nettement les minorations effectives pour le nombre de classes des corps quadratiques imaginaires [82, 131].

0.3. La conjecture de Birch et Swinnerton-Dyer p-adique

En p-adique, le produit eulérien ci-dessus ne converge nulle part, mais on peut construire une fonction L p-adique[8] à partir des valeurs en 1 de la fonction L complexe tordue[9] par des caractères de Dirichlet de conducteur une puissance de p. Cette fonction L p-adique dépend d'un choix supplémentaire : on factorise le facteur d'Euler en p de $L(E,s)$ sous la forme $(1-\alpha_1 p^{-s})(1-\alpha_2 p^{-s})$ et on choisit $\alpha\in\{\alpha_1,\alpha_2\}$ vérifiant[10] $v_p(\alpha)<1$.

La construction de la fonction L p-adique $L_{p,\alpha}(E,s)$ de E associée à α repose sur la théorie des symboles modulaires[11] qui permet [118, 4, 112, 192] de démontrer :

---

[6]On peut, le cas échéant, vérifier que $r_\infty(E)\geq 3$ grâce au théorème de Gross-Zagier.

[7]En particulier, démontrer la conjecture 0.6 sous la forme faible « $r_\infty(E)=r(E)$ » ne fournit pas d'algorithme déterministe pour calculer $r(E)$ et $E(\mathbf{Q})$. Par contre, la conjecture 0.6 (même un peu affaiblie sous la forme $\lim_{s\to 1}(s-1)^{-r(E)}L(E,s)=n\cdot\Omega_E^+\cdot R_\infty(E)$, avec n entier ≥ 1) fournit un tel algorithme, le point étant que plus $R_\infty(E)$ est petit et plus les générateurs de $E(\mathbf{Q})$ sont faciles à trouver.

[8]Il faut probablement supposer $p\neq 2$ ou $p\geq 5$ dans certains des énoncés qui suivent au niveau de ce qui est connu.

[9]Si χ est un tel caractère, on note $L(E,\chi,s)$ la fonction L de E tordue par χ ; elle est définie par la série de Dirichlet $L(E,\chi,s)=\sum_{n=1}^{+\infty}\chi(n)a_n n^{-s}$. Si le conducteur de χ n'est pas premier au conducteur de E, la fonction $L(E,\chi,s)$ n'est pas forcément primitive ; il peut manquer des facteurs d'Euler en les nombres premiers divisant N_E.

[10]Ce n'est pas toujours possible : si E a réduction additive en p, alors $\alpha_1=\alpha_2=0$ et on ne sait pas construire de fonction L p-adique dans ce cas (sauf si la courbe acquiert bonne réduction sur une extension abélienne de $\mathbf{Q}$ (cf. [62])). Si E a réduction multiplicative, alors $\{\alpha_1,\alpha_2\}=\{a_p,0\}$, et on peut prendre $\alpha=a_p\in\{\pm 1\}$. Si E a bonne réduction, il y a deux cas de figure possibles : si $v_p(a_p)>0$ (i.e. si E a bonne réduction supersingulière), alors il y a deux choix possibles pour α puisque $v_p(\alpha_1)=v_p(\alpha_2)=1/2$, et si $v_p(a_p)=0$ (bonne réduction ordinaire), alors une seule des deux racines α_1,α_2 est de valuation <1 (de valuation 0), alors que l'autre est de valuation 1 (voir [150] et la rem. 4.12 pour ce dernier cas).

[11]Panchishkin [133] a récemment trouvé une définition alternative de cette fonction qui colle nettement plus à la construction que l'on obtient en utilisant le système d'Euler de Kato.

THÉORÈME 0.8. — *Soient* Ω_{E}^{+} *et* Ω_{E}^{-} *les périodes réelles et imaginaires pures de* ω_{E}. *Alors*

(i) *si* χ *est un caractère de Dirichlet,* $\mathrm{L}(\mathrm{E},\chi,1)\in\overline{\mathbf{Q}}\cdot\Omega_{\mathrm{E}}^{\chi(-1)}$;

(ii) *il existe une* (unique) *distribution* $\mu_{\mathrm{E},\alpha}$ *d'ordre* $v_p(\alpha)$ *sur* $\mathbf{Z}_p$, *telle que l'on ait*

$$\int_{p\mathbf{Z}_p}\phi(x)\mu_{\mathrm{E},\alpha}(x)=\alpha^{-1}\int_{\mathbf{Z}_p}\phi(px)\mu_{\mathrm{E},\alpha}(x)$$

quelle que soit ϕ *localement analytique sur* $p\mathbf{Z}_p$, *et*

$$\int_{\mathbf{Z}_p}\mu_{\mathrm{E},\alpha}(x)=(1-\alpha^{-1})^b\frac{\mathrm{L}(\mathrm{E},1)}{\Omega_{\mathrm{E}}^{+}}\quad\text{et}\quad\int_{\mathbf{Z}_p}\chi(x)\mu_{\mathrm{E},\alpha}(x)=p^n\alpha^{-n}\frac{\mathrm{L}(\mathrm{E},\chi^{-1},1)}{\mathrm{G}(\chi^{-1})\cdot\Omega_{\mathrm{E}}^{\chi(-1)}}$$

si $n\geq 1$ *et* χ *est un caractère de Dirichlet*[12] *de conducteur* p^n, *et* $b=0$ *(resp.* $b=1$*) si* E *a mauvaise réduction multiplicative (resp. bonne réduction).*

DÉFINITION 0.9. — *La fonction* L p*-adique* $s\mapsto\mathrm{L}_{p,\alpha}(\mathrm{E},s)$ *de* E *associée à* α *est la fonction définie, pour* $s\in\mathbf{Z}_p$, *par la formule*

$$\mathrm{L}_{p,\alpha}(\mathrm{E},s)=\int_{\mathbf{Z}_p^*}\langle x\rangle^{s-1}\,\mu_{\mathrm{E},\alpha},\quad\text{avec }\langle x\rangle^{s-1}=\exp((s-1)\log x).$$

REMARQUE 0.10. — On déduit du théorème 0.8 la formule

$$\mathrm{L}_{p,\alpha}(\mathrm{E},1)=(1-\alpha^{-1})^{b+1}\frac{\mathrm{L}(\mathrm{E},1)}{\Omega_{\mathrm{E}}^{+}}.$$

En particulier, si $\alpha=1$, alors la fonction $\mathrm{L}_{p,\alpha}(\mathrm{E},s)$ a un zéro supplémentaire en $s=1$. La courbe E a alors réduction multiplicative déployée et le théorème d'uniformisation de Tate [186] nous fournit $q(\mathrm{E})\in\mathbf{Q}_p^*$, de valuation non nulle, tel que E soit isomorphe, en tant qu'espace analytique rigide, au quotient de $\mathbf{G}_m$ par le groupe engendré par $q(\mathrm{E})$. Ceci nous permet de définir l'invariant $\mathscr{L}$ de E par la formule $\mathscr{L}_{\mathrm{E}}=\frac{\log q(\mathrm{E})}{v_p(q(\mathrm{E}))}$.

THÉORÈME 0.11. — *Si* $\alpha=1$, *alors*[13] $\mathrm{L}'_{p,\alpha}(\mathrm{E},1)=\mathscr{L}_{\mathrm{E}}\cdot\dfrac{\mathrm{L}(\mathrm{E},1)}{\Omega_{\mathrm{E}}^{+}}$.

On sait définir un[14] accouplement *hauteur p-adique* sur l'espace vectoriel $\mathbf{Q}_p\otimes\mathrm{E}(\mathbf{Q})$, mais celui-ci dépend du choix d'un scindage de la filtration de Hodge sur $\mathbf{Q}_p\otimes_{\mathbf{Q}}\mathrm{H}^1_{\mathrm{dR}}(\mathrm{E})$

[12] On considère χ comme une fonction localement constante sur $\mathbf{Z}_p$, nulle sur $p\mathbf{Z}_p$, et on note $\mathrm{G}(\chi^{-1})=\sum_{a\in(\mathbf{Z}/p^n\mathbf{Z})^*}\zeta_{p^n}^a\chi^{-1}(a)$ la somme de Gauss de χ^{-1}.

[13] Ce théorème (cas particulier de la conjecture de Mazur-Tate-Teitelbaum) a été démontré par Greenberg et Stevens [85] en utilisant les familles de formes modulaires de Hida.

[14] On a trois définitions de cette hauteur p-adique : deux algébriques, l'une via la théorie d'Iwasawa [165, 139], l'autre via la cohomologie galoisienne [126, 139, 141], et une analytique utilisant l'intégration p-adique [46, 52, 197] ou les fonctions thêta p-adiques [119, 120, 130]. Il n'est pas évident a priori que ces définitions coïncident, mais c'est le cas ([139] pour les deux constructions algébriques et [165, 24, 95] pour la comparaison « algébrique-analytique »), ce qui permet de vérifier que les résultats que l'on obtient du côté de la théorie d'Iwasawa sont compatibles avec la conjecture de Birch et Swinnerton-Dyer via la conjecture principale. La définition analytique est obtenue en p-adifiant la définition de la hauteur de Néron-Tate (note 4) comme somme de symboles locaux (cf. [135] pour une définition à la Tate), la contribution en un premier $\ell\neq p$ restant la même, alors que la contribution à l'infini est transférée en p

(i.e. d'un supplémentaire de $\mathbf{Q}_p \cdot \omega_{\mathrm{E}}$). On note $\langle\ ,\ \rangle_{p,\alpha}$ l'accouplement correspondant à la droite de $\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathrm{H}^1_{\mathrm{dR}}(\mathrm{E})$ sur laquelle frobenius[15] agit par multiplication par α, et $\mathrm{R}_{p,\alpha}(\mathrm{E})$ le régulateur correspondant.

Conjecture 0.12 (Mazur-Tate-Teitelbaum). — (i) *L'ordre du zéro en $s=1$ de la fonction $\mathrm{L}_{p,\alpha}(\mathrm{E},s)$ est $\geq r(\mathrm{E})$ et on a*

$$\lim_{s\to 1}(s-1)^{-r(\mathrm{E})}\mathrm{L}_{p,\alpha}(\mathrm{E},s) = (1-\alpha^{-1})^{b+1}\cdot|\text{Ш}(\mathrm{E})|\cdot \mathrm{R}_{p,\alpha}(\mathrm{E})\cdot\prod_v m_v.$$

(ii) *Si $\alpha=1$, l'ordre du zéro en $s=1$ de la fonction $\mathrm{L}_{p,\alpha}(\mathrm{E},s)$ est $\geq r(\mathrm{E})+1$ et on a*

$$\lim_{s\to 1}(s-1)^{-r(\mathrm{E})-1}\mathrm{L}_{p,\alpha}(\mathrm{E},s) = \mathscr{L}_{\mathrm{E}}\cdot|\text{Ш}(\mathrm{E})|\cdot \mathrm{R}_{p,\alpha}(\mathrm{E})\cdot\prod_v m_v.$$

Remarque 0.13. — (i) La non nullité de $\mathscr{L}_{\mathrm{E}}$ (conjecturée par Manin) a été démontrée par Barré, Diaz, Gramain et Philibert [5, 193] par des techniques de transcendance.

(ii) Contrairement au cas archimédien, on ne sait pas montrer que l'accouplement *hauteur p-adique* est non dégénéré[16], et démontrer la non nullité de $\mathrm{R}_{p,\alpha}(\mathrm{E})$ semble être du même ordre de difficulté que prouver la conjecture de Leopoldt[17]...

En dehors du théorème 0.11 ci-dessus, on dispose d'un analogue p-adique du théorème de Gross-Zagier :

par l'intermédiaire d'une fonction de Green p-adique. Si $\partial = \frac{d}{\omega_{\mathrm{E}}}$ est l'opérateur différentiel invariant par translation sur E, dual de $\omega_{\mathrm{E}} = \frac{dx}{y}$, si v est une place de $\mathbf{Q}$, et si D est un diviseur de E, la fonction de Green de D en v s'obtient, par translation, à partir de la fonction de Green G_v de 0, qui est une fonction analytique réelle si $v=\infty$, localement analytique si v est finie, solution d'une équation différentielle du type $\partial^2\mathrm{G}_v = x+u$, avec $u\in\overline{\mathbf{Q}}_v$. Si $v=\infty$, le choix de u est imposé par la périodicité de G_v (vue comme fonction sur $\mathbf{C}$) par rapport au réseau des périodes de ω_{E} (u s'exprime alors en termes de la série d'Eisenstein non holomorphe E_2^*). Par contre, si $v=p$ est une place finie, on peut choisir u, ce qui revient à choisir un scindage de la filtration de Hodge, totalement arbitrairement. C'est pour cela que « la » hauteur p-adique dépend du choix d'un tel scindage.

[15] L'existence de α implique que E a bonne réduction ou est semi-stable, et donc que $\mathbf{Q}_p\otimes_{\mathbf{Q}}\mathrm{H}^1_{\mathrm{dR}}(\mathrm{E})$ est naturellement isomorphe à la cohomologie (log)-cristalline de E, ce qui permet de le munir d'une action du frobenius φ.

[16] En fait, on ne sait même pas démontrer qu'il n'est pas identiquement nul sauf dans le cas de multiplication complexe [21].

[17] De manière générale, montrer qu'une fonction L p-adique ne s'annule pas en un entier est un problème difficile (alors que le problème analogue pour une fonction L complexe est en général très facile), et les seuls résultats généraux dont on dispose, pour le moment, reposent sur des techniques de transcendance. La conjecture de Leopoldt en est un exemple particulièrement frustrant. Si K est un corps de nombres, la formule analytique du nombre de classes est aussi équivalente à l'existence d'un pôle simple en $s=1$ pour la fonction zêta de Dedekind ζ_{K} de K, de résidu

$$\lim_{s\to 1}(s-1)\zeta_{\mathrm{K}}(s) = \frac{2^{r_1}\,(2\pi)^{r_2}\cdot|\mathrm{Pic}(\mathscr{O}_{\mathrm{K}})|\cdot \mathrm{R}_\infty(\mathrm{K})}{\sqrt{|\mathrm{D}_{\mathrm{K}}|}},$$

où D_{K} est le discriminant de K. Si K est totalement réel (i.e. $r_2=0$ et $r_1=[\mathrm{K}:\mathbf{Q}]$), on sait lui associer [168, 6, 34, 66] une fonction zêta p-adique $\zeta_{\mathrm{K},p}$ et on dispose [50] de la formule analytique

THÉORÈME 0.14. — *Si* $r_\infty(\mathrm{E}) = 1$ *et* E *a bonne réduction ordinaire*[18], *alors*

$$\mathrm{L}'_{p,\alpha}(\mathrm{E},1) = (1-\alpha^{-1})^2 \cdot \mathrm{R}_{p,\alpha}(\mathrm{E}) \cdot \Big(\mathrm{R}_\infty(\mathrm{E})^{-1}\frac{\mathrm{L}'(\mathrm{E},1)}{\Omega_{\mathrm{E}}^+}\Big).$$

Finalement, le résultat le plus spectaculaire, pour lequel on n'a pas d'équivalent en complexe, est le théorème suivant de Kato[19] [102] auquel le reste du texte va être consacré.

THÉORÈME 0.15. — *L'ordre du zéro de* $\mathrm{L}_{p,\alpha}(\mathrm{E},s)$ *en* $s=1$ *est* $\geq r(\mathrm{E})$ *et même* $\geq r(\mathrm{E})+1$ *si* $\alpha = 1$. *De plus, si cette inégalité est une égalité, alors la* p*-partie* $\text{Ш}_{p^\infty}(\mathrm{E})$ *de* $\text{Ш}(\mathrm{E})$ *est finie et* $\mathrm{R}_{p,\alpha}(\mathrm{E}) \neq 0$.

REMARQUE 0.16. — (i) En partant de courbes de rang ≥ 24, cela nous fournit des fonctions L p-adiques ayant un zéro d'ordre ≥ 24 en $s=1$.

(ii) Vérifier la non nullité d'un nombre p-adique peut (contrairement à sa nullité) se faire en calculant ce nombre avec une précision suffisante. Le th. 0.15 nous fournit donc, en principe, un critère analytique pour vérifier que la p-partie du groupe de Tate-Shafarevitch est finie même si le rang est très grand[20].

0.4. **Des courbes elliptiques aux formes modulaires**

Il faut être bien conscient de ce que l'on serait totalement démuni pour étudier la fonction L d'une courbe elliptique si l'on ne disposait que de sa définition comme produit eulérien[21]. Tous les beaux théorèmes évoqués ci-dessus s'appuient de manière cruciale sur le fait que la conjecture de Taniyama-Weil est maintenant un théorème grâce aux travaux de Wiles [196, 132, 170] et ceux de Breuil, Conrad, Diamond et Taylor [29, 69]. Ceci se traduit de la manière suivante :

THÉORÈME 0.17. — *Si* E *est une courbe elliptique définie sur* $\mathbf{Q}$, *de conducteur* $\mathrm{N_E}$, *et si* $\mathrm{L}(\mathrm{E},s) = \sum_{n=1}^{+\infty} a_n n^{-s}$, *alors* $f_{\mathrm{E}}(\tau) = \sum_{n=1}^{+\infty} a_n q^n$ (avec $q = e^{2i\pi\tau}$) *est une forme modulaire primitive de poids* 2 *pour* $\Gamma_0(\mathrm{N_E})$.

---

p-adique du nombre de classes :

$$\lim_{s\to 1}(s-1)\zeta_{\mathrm{K},p}(s) = \frac{2^{[\mathrm{K}:\mathbf{Q}]}\cdot|\mathrm{Pic}(\mathscr{O}_\mathrm{K})|\cdot \mathrm{R}_p(\mathrm{K})}{\sqrt{|\mathrm{D_K}|}} \cdot \prod_{\mathfrak{p}|p}(1-(\mathrm{N}\mathfrak{p})^{-1}),$$

où le régulateur p-adique $\mathrm{R}_p(\mathrm{K})$ est défini par la même formule que $\mathrm{R}_\infty(\mathrm{K})$, mais en remplaçant le logarithme complexe par le logarithme p-adique. Malheureusement, on ne sait prouver que $\mathrm{R}_p(\mathrm{K}) \neq 0$ (conjecture de Leopoldt) que si K est une extension abélienne de $\mathbf{Q}$, en utilisant le fait que le régulateur est alors un produit de formes linéaires de logarithmes de nombres algébriques que l'on peut étudier par une variante p-adique [30] de la méthode de Baker.

[18]Ce théorème est dû à Perrin-Riou [136] ; j'ignore s'il a été étendu au cas supersingulier.

[19]Si E est de type CM, ce résultat remonte à Rubin [156], au moins dans le cas ordinaire.

[20]Cf. [147] pour une utilisation de ce point.

[21]On ne saurait pas que la fonction L est définie en $s=1$ et on ne saurait pas construire la fonction L p-adique associée à E.

Corollaire 0.18. — *La fonction* $\mathrm{L}(\mathrm{E}, s)$ *possède un prolongement analytique à tout le plan complexe. De plus, il existe* $\varepsilon_{\mathrm{E}} \in \{\pm 1\}$ *tel que la fonction* $\Lambda(\mathrm{E}, s) = \frac{\Gamma(s)}{(2\pi)^s} \mathrm{N}_{\mathrm{E}}^{s/2} \mathrm{L}(\mathrm{E}, s)$ *vérifie l'équation fonctionnelle* $\Lambda(\mathrm{E}, s) = \varepsilon_{\mathrm{E}} \cdot \Lambda(\mathrm{E}, 2-s)$.

Remarque 0.19. — (i) Si $\varepsilon_{\mathrm{E}} = -1$, la fonction $\mathrm{L}(\mathrm{E}, s)$ s'annule en $s = 1$. La conjecture de Birch et Swinnerton-Dyer prédit alors que $\mathrm{E}(\mathbf{Q})$ est un groupe infini. Nekovář [128] a démontré que, si $Ш_{p^\infty}(\mathrm{E})$ est fini pour au moins un premier p en lequel E a bonne réduction ordinaire, alors $\mathrm{E}(\mathbf{Q})$ est effectivement infini[22].

(ii) Comme Γ a des pôles simples aux entiers négatifs, l'équation fonctionnelle ci-dessus et la non annulation de $\mathrm{L}(\mathrm{E}, s)$ pour $\mathrm{Re}(s) \geq 2$ impliquent que $\mathrm{L}(\mathrm{E}, s)$ a des zéros simples en tous les entiers négatifs.

Théorème 0.20. — *Si* E *est une courbe elliptique définie sur* $\mathbf{Q}$ *de conducteur* N_{E}, *il existe un morphisme surjectif* $\pi_{\mathrm{E}} : \mathscr{H} \to \mathrm{E}$ *de surfaces de Riemann, se factorisant à travers* $\Gamma_0(\mathrm{N}_{\mathrm{E}})\backslash\mathscr{H}$, *tel que* $\pi_{\mathrm{E}}(i\infty) = 0$. *De plus*

(i) $\pi_{\mathrm{E}}^* \omega_{\mathrm{E}} = c_{\mathrm{E}} f_{\mathrm{E}}$, *avec* $c_{\mathrm{E}} \in \mathbf{Z}$;

(ii) *si* $\mathrm{P} \in \mathbf{P}^1(\mathbf{Q})$ *est une pointe de* $\mathscr{H}$, *alors* $\pi_{\mathrm{E}}(\mathrm{P}) \in \mathrm{E}(\mathbf{Q})_{\mathrm{tors}}$.

Remarque 0.21. — (i) Le théorème 0.20 se déduit[23] du théorème 0.17, mais n'en est pas une conséquence formelle. Il résulte de l'existence d'une courbe elliptique E' quotient de $\mathrm{X}_0(\mathrm{N}_{\mathrm{E}})$ dont la fonction L est égale à $\mathrm{L}(f_{\mathrm{E}}, s)$ (travaux d'Eichler-Shimura [70, 172, 173, 174, 176] et Carayol [31]) et de ce que deux courbes elliptiques définies sur $\mathbf{Q}$ ayant même fonction L sont isogènes. Ce dernier fait a été démontré par Serre [167] dans le cas où $j(\mathrm{E}) \notin \mathbf{Z}$, et en toute généralité par Faltings [71, 65] comme cas particulier de la conjecture de Tate. Une autre démonstration utilisant des techniques de transcendance a été obtenue par Chudnovsky [38] (voir aussi [28] et [35]).

(ii) Le théorème 0.17 est un cas particulier de la correspondance (conjecturale) de Langlands entre motifs et formes automorphes arithmétiques. Il semble beaucoup plus difficile de généraliser le théorème 0.20 en une conjecture fournissant une description automorphe d'un motif quelconque. Le cas le plus simple posant problème est celui d'une courbe elliptique E, définie sur un corps quadratique réel, que l'on pourrait s'attendre à voir apparaître dans le H^1 d'une variété de Shimura convenable, mais Blasius a montré que ce n'est pas le cas si E a bonne réduction partout et n'est pas isogène (sur $\overline{\mathbf{Q}}$) à sa conjuguée.

(iii) Les motifs associés aux formes modulaires ont une structure extrêmement riche. On peut jouer sur les aspects « variété de modules » ou « quotient du demi-plan de Poincaré »

[22] Il a en fait démontré que la parité du corang du groupe de Selmer est celle prédite par la conjecture de Birch et Swinnerton-Dyer. Dans le cas CM, la non finitude du groupe de Selmer si $\varepsilon_{\mathrm{E}} = -1$ remonte à Greenberg [84] dans le cas ordinaire et à Rubin [155] dans le cas supersingulier, et la parité du corang du groupe de Selmer à Guo [87].

[23] Sauf le (ii), pour lequel on a en plus besoin du théorème de Manin-Drinfeld.

de $X_0(N)$ pour construire de manière systématique des objets (symboles modulaires, points de Heegner, unités de Siegel...) permettant d'étudier leur arithmétique. Par contraste, on ne sait pas dire grand-chose directement de l'arithmétique d'une courbe elliptique. Le théorème 0.20 qui établit un isomorphisme entre la courbe elliptique E et le motif associé à f_E est donc crucial pour étudier l'arithmétique de E. De fait, les théorèmes 0.11 et 0.15 sont obtenus via le théorème 0.20, comme cas particuliers de théorèmes généraux (cf. th. 0.22, 0.23 et 4.16) sur les motifs associés aux formes modulaires de poids quelconque ; ils correspondent au cas des formes modulaires de poids 2 à coefficients rationnels.

0.5. **Formes modulaires de poids quelconque**

Soit $f = \sum_{n=1}^{+\infty} a_n q^n$ une forme primitive de niveau N, poids k et caractère ε. Soit $\mathbf{Q}(f) = \mathbf{Q}(a_1, \ldots, a_n, \ldots)$; c'est une extension finie de $\mathbf{Q}$ contenue dans $\overline{\mathbf{Q}}$. Soit p un nombre premier et soit $\mathbf{Q}_p(f) = \mathbf{Q}_p(a_1, \ldots, a_n, \ldots)$; c'est une extension finie de $\mathbf{Q}_p$ dont on note O_p l'anneau des entiers. D'après Deligne [63], on peut associer à f une $\mathbf{Q}_p(f)$-représentation V_f de $\mathscr{G}_{\mathbf{Q}}$, de dimension 2, non ramifiée en dehors de Np, caractérisée par le fait que le déterminant de $1 - \mathrm{Fr}_\ell^{-1}\mathrm{X}$ agissant sur V_f est $1 - a_\ell \mathrm{X} + \ell^{k-1}\varepsilon(\ell)\mathrm{X}^2$, où $\mathrm{Fr}_\ell \in \mathscr{G}_{\mathbf{Q}}$ est un frobenius arithmétique en ℓ si $\ell \nmid \mathrm{N}p$.

Si T_f est un O_p-réseau de V_f stable[24] par $\mathscr{G}_{\mathbf{Q}}$, si $j \in \mathbf{Z}$, et si K est une extension finie de $\mathbf{Q}$, on définit[25] le groupe de Selmer $\mathrm{Sel}(\mathrm{T}_f(j)/\mathrm{K})$ qui est un O_p-module isomorphe à $(\mathbf{Q}_p(f)/\mathrm{O}_p)^r \oplus \mathrm{X}$, où X est fini et $r = \mathrm{corg}_{\mathrm{O}_p}(\mathrm{Sel}(\mathrm{T}_f(j))/\mathrm{K})$ est un entier.

Si f est la forme modulaire associée à une courbe elliptique E définie sur $\mathbf{Q}$ et si $j = 1$, on peut prendre pour $\mathrm{T}_f(1)$ le module de Tate $\mathrm{T}_p(\mathrm{E})$ de E (i.e. le $\mathbf{Z}_p$-module des familles $(u_n)_{n\in\mathbf{N}}$ d'éléments de $\mathrm{E}(\overline{\mathbf{Q}})$ vérifiant $u_0 = 0$ et $pu_{n+1} = u_n$). Si K est une extension finie de $\mathbf{Q}$, alors $\mathrm{Sel}(\mathrm{T}_p(\mathrm{E})/\mathrm{K})$ est la p-partie $\mathrm{Sel}_{p^\infty}(\mathrm{E}/\mathrm{K})$ du groupe de Selmer de E sur K, et on a la suite exacte

$$0 \to \mathrm{E}(\mathrm{K}) \otimes (\mathbf{Q}_p/\mathbf{Z}_p) \to \mathrm{Sel}(\mathrm{T}_p(\mathrm{E})/\mathrm{K}) \to Ш_{p^\infty}(\mathrm{E}/\mathrm{K}) \to 0.$$

En particulier, $\mathrm{corg}(\mathrm{Sel}(\mathrm{T}_p(\mathrm{E})/\mathrm{K})) = r(\mathrm{E}/\mathrm{K}) + \mathrm{corg}(Ш_{p^\infty}(\mathrm{E}/\mathrm{K}))$, et $Ш_{p^\infty}(\mathrm{E}/\mathrm{K})$ est fini si et seulement si $\mathrm{corg}(\mathrm{Sel}(\mathrm{T}_p(\mathrm{E})/\mathrm{K})) = r(\mathrm{E}/\mathrm{K})$.

THÉORÈME 0.22. — *Soit f une forme primitive de poids $k \geq 2$, soit $j \in \{1, \ldots, k-1\}$ un entier, et soit T_f un réseau de V_f stable par $\mathscr{G}_{\mathbf{Q}}$. Si* K *une extension finie abélienne*

[24]Un tel réseau existe toujours car $\mathscr{G}_{\mathbf{Q}}$ est un groupe compact.

[25]Si v est une place de K, on définit le sous-groupe $\mathrm{H}^1_f(\mathscr{G}_{\mathrm{K}_v}, \mathrm{V}_f(j))$ de $\mathrm{H}^1(\mathscr{G}_{\mathrm{K}_v}, \mathrm{V}_f(j))$ comme le noyau de l'application de $\mathrm{H}^1(\mathscr{G}_{\mathrm{K}_v}, \mathrm{V}_f(j))$ dans $\mathrm{H}^1(\mathrm{I}_{\mathrm{K}_v}, \mathrm{V}_f(j))$ (resp. $\mathrm{H}^1(\mathscr{G}_{\mathrm{K}_v}, \mathbf{B}_{\mathrm{cris}} \otimes_{\mathbf{Q}_p} \mathrm{V}_f(j))$) si v est une place finie ne divisant pas p et $\mathrm{I}_{\mathrm{K}_v}$ est le sous-groupe d'inertie de $\mathscr{G}_{\mathrm{K}_v}$ (resp. si v divise p et $\mathbf{B}_{\mathrm{cris}}$ est un des anneaux de Fontaine). On définit alors $\mathrm{H}^1_{/f}(\mathscr{G}_{\mathrm{K}_v}, \mathrm{V}_f(j)/\mathrm{T}_f(j))$ comme le quotient de $\mathrm{H}^1(\mathscr{G}_{\mathrm{K}_v}, \mathrm{V}_f(j)/\mathrm{T}_f(j))$ par l'image de $\mathrm{H}^1_f(\mathscr{G}_{\mathrm{K}_v}, \mathrm{V}_f(j))$ et on a

$$\mathrm{Sel}(\mathrm{T}_f(j)/\mathrm{K}) = \mathrm{Ker}\big(\mathrm{H}^1(\mathscr{G}_{\mathrm{K}}, \mathrm{V}_f(j)/\mathrm{T}_f(j)) \longrightarrow \oplus_v \mathrm{H}^1_{/f}(\mathscr{G}_{\mathrm{K}_v}, \mathrm{V}_f(j)/\mathrm{T}_f(j))\big).$$

de $\mathbf{Q}$*, si* $\eta : \mathrm{Gal}(\mathrm{K}/\mathbf{Q}) \to \overline{\mathbf{Q}}^*$ *est un caractère de Dirichlet, et si* $\mathrm{L}(f,\eta,j) \neq 0$*, le groupe* $\mathrm{Sel}(\mathrm{T}_f(j)/\mathrm{K})^{(\eta)}$ *est un groupe fini, nul si p est assez grand*[26].

Soit α une racine du polynôme $\mathrm{X}^2 - a_p\mathrm{X} + \varepsilon(p)p^{k-1}$ avec $v_p(\alpha) < k-1$. Comme pour les courbes elliptiques, on peut utiliser la théorie des symboles modulaires pour construire une fonction L p-adique $\mathrm{L}_{p,\alpha}(f,\eta\chi_{\mathrm{cycl}}^j,s)$, où η est un caractère d'ordre fini et j un entier, interpolant les valeurs de la fonction L complexe en les caractères critiques (i.e. les $\mathrm{L}(f,\chi,j)$, où χ est un caractère de Dirichlet et j un entier, avec $1 \le j \le k-1$). On a alors le théorème suivant [102] qui contient le théorème 0.15 comme cas particulier (à la non annulation du régulateur près).

Théorème 0.23. — *L'ordre du zéro en* $s = 0$ *de la fonction* $\mathrm{L}_{p,\alpha}(f,\eta\chi_{\mathrm{cycl}}^j,s)$ *est* $\geq \mathrm{corg}(\mathrm{Sel}(\mathrm{T}_f(j)/\mathrm{K})^{(\eta)})$ *et même* $\geq \mathrm{corg}(\mathrm{Sel}(\mathrm{T}_f(j)/\mathrm{K})^{(\eta)}) + 1$*, si* $j = \frac{k}{2}$ *et* $\alpha = p^{j-1}\eta(p)^{-1}$.

Remarque 0.24. — L'ordre d'annulation d'une fonction L complexe peut s'aborder sous l'angle de la théorie analytique des nombres. De ce point de vue, on dispose des résultats suivants :

(i) La condition $\mathrm{L}(f,\eta,j) \neq 0$ est automatique si $j \neq \frac{k}{2}, \frac{k-1}{2}$: si $j > \frac{k+1}{2}$ cela suit de ce que le produit eulérien définissant $\mathrm{L}(f,\eta,j)$ est absolument convergent grâce à la conjecture de Ramanujan-Peterson ; le cas $j = \frac{k+1}{2}$ (bord de la bande critique) est un théorème de Jacquet et Shalika [97] et les autres cas s'en déduisent en utilisant l'équation fonctionnelle[27].

(ii) Si S est un ensemble fini de nombres premiers et $\mathbf{Q}_{\mathrm{S}}^{\mathrm{ab}}$ est l'extension abélienne maximale de $\mathbf{Q}$ non ramifiée en dehors de S, Rohrlich [154] a démontré que

$$\left\{\eta : \mathrm{Gal}(\mathbf{Q}_{\mathrm{S}}^{\mathrm{ab}}/\mathbf{Q}) \to \mathbf{C}^*,\ \mathrm{L}(f,\eta,k/2) = 0\right\}$$

est fini. Le (i) du théorème 0.22 permet donc de montrer que le groupe $\mathrm{E}(\mathbf{Q}_{\mathrm{S}}^{\mathrm{ab}})$ est de rang fini ; plus généralement, le groupe $\mathrm{A}(\mathbf{Q}_{\mathrm{S}}^{\mathrm{ab}})$ est de rang fini si A est une variété abélienne quotient de la jacobienne d'une courbe modulaire.

(iii) En comparant l'inégalité du théorème 0.22 avec ce que prédisent les conjectures de Beilinson, on obtient l'inégalité *conjecturale*

$$\mathrm{ord}_{s=j}\mathrm{L}(f,\eta,s) \le \mathrm{ord}_{s=0}\mathrm{L}_{p,\alpha}(f,\eta\chi_{\mathrm{cycl}}^j,s)$$

qui ne fait intervenir que des objets définis analytiquement à partir de la forme modulaire. Peut-on démontrer cette inégalité par des techniques de théorie analytique des nombres ? (Le problème ne se pose que pour $j = \frac{k}{2}$ d'après ce qui précède.)

[26] Il faut que l'image de $\mathscr{G}_{\mathbf{Q}}$ dans la représentation modulo p soit assez grosse, ce qui est le cas pour p grand, si f n'est pas de type CM, d'après un théorème de Serre [169] (pour une courbe elliptique) et Ribet [151, 153]. Le cas CM se déduit des résultats de Rubin [158].

[27] Les zéros potentiels pour $j = \frac{k-1}{2}$ viennent de ce que $\mathrm{L}(f,\eta,s)$ n'étant pas forcément primitive, certains des facteurs d'Euler manquants peuvent avoir un zéro en $s = \frac{k-1}{2}$.

(iv) En utilisant les « formules explicites », on peut borner [124] l'ordre du zéro en $s = \frac{k}{2}$ de la fonction $\mathrm{L}(f,\eta,s)$ en fonction de k et N. Peut-on obtenir des bornes similaires pour l'ordre du zéro de $\mathrm{L}_{p,\alpha}$? On pourrait peut-être en tirer la finitude du groupe de Tate-Shafarevitch (ou au moins la finitude de sa p-partie[28] pour tout p) pour des courbes elliptiques de grand rang et « petit » conducteur comme celles obtenues [124] en maximisant le nombre de points modulo p pour beaucoup de petits p.

0.6. **Survol de la démonstration**

0.6.1. *Systèmes d'Euler et bornes pour les groupes de Selmer.* Grâce aux travaux de Kolyvagin [107], étendus par Kato [100], Perrin-Riou [143] et Rubin [159] (voir aussi [116]), on dispose d'une machine extrêmement puissante (dérivées de Kolyvagin) pour borner le groupe de Selmer d'une représentation p-adique V de $\mathscr{G}_{\mathbf{Q}}$. Pour fonctionner, la machine nécessite la construction d'un *système d'Euler* pour $\mathrm{V}^*(1)$, c'est-à-dire la construction d'une famille de classes de cohomologies $c_{\mathrm{M}} \in \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}(\zeta_{\mathrm{M}})}, \mathrm{T}^*(1))$, T^* réseau de V^* et M parcourant[29] les entiers ≥ 1, vérifiant les relations

$$\mathrm{cor}_{\mathbf{Q}(\zeta_{\mathrm{M}\ell})/\mathbf{Q}(\zeta_{\mathrm{M}})} c_{\mathrm{M}\ell} = \begin{cases} c_{\mathrm{M}} & \text{si } \ell | \mathrm{M}, \\ c_{\mathrm{M}} \star \mathrm{P}_\ell(\mathrm{Fr}_\ell^{-1}) & \text{si } \ell \nmid \mathrm{M} \text{ et V est non ramifiée en } \ell, \end{cases}$$

où $\mathrm{P}_\ell(\ell^{-s})$ est le facteur d'Euler[30] en ℓ de la fonction L attachée à V. On obtient alors une borne pour l'ordre du groupe de Selmer de V en termes de l'indice de c_1 dans $\mathrm{H}^1(\mathscr{G}_{\mathbf{Q}}, \mathrm{T}^*(1))$. Cette borne ne représente qu'une partie du travail pour obtenir des énoncés du type de la conjecture de Birch et Swinnerton-Dyer car il reste à relier l'indice de c_1 dans $\mathrm{H}^1(\mathscr{G}_{\mathbf{Q}}, \mathrm{T}^*(1))$ à une valeur spéciale de fonction L.

0.6.2. *Conjectures de Beilinson et systèmes d'Euler.* La construction de systèmes d'Euler est une activité totalement artisanale. Si V est la réalisation p-adique d'un motif $\mathbb{M}$, on peut essayer de construire « géométriquement » des éléments des groupes $\mathrm{H}^1(\mathbf{Q}(\zeta_{\mathrm{M}}), \mathbb{M}^*(1))$ d'extensions du motif trivial par le motif $\mathbb{M}^*(1)$ et considérer leurs réalisations p-adiques. L'existence ou la non existence de telles extensions est prédite par la conjecture de Beilinson [7]. D'après cette conjecture, si $\mathrm{L}(\mathbb{M},\eta,s)$ a un zéro simple en $s = 0$ pour tout caractère de Dirichlet η, il existe une famille $c_{\mathrm{M}} \in \mathrm{H}^1(\mathbf{Q}(\zeta_{\mathrm{M}}), \mathbb{M}^*(1))$,

[28] Profitons de l'occasion pour signaler que, contrairement à ce que prétend une rumeur persistante, on ne semble pas savoir démontrer que $Ш_{p^\infty}(\mathrm{E}/\mathrm{K})$ est divisible pour presque tout p. Cette rumeur provient d'une note de bas de page [32, p. 240] dans laquelle Cassels écrit que Shafarevitch lui a dit savoir démontrer le résultat en question, mais Colliot-Thélène m'a signalé que, dans [33, p. 277], Cassels écrit que Shafarevich lui a dit que la preuve prévue s'était heurtée à des difficultés imprévues...

[29] Plus généralement, on peut remplacer $\mathbf{Q}$ par une extension finie F et la tour des corps cyclotomiques par les extensions finies K de F contenues dans une extension abélienne suffisamment grande F_∞ de F.

[30] i.e. $\mathrm{P}_\ell(\mathrm{X}) = \det(1 - \mathrm{X} \cdot \mathrm{Fr}_\ell^{-1}|_{\mathrm{V}})$.

$\mathrm{M} \geq 1$ et une constante C, telle que l'on ait

$$\mathrm{L}'(\mathbb{M}, \eta, 0) = \mathrm{C} \cdot \sum_{\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_{\mathrm{M}})/\mathbf{Q})} \eta(\sigma) \cdot \mathrm{reg}_\infty(c_{\mathrm{M}} \star \sigma),$$

pour tout $\mathrm{M} \geq 1$ et tout caractère η de conducteur M, où reg_∞ est l'application régulateur. De tels éléments sont (conjecturalement) uniquement déterminés à addition près d'éléments de torsion et, dans les cas favorables[31], leurs réalisations p-adiques forment un système d'Euler[32].

0.6.3. *Torsion à la Soulé et lois de réciprocité explicites.* On dispose d'une méthode (torsion à la Soulé [181]) pour obtenir un système d'Euler pour $\mathrm{V}^*(k)$, $k \in \mathbf{Z}$, à partir d'un système d'Euler pour $\mathrm{V}^*(1)$. En d'autres termes, la construction d'un système d'Euler pour n'importe quel tordu de $\mathrm{V}^*(1)$ permet de borner le groupe de Selmer de V.

Comme nous l'avons mentionné plus haut, la borne obtenue ne fait absolument pas intervenir de valeur spéciale de fonction L. Cependant, l'expérience montre que, si on est parti d'un système d'Euler relié aux valeurs spéciales de fonctions L pour un tordu de $\mathrm{V}^*(1)$, alors les tordus du système d'Euler continuent[33] à être reliés aux valeurs spéciales de fonctions L en les points considérés. C'est le royaume des lois de réciprocité explicites [96, 195, 44, 27, 98, 99, 51, 103, 11, 36, 101, 162, 164, 78, 79, ...] qui constituent en général le point le plus technique des démonstrations.

0.6.4. *Le système d'Euler de Kato* ([102, §§ 1-5 et § 8]). Si E est une courbe elliptique définie sur $\mathbf{Q}$ et $\mathbb{M}$ est le motif $h_1(\mathrm{E})$ (dont la réalisation p-adique est $\mathbf{Q}_p \otimes \mathrm{T}_p(\mathrm{E})$, où $\mathrm{T}_p(\mathrm{E})$ est le module de Tate de E), alors $\mathrm{H}^1(\mathbf{Q}(\zeta_{\mathrm{M}}), \mathbb{M}^*(1)) = \mathbf{Q} \otimes \mathrm{E}(\mathbf{Q}(\zeta_{\mathrm{M}}))$, et on

[31] C'est le cas pour les motifs attachés aux formes modulaires. Dans le cas général, il y a une obstruction de nature locale à l'existence de systèmes compatibles de classes de cohomologies « géométriques » à valeurs dans un réseau (cf. [144, 145] pour les cas de « bonne réduction » et de « réduction semi-stable » et [13] pour le cas général). Les éléments prédits par la conjecture de Beilinson doivent donc faire intervenir des dénominateurs, et il semble intéressant d'essayer de comprendre ce que l'on peut en tirer (par exemple pour un motif dont tous les nombres de Hodge sont différents car, dans ce cas, la conjecture de Beilinson a l'air de suggérer l'apparition d'un nouveau système compatible « de rang 1 » en chacun des twists par un des poids de Hodge-Tate).

[32] On peut voir le système c_{M}, $\mathrm{M} \geq 1$, comme une incarnation algébrique de la fonction L du motif $\mathbb{M}$. Si $\mathrm{L}(\mathbb{M}, \eta, s)$ a, en $s = 0$, un zéro d'ordre $r \geq 2$, alors le groupe $\mathrm{H}^1(\mathbf{Q}(\zeta_{\mathrm{M}}), \mathbb{M}^*(1))$ est un $\mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(\zeta_{\mathrm{M}})/\mathbf{Q})]$-module de rang r ; c'est le déterminant de ce groupe qui est relié à la fonction L via l'application régulateur, et l'existence d'un système d'Euler ne semble pas automatique ; en tout cas, on n'a aucun exemple auquel se rattacher pour essayer de deviner ce qui est vrai.

[33] Il y a de quoi rester un peu perplexe : on part d'un système compatible d'éléments motiviques pour l'extension cyclotomique, on choisit un nombre premier p, on prend la réalisation étale p-adique du système, on la tord par une représentation « indépendante de p », on fait entrer le résultat du côté galoisien dans le labyrinthe des anneaux de Fontaine, et il ressort du côté de Rham sous la forme d'un système compatible pour l'extension cyclotomique quasiment *indépendant de* p ! C'est d'autant plus remarquable qu'il n'y a rien qui puisse permettre de prédire, dans l'état actuel de notre compréhension, que les éléments que l'on va récupérer vont être définis sur $\overline{\mathbf{Q}}$...

est ramené à construire de manière systématique des points de E rationnels sur $\mathbf{Q}(\zeta_{\mathrm{M}})$. Malheureusement, la conjecture de Birch et Swinnerton-Dyer et le théorème de Rohrlich (cf. (ii) de la rem. 0.24) montrent que ceci n'est pas possible. Par contre, si $n \geq 1$, le groupe $\mathrm{H}^1(\mathbf{Q}(\zeta_{\mathrm{M}}), h_1(\mathrm{E})(n))$ est un $\mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(\zeta_{\mathrm{M}})/\mathbf{Q})]$-module de rang 1 d'après la conjecture de Beilinson car $\mathrm{L}(\mathrm{E}, \eta, s)$ a un zéro simple[34] en $s = 1 - n$, quel que soit le caractère de Dirichlet η. On est donc ramené à construire explicitement les éléments de $\mathrm{H}^1(\mathbf{Q}(\zeta_{\mathrm{M}}), h_1(\mathrm{E})(n))$ dont l'existence est prédite par la conjecture de Beilinson et à les normaliser correctement pour en faire un système d'Euler.

Pour $n = 1$, le projet a été mené à bien[35] par Beilinson [7] qui a construit, en partant d'unités de Siegel[36] sur la courbe modulaire Y(N) (avec N = multiple du conducteur de E), des éléments dans le K_2 de la courbe[37] elliptique E dont les images par l'application régulateur font intervenir les dérivées premières en $s = 0$ des tordues de la fonction L de E par les caractères de Dirichlet.

La théorie de Kummer permet d'associer à une unité sur Y(M) (et donc à une unité de Siegel) une classe de cohomologie dans $\mathrm{H}^1_{\mathrm{et}}(\mathrm{Y}(\mathrm{M}), \mathbf{Z}_p(1))$. En faisant le cup-produit de deux de ces classes, on obtient une classe dans $\mathrm{H}^2_{\mathrm{et}}(\mathrm{Y}(\mathrm{M}), \mathbf{Z}_p(2))$ qui n'est autre que l'image, au signe près, de l'élément de Beilinson par l'application classe de Chern. Kato a trouvé un moyen de normaliser[38] les unités de Siegel et les éléments de Beilinson pour

---

[34] Ce zéro peut être d'ordre ≥ 1 si $n = 0$ et E a potentiellement réduction multiplicative en une place divisant le conducteur de η, la fonction $\mathrm{L}(\mathrm{E}, \eta, s)$ n'étant pas forcément primitive.

[35] Beilinson ne s'est pas arrêté en si bon chemin : comme confirmation de ses conjectures générales sur les valeurs spéciales de fonctions L de motifs, il a [8]

• construit, si $k \geq 2$, des éléments « d'Eisenstein » dans la K-théorie de la variété de Kuga-Sato $\mathrm{Y}^{(k-2)}(\mathrm{M})$ (rappelons que Y(M) étant un espace de module de courbes elliptiques, on dispose d'une courbe elliptique universelle $\mathscr{E}$ au-dessus de Y(M) ; la variété $\mathrm{Y}^{(k-2)}(\mathrm{M})$ est alors obtenue à partir du produit de $k-2$ copies de $\mathscr{E}$ au-dessus de Y(M)) dans la cohomologie de laquelle sont découpés [160] les motifs associés aux formes modulaires de poids k ; pour $k = 2$, on récupère les unités de Siegel ;

• déduit de ces éléments d'Eisenstein, par cup-produit et image directe, des éléments dans la cohomologie motivique de la courbe modulaire ;

• calculé l'image de ces éléments par l'application régulateur et vérifié que le résultat faisait intervenir les dérivées des fonctions L de formes modulaires de poids 2 en $s = 2 - k$.

Par ailleurs, Scholl [67, 163] a construit, par cup-produit à partir des éléments d'Eisenstein de Beilinson, des éléments dans la cohomologie motivique de la variété de Kuga-Sato $\mathrm{Y}^{(k-2)}(\mathrm{M})$ dont l'image par l'application régulateur fait intervenir les dérivées des fonctions L de formes modulaires de poids k en $s = -n$, $n \in \mathbf{N}$.

[36] Ces unités, appelées aussi *unités modulaires*, sont définies comme des produits infinis (cf. [108] par exemple) ; on obtient de la sorte des fonctions modulaires sans zéro ni pôle sur le demi-plan de Poincaré dont le q-développement est à coefficients dans $\mathbf{Q}(\zeta_{\mathrm{N}})$, ce qui nous fournit des fonctions inversibles sur la courbe Y(N) qui est une courbe algébrique affine définie sur $\mathbf{Q}(\zeta_{\mathrm{N}})$.

[37] On commence par construire des éléments dans le K_2 de Y(N) que l'on projette dans $\mathrm{K}_2(\mathrm{E})$ en utilisant le morphisme $\mathrm{Y}(\mathrm{N}) \to \mathrm{E}$ fourni par le théorème 0.20.

[38] Scholl [162] en a fait de même avec les éléments de Beilinson dans la K-théorie de la variété de Kuga-Sato.

obtenir de la sorte un système cohérent de classes $c_{\mathrm{M}} \in \mathrm{H}^2_{\mathrm{et}}(\mathrm{Y}(\mathrm{M}), \mathbf{Z}_p(2))$, $\mathrm{M} \geq 1$. En utilisant la technique de torsion à la Soulé (pour une extension de type $\mathbf{GL}_2$ au lieu de l'extension cyclotomique qui est de type $\mathbf{GL}_1$), cela lui permet de construire, si $k \geq 2$ et $j \in \mathbf{Z}$, un système cohérent de classes $c_{\mathrm{M}}(k,j) \in \mathrm{H}^2_{\mathrm{et}}(\mathrm{Y}(\mathrm{M}), \mathrm{W}_k(j))$, $\mathrm{M} \geq 1$, où W_k est le système local sur $\mathrm{Y}(\mathrm{M})$ dans la cohomologie duquel on découpe les représentations p-adiques associées aux formes modulaires de poids k et niveau M.

Maintenant, la courbe $\mathrm{Y}(\mathrm{M})$ étant affine, on a $\mathrm{H}^2_{\mathrm{et}}(\mathrm{Y}(\mathrm{M})_{\overline{\mathbf{Q}}}, \mathrm{W}_k(j)) = 0$, ce qui fournit une application naturelle[39]

$$\mathrm{H}^2_{\mathrm{et}}(\mathrm{Y}(\mathrm{M}), \mathrm{W}_k(j)) \to \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}(\zeta_{\mathrm{M}})}, \mathrm{H}^1_{\mathrm{et}}(\mathrm{Y}(\mathrm{M})_{\overline{\mathbf{Q}}}, \mathrm{W}_k(j))).$$

Si f est une forme primitive de poids k et de niveau divisant M, il n'y a plus qu'à projeter l'image de $c_{\mathrm{M}}(k,j)$ sur la composante de $\mathrm{H}^1_{\mathrm{et}}(\mathrm{Y}(\mathrm{M})_{\overline{\mathbf{Q}}}, \mathrm{W}_k(j))$ correspondant à f, pour obtenir le système d'Euler $c_{\mathrm{M}}(f,j) \in \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}(\zeta_{\mathrm{M}})}, \mathrm{V}_f(j))$, $\mathrm{M} \geq 1$ que l'on cherchait à construire[40] (ce système d'Euler permet de borner le groupe de Selmer de $\mathrm{V}_f(j)^*(1) = \mathrm{V}_{f^*}(k-j)$).

0.6.5. *La loi de réciprocité explicite de Kato* ([101] et [102, §§ 9-11]). Le point le plus délicat est de relier les classes de cohomologie construites dans le numéro précédent aux valeurs spéciales de fonctions L. Pour ce faire, on utilise deux applications *exponentielles duales* utilisant l'anneau $\mathbb{B}^+_{\mathrm{dR}}$ de Fontaine [73, 74, 57, 55] pour deux corps différents : le corps $\overline{\mathbf{Q}}_p$, et le corps $\overline{\mathscr{K}}$, clôture algébrique du corps des fractions[41] $\mathscr{K}$ du complété de $\mathbf{Z}_p[[q]][q^{-1}]$ pour la topologie p-adique. Si V est une représentation de de Rham de $\mathscr{G}_{\mathbf{Q}_p(\zeta_{\mathrm{M}})}$, le cup-produit avec $\log \chi_{\mathrm{cycl}} \in \mathrm{H}^0(\mathscr{G}_{\mathbf{Q}_p(\zeta_{\mathrm{M}})}, \mathbf{Q}_p)$ fournit un isomorphisme

$$\mathrm{H}^0(\mathscr{G}_{\mathbf{Q}_p(\zeta_{\mathrm{M}})}, \mathbb{B}^+_{\mathrm{dR}}(\overline{\mathbf{Q}}_p) \otimes \mathrm{V}) \cong \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}_p(\zeta_{\mathrm{M}})}, \mathbb{B}^+_{\mathrm{dR}}(\overline{\mathbf{Q}}_p) \otimes \mathrm{V}),$$

et on définit $\exp^*$ comme l'inverse de cet isomorphisme. Ce qui précède s'applique en particulier à la représentation $\mathrm{W}_{k,j} = \mathrm{H}^1_{\mathrm{et}}(\mathrm{Y}(\mathrm{M})_{\overline{\mathbf{Q}}_p}, \mathrm{W}_k(j))$. Par ailleurs, si $\mathrm{M} \geq 1$, et

[39]Gealy [80] a vérifié que, si $j \geq k$, les éléments de Kato et les éléments (cf. note 35) de Beilinson ($j = k$) et Scholl ($j \geq k$) ont même image dans $\mathrm{H}^1(\mathscr{G}_{\mathbf{Q}(\zeta_{\mathrm{M}})}, \mathrm{H}^1_{\mathrm{et}}(\mathrm{Y}(\mathrm{M})_{\overline{\mathbf{Q}}}, \mathrm{W}_k(j)))$, ce qui est une illustration du phénomène mentionné au n$^{\mathrm{o}}$ 0.6.3. Scholl a démontré (cf. note 43) un résultat du même type en ce qui concerne les éléments de Beilinson.

[40]Cette description « du » système d'Euler associé à f est un peu idéalisée. On est en fait forcé de faire un certain nombre de choix au cours de la construction, ce qui nous fournit toute une famille de systèmes d'Euler, mais aucun d'eux n'est optimal (i.e. les valeurs spéciales de fonctions L que l'on obtient via la loi de réciprocité explicite sont multipliées par des facteurs parasites). On peut construire un système d'Euler optimal [102, § 12] à partir de cette famille de systèmes d'Euler, mais c'est au prix de pas mal de complications techniques... En particulier, la normalisation de ce système d'Euler passe par la loi de réciprocité explicite.

[41]Ce corps apparaît naturellement comme complété du corps des fonctions de $\mathrm{Y}(1)$ en la pointe $i\infty$. En associant son q-développement à une forme modulaire, cela permet de voir les formes modulaires comme des éléments de $\overline{\mathscr{K}}$.

$\mathscr{K}_{\mathrm{M}} = \mathscr{K}[q^{1/\mathrm{M}}, \zeta_{\mathrm{M}}]$, on dispose, si $1 \leq j \leq k-1$, d'un isomorphisme naturel

$$\exp^* : \mathrm{H}^2(\mathscr{G}_{\mathscr{K}_{\mathrm{M}}}, \mathbb{B}^+_{\mathrm{dR}}(\overline{\mathscr{K}}) \otimes \mathrm{W}_k(j)) \cong \mathscr{K}_{\mathrm{M}}.$$

En utilisant ces deux isomorphismes, l'injection naturelle de $\mathbb{B}^+_{\mathrm{dR}}(\overline{\mathbf{Q}}_p)$ dans $\mathbb{B}^+_{\mathrm{dR}}(\overline{\mathscr{K}})$, la localisation de $\mathrm{Y}(\mathrm{M})_{\mathbf{Q}_p(\zeta_{\mathrm{M}})}$ à $\mathscr{K}_{\mathrm{M}}$ et l'isomorphisme[42]

$$\mathrm{H}^1\big(\mathscr{G}_{\mathbf{Q}_p(\zeta_{\mathrm{M}})}, \mathbb{B}^+_{\mathrm{dR}}(\overline{\mathbf{Q}}_p) \otimes \mathrm{H}^1_{\mathrm{et}}\big(\mathrm{Y}(\mathrm{M})_{\overline{\mathbf{Q}}_p}, \mathrm{W}_k(j)\big)\big) \cong \mathrm{H}^2_{\mathrm{et}}\big(\mathrm{Y}(\mathrm{M})_{\mathbf{Q}_p(\zeta_{\mathrm{M}})}, \mathbb{B}^+_{\mathrm{dR}}(\overline{\mathbf{Q}}_p) \otimes \mathrm{W}_k(j)\big)$$

fourni par la suite spectrale de Hochschild-Serre, on obtient le diagramme suivant :

$$\begin{tikzcd}
 & \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}(\zeta_{\mathrm{M}})}, \mathrm{W}_{k,j}) \arrow[d] & \\
\mathrm{H}^0(\mathscr{G}_{\mathbf{Q}_p(\zeta_{\mathrm{M}})}, \mathbb{B}^+_{\mathrm{dR}}(\overline{\mathbf{Q}}_p) \otimes \mathrm{W}_{k,j}) & \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}_p(\zeta_{\mathrm{M}})}, \mathbb{B}^+_{\mathrm{dR}}(\overline{\mathbf{Q}}_p) \otimes \mathrm{W}_{k,j}) \arrow[l, "\exp^*"', "\sim"] \arrow[r, "\exp^*"] & \mathscr{K}_{\mathrm{M}}.
\end{tikzcd}$$

Le résultat crucial sur lequel tout repose est une formule explicite pour l'image de $c_{\mathrm{M}}(k,j)$, $1 \leq j \leq k-1$, dans $\mathscr{K}_{\mathrm{M}}$. Cette formule fait intervenir le q-développement du produit de deux séries d'Eisenstein[43]. En particulier, cela permet d'identifier $\mathrm{H}^0(\mathscr{G}_{\mathbf{Q}_p(\zeta_{\mathrm{M}})}, \mathbb{B}^+_{\mathrm{dR}}(\overline{\mathbf{Q}}_p) \otimes \mathrm{W}_{k,j})$ à un espace de formes modulaires et d'obtenir du même coup une version d'une partie du théorème de comparaison[44] entre la cohomologie étale p-adique et la cohomologie de de Rham.

Il reste à projeter tous les objets sur la composante correspondant à f pour terminer le calcul. Cette dernière étape demande de calculer le produit scalaire de Petersson de f avec un produit de deux séries d'Eisenstein, ce qui se fait au moyen de la méthode de Rankin, et le résultat fait intervenir les valeurs spéciales des fonctions L attachées à f et à ses tordues par des caractères de Dirichlet[45].

---

[42]Comme la cohomologie étale à coefficients dans quelque chose d'aussi gros que $\mathbb{B}^+_{\mathrm{dR}}(\overline{\mathbf{Q}}_p) \otimes \mathrm{W}_k(j)$ n'est pas vraiment définie, on utilise le fait que $\mathrm{Y}(\mathrm{M})$ est une courbe affine sur un corps et donc que sa cohomologie étale est aussi la cohomologie continue de son groupe fondamental.

[43]Scholl [164] a suivi le même chemin pour étudier le système d'Euler qu'il a construit en partant des éléments K-théoriques de Beilinson. En particulier, en utilisant une variante d'une loi de réciprocité explicite de Kato [101], il a calculé l'image par l'application $\exp^*$ du tordu à la Soulé de ce système d'Euler par $\mathbf{Q}_p(-1)$. Comme on tombe sur le même produit de séries d'Eisenstein que Kato pour $c_{\mathrm{M}}(k, k-1)$, cela permet, en utilisant le fait que les deux systèmes d'Euler vivent dans un même module de rang 1 sur l'algèbre d'Iwasawa (ce calcul de rang est un des résultats non triviaux que l'on obtient par la méthode des systèmes d'Euler), de montrer qu'ils coïncident.

[44]On peut se demander si l'identification ainsi obtenue est compatible avec celle déduite des théorèmes de comparaison de Faltings [72] ou Tsuji [189, 190] ; Kato a vérifié [102, §11] la compatibilité avec le théorème de comparaison de Tsuji, et la compatibilité avec celui de Faltings devrait être plus ou moins automatique car la définition des applications $\exp^*$ repose sur la notion d'extension presque étale qui est au cœur de l'approche de Faltings. D'un autre côté, cette compatibilité ne semble pas nécessaire pour les applications aux fonctions L de formes modulaires.

[45]Ce type de résultats remonte aux travaux de Shimura [177].

0.6.6. *La machine de Perrin-Riou* [141, 142, 54] *et la conjecture principale.* Une comparaison des formules ainsi obtenues avec celles fournies par la loi de réciprocité explicite [36] pour les représentations de de Rham de $\mathscr{G}_{\mathbf{Q}_p(\zeta_{\mathrm{M}})}$ permet de montrer que la fonction L p-adique attachée à une forme modulaire est l'image du système d'Euler de Kato par la machine de Perrin-Riou[46], ce qui permet d'utiliser les résultats généraux de Perrin-Riou [142, 54] concernant les fonctions L p-adiques attachées aux représentations p-adiques. En utilisant cette machine, Perrin-Riou a construit (de manière purement algébrique) une fonction L d'Iwasawa attachée à une représentation p-adique de $\mathscr{G}_{\mathbf{Q}}$ et minoré l'ordre du zéro d'une telle fonction en tous les entiers en termes de groupes de Selmer[47]. Comme par ailleurs, la méthode de Kolyvagin [100, 143, 159] permet de démontrer que la fonction L d'Iwasawa divise la fonction L p-adique, cela nous fournit la minoration cherchée pour l'ordre du zéro de la fonction L p-adique, ainsi qu'une moitié de la « conjecture principale » [142, 54] selon laquelle les fonctions L p-adique et d'Iwasawa sont égales, à multiplication près par une unité de l'algèbre d'Iwasawa.

0.7. **Remords**

Les points suivants mériteraient qu'on leur consacre plus de place.

0.7.1. *Formes modulaires à multiplication complexe.* Les formes modulaires correspondent (au moins conjecturalement) aux motifs de rang 2 sur $\mathbf{Q}$. Parmi ceux-ci se trouvent les motifs de type CM qui sont de rang 1 sur une extension quadratique imaginaire K de $\mathbf{Q}$, mais sont vus comme motifs de rang 2 sur $\mathbf{Q}$. Ces motifs de type CM sont plus faciles à manier, et tous les énoncés des n° 0.3-0.5 ont été démontrés dans le cas de type CM avant le cas général. Par exemple, pour une courbe elliptique E de type CM, le prolongement analytique de la fonction $\mathrm{L}(\mathrm{E}, s)$ remonte à Deuring [68] : cette fonction s'exprime en termes de fonction L attachées à des caractères de Hecke de K ; le théorème 0.20 a, quant à lui été démontré par Shimura [175] ; la finitude de $\mathrm{E}(\mathbf{Q})$, si $\mathrm{L}(\mathrm{E}, 1) \neq 0$, est due à Coates et Wiles [41, 42, 111], et la finitude de Ш(E) sous la même hypothèse, à Rubin [157] dont la démonstration avait été inspirée par un résultat de Thaine [187] que l'on peut voir comme une première approximation de la méthode de Kolyvagin. Finalement, l'inégalité entre l'ordre du zéro de la fonction L p-adique et le corang du groupe de Selmer d'un motif à multiplication complexe est une conséquence de la conjecture principale démontrée par Rubin [158].

En fait, on ne peut pas retrouver les résultats de Rubin via le système d'Euler de Kato car l'image de $\mathscr{G}_{\mathbf{Q}}$ dans la représentation p-adique V associée à un motif de type CM est

[46] Cette machine est une vaste généralisation des séries de Coleman [43] qui fournissent une construction des fonctions L p-adiques attachées aux caractères de Dirichlet à partir du système d'Euler des unités cyclotomiques

[47] Elle a de plus vérifié, pour cette fonction L d'Iwasawa, la conjecture de Bloch-Kato à une unité près dans le cas où la minoration précédente est une égalité, ce qui devrait toujours être le cas sauf si on est en présence de zéros « triviaux » ou « supplémentaires ».

trop petite pour que la méthode des systèmes d'Euler puisse fonctionner. La démonstration de Rubin utilise à la place le système d'Euler des unités elliptiques (cf. aussi [1]).

0.7.2. *Courbes elliptiques supersingulières.* Si E est une courbe elliptique ordinaire, définie sur $\mathbf{Q}$, le dual de Pontryagin de $\mathrm{Sel}_p(\mathrm{E}/\mathbf{Q}(\zeta_{p^\infty}))$ est de torsion comme module sur l'algèbre d'Iwasawa (ex-conjecture de Mazur, maintenant un théorème grâce aux travaux de Kato). On en déduit le fait [113] que $\mathrm{E}(\mathbf{Q}(\zeta_{p^\infty}))$ est de rang fini et qu'il existe $n_0 \in \mathbf{N}$, $\lambda, \mu \in \mathbf{N}$ et $\nu \in \mathbf{Z}$ tels que, si $n \geq n_0$, on ait

$$\left|Ш(\mathrm{E}/\mathbf{Q}(\zeta_{p^n}))/Ш(\mathrm{E}/\mathbf{Q}(\zeta_{p^{n_0}}))\right| = p^{\lambda n+\mu p^n+\nu}.$$

Si E est supersingulière, le dual de Pontryagin de $\mathrm{Sel}_p(\mathrm{E}/\mathbf{Q}(\zeta_{p^\infty}))$ n'est plus de torsion[48] et la situation est plus compliquée, mais on peut quand même, en utilisant les résultats de Kato, montrer [140, 147] que $\mathrm{E}(\mathbf{Q}(\zeta_{p^\infty}))$ est de rang fini, et donner des formules [109, 147] pour la croissance du groupe de Tate-Shafarevitch dans la tour cyclotomique. Si $p \geq 5$ ou, plus généralement, si $a_p = 0$, une remarque[49] de Pollack [148] a donné naissance à une série de jolis travaux [106, 93, 149, 61] précisant et étendant les résultats mentionnés ci-dessus.

0.7.3. *La direction anticyclotomique.* Soit E une courbe elliptique définie sur $\mathbf{Q}$ ou, plus généralement, soit f une forme primitive de poids $k \geq 2$ pair, dont les coefficients du q-développement sont totalement réels. Soit K une extension quadratique de $\mathbf{Q}$. Si on regarde l'équation fonctionnelle de $\mathrm{L}(f \otimes \eta, s)$ pour $\eta : \mathrm{Gal}(\mathrm{K}^{\mathrm{ab}}/\mathrm{K}) \to \mathbf{C}^*$ d'ordre fini, on s'aperçoit qu'il existe une grosse sous-extension L_∞ de l'extension anticyclotomique[50] $\mathrm{K}^{\mathrm{anti}}$ de K telle que l'on ait $\mathrm{L}(f \otimes \eta, \frac{k}{2}) = 0$, quel que soit $\eta : \mathrm{Gal}(\mathrm{L}_\infty/\mathrm{K}) \to \mathbf{C}^*$ d'ordre fini. Ceci laisse entrevoir la possibilité de construire de manière systématique des éléments motiviques dans $\mathrm{H}^1(\mathscr{G}_\mathrm{L}, \mathrm{V}_f(\frac{k}{2})^*(1)) = \mathrm{H}^1(\mathscr{G}_\mathrm{L}, \mathrm{V}_f(\frac{k}{2}))$, L parcourant les extensions finies de K contenues dans L_∞. De fait, si K est imaginaire, on sait construire ces éléments : ce sont les points de Heegner[51], ou, si $k > 2$, les cycles de Heegner.

Ces points et cycles de Heegner jouent un rôle fondamental dans la démonstration du théorème de Gross-Zagier [86] et de son analogue p-adique [136, 127], et Kolyvagin a développé ses techniques de dérivation pour démontrer l'égalité $r(\mathrm{E}) = r_\infty(\mathrm{E})$ et la

[48]Par exemple, si $(\Omega_\mathrm{E}^+)^{-1}\mathrm{L}(\mathrm{E}, 1)$ est une unité p-adique, Kurihara [109] a montré, en utilisant les résultats de Kato, que ce module est en fait libre de rang 1, ce qui constitue une vérification de la conjecture principale. Perrin-Riou [147] a généralisé le résultat de Kurihara, ce qui lui permet de vérifier, grâce à des calculs sur ordinateur, la conjecture principale dans des cas particuliers, sans supposer que $(\Omega_\mathrm{E}^+)^{-1}\mathrm{L}(\mathrm{E}, 1)$ est une unité p-adique ou même que $\mathrm{L}(\mathrm{E}, 1) \neq 0$.

[49]Cette remarque part de l'observation que, si $a_p = 0$, et si $1 - a_p p^{-s} + p^{1-2s} = (1 - \alpha_1 p^{-s})(1 - \alpha_2 p^{-s})$, alors $\alpha_1 = -\alpha_2$, et les distributions $\mu_{\mathrm{E},\alpha_1} \pm \mu_{\mathrm{E},\alpha_2}$ du th. 0.8 ont beaucoup de zéros triviaux.

[50]$\mathrm{K}^{\mathrm{anti}}$ est la plus grande extension abélienne L de K telle que l'élément non trivial de $\mathrm{Gal}(\mathrm{K}/\mathbf{Q})$ agisse par multiplication par -1 sur $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$.

[51]Si $\pi_\mathrm{E} : \mathscr{H} \to \mathrm{E}$ est une uniformisation de E par le demi-plan de Poincaré se factorisant à travers $\mathrm{Y}_0(\mathrm{N}_\mathrm{E})$, les points de Heegner sont les images de $\mathrm{K} \cap \mathscr{H}$.

finitude de Ш(E) pour une courbe elliptique ayant un zéro d'ordre ≤ 1 en $s = 1$, à partir du système d'Euler des points de Heegner [107] (cf. [125] pour une extension en poids supérieur à 2). Ils jouent aussi un rôle fondamental dans le résultat de Nekovář [128] sur la parité du corang des groupes de Selmer via la démonstration d'une conjecture de Mazur [114], sur la non trivialité « asymptotique » des points de Heegner, par Vatsal [191] et Cornut [49] (voir aussi [117]).

Par ailleurs, ces points et cycles de Heegner, et leurs analogues p-adiques obtenus en utilisant l'uniformisation de courbes de Shimura par le demi-plan de Drinfeld (demi-plan de Poincaré p-adique) permettent de démontrer [14, 15, 16, 17, 20, 18, 19, 61, 94] des versions anticyclotomiques de la plupart des résultats des n° 0.3 et 0.5. Nous renvoyons à [18] pour une introduction à ce cercle d'idées. Signalons juste que la situation anticyclotomique présente quelques particularités intéressantes. C'est le seul cas, à ma connaissance, où l'on sache construire une fonction L p-adique comme transformée de Mellin d'une forme modulaire p-adique (i.e. une construction purement p-adique de la fonction L p-adique). En outre, Darmon [60] a proposé une construction conjecturale de points rationnels sur des extensions abéliennes d'un corps quadratique réel qui mélange le complexe et le p-adique de manière particulièrement alléchante.

0.7.4. *La méthode de Ribet.* On ne peut espérer démontrer, à partir d'un système d'Euler, qu'une divisibilité du type « ordre d'un groupe de Selmer » divise « valeur spéciale de fonction L ». Dans le cas des motifs de rang 1 sur $\mathbf{Q}$, cela suffit pour montrer une égalité car on dispose de la formule analytique du nombre de classes[52].

Dans le cas général, il semble qu'il va falloir construire explicitement des éléments dans les groupes de Selmer pour démontrer une divisibilité dans l'autre sens. Pour les motifs de rang 1 sur $\mathbf{Q}$, cela a été fait par Ribet [152] en utilisant le fait que la divisibilité d'une valeur spéciale de fonction L se traduit par l'existence d'une congruence entre une série d'Eisenstein (i.e. une forme modulaire « provenant de $\mathbf{GL}_1$ ») et une forme parabolique f ; on peut alors utiliser la représentation galoisienne attachée à f pour construire un élément du groupe de Selmer du motif de rang 1 (qui n'est rien d'autre qu'une partie du groupe des classes d'une extension cyclotomique). La méthode de Ribet a été étendue par Mazur et Wiles [123, 39], ce qui leur a permis de démontrer la conjecture principale dans le cas cyclotomique (en fait ils ne démontrent qu'une divisibilité et concluent en utilisant la formule analytique du nombre de classes).

Ce n'est que récemment que la méthode de Ribet a été étendue aux motifs de rang 2 (les ingrédients automorphes entrant dans les constructions, ainsi que les démonstrations, se sont nettement sophistiqués[53] en passant de $\mathbf{GL}_1$ à $\mathbf{GL}_2$...). Si f est une forme primitive

[52]On tord pour se ramener aux caractères d'ordre fini et on fait le produit sur tous les caractères de conducteur divisant un entier N fixé ; la formule analytique du nombre de classes pour $\mathbf{Q}(\zeta_{\mathrm{N}})$ montrant alors que le produit de ces divisibilités est une égalité, ce qui permet de conclure.

[53] En particulier, la construction ne fournit pas automatiquement, contrairement au cas considéré par Ribet, les extensions que l'on cherche : les semi-simplifiées des représentations que l'on construit par voie

de poids $2k$ dont la fonction L vérifie l'équation fonctionnelle $\Lambda(f,s) = -\Lambda(f,2k-s)$, où l'on a posé $\Lambda(f,s) = \frac{\Gamma(s)}{(2\pi)^s}\mathrm{N}^{s/2}\mathrm{L}(f,s)$, la fonction $\mathrm{L}(f,s)$ a un zéro d'ordre ≥ 1 (car impair) en $s = k$, et les conjectures de Beilinson et de Bloch-Kato prédisent l'existence d'extensions non triviales, ayant « bonne réduction partout », de la représentation triviale par $\mathrm{V}_f(k)$. En utilisant des congruences entre formes automorphes pour $\mathbf{U}(2,1)$, Bellaïche [9] a démontré l'existence de telles extensions modulo p, pour « beaucoup de p », si f est de type CM. En utilisant des familles de représentations galoisiennes associées à des formes automorphes pour $\mathbf{GSp}_4$, Skinner et Urban [178] ont construit (au moins en niveau 1) de telles extensions dans le cas où f est ordinaire en p, et Bellaïche et Chenevier [10] ont combiné[54] les méthodes de [9, 178], pour traiter le cas CM en utilisant des familles de représentations galoisiennes associées à des formes automorphes pour $\mathbf{U}(3)$. Il est à noter que, dans le cas CM, on peut déduire l'existence de telles extensions des travaux de Rubin [158] sur la conjecture principale (en utilisant encore une fois la formule analytique du nombre de classes pour transformer une divisibilité dans le mauvais sens en égalité), et que, dans le cas général, cette existence peut aussi se déduire du résultat de Nekovář [128] concernant la parité du corang des groupes de Selmer, mais que les constructions automorphes de Bellaïche, Chenevier, Skinner et Urban sont pleines de promesses pour l'avenir. Par ailleurs, en ce qui concerne la conjecture principale pour une forme modulaire ordinaire en p, Skinner et Urban [179] ont démontré, modulo l'existence de représentations galoisiennes attachées aux formes automorphes sur le groupe $\mathbf{U}(2,2)$, la divisibilité opposée à celle démontrée par Kato, ce qui fournit une démonstration de cette conjecture principale (malheureusement conditionnelle pour le moment).

Signalons encore, dans ce cercle d'idées, dans le cas des motifs de rang 2 de type CM, la méthode de Mazur et Tilouine [122, 188] et son extension [90, 91, 89] à un corps CM quelconque.

---

automorphe comportent 3 facteurs au lieu de 2, et il faut éliminer les extensions parasites éventuelles pour démontrer que l'on a bien construit l'extension voulue. Cette problématique apparaît dans [9], et la non existence d'extensions parasites correspond à un cas particulier des conjectures de Bloch-Kato [27] qui peut se déduire, dans le cas considéré par Bellaïche, des résultats de Rubin [158]. Pour résoudre le même type de problèmes dans leur cas [178], Skinner et Urban s'appuient à la place sur le théorème 0.22 (de Kato). Par ailleurs, un résultat récent de Kisin [105], concernant la variation du $\mathrm{D}_{\mathrm{cris}}$ d'une représentation dans une famille, joue un grand rôle pour contrôler la bonne réduction en p des extensions construites via les familles de formes automorphes [178, 10].

[54]Ils ont aussi réussi à éliminer le recours aux résultats profonds de Rubin et Kato pour se débarrasser des extensions parasites éventuelles mentionnées dans la note 53, et ont ramené leur non existence à celle d'extensions de $\mathbf{Q}_p$ par $\mathbf{Q}_p(1)$ (sur un corps quadratique imaginaire) ayant bonne réduction partout, ce qui suit de la théorie de Kummer et de ce que l'anneau des entiers d'un corps quadratique imaginaire n'a pas d'unité d'ordre infini.

0.8. **Organisation de l'article**

La démonstration de Kato des th. 0.15, 0.22 et 0.23 est découpée en quatre gros articles [100, 101, 102, 103] ; le texte principal ne couvre pas la totalité de cette démonstration. Il contient en particulier une construction du système d'Euler de Kato (chap. 1), une esquisse de démonstration de la loi de réciprocité explicite de Kato (chap. 2), et une analyse assez précise du lien entre le système d'Euler de Kato et les fonctions L p-adiques de formes modulaires (chap. 4). Il manque un traitement de la méthode des systèmes d'Euler (correspondant à [100], et utilisée de manière cruciale pour démontrer les résultats du chap. 3), ainsi que des rappels un peu conséquents sur la machine de Perrin-Riou et les résultats qui en sortent (correspondant aux §§ 17-18 de [102]), mais ces techniques ont déjà fait l'objet d'exposés [138, 54] à ce séminaire. J'ai assez sensiblement modifié le point de vue par rapport à celui de Kato ; j'espère que cela n'a pas introduit d'erreur fatale (je n'ai pas vérifié tous les détails, mais ça a une bonne tête).

1. LE SYSTÈME D'EULER DE KATO

Ce chapitre est consacré à la construction du (ou plutôt des) système d'Euler de Kato. Par rapport à la présentation qu'en donnent Kato [102] ou Scholl [162], il y a deux différences sensibles : la situation a été complètement adélisée, ce qui rend les calculs de corestriction quasi automatiques (mais ne rend pas les notations plus digestes...) et la géométrie algébrique a disparu (par exemple, la cohomologie étale des courbes modulaires a été remplacée par la cohomologie continue de leur groupe fondamental, ou plutôt d'un groupe $\Pi_{\mathbf{Q}}$ qui leur est commensurable, et qui est défini de manière purement modulaire).

1.1. **Notations et préliminaires**

1.1.1. *Adèles.* On note $\mathscr{P}$ l'ensemble des nombres premiers et $\widehat{\mathbf{Z}}$ le complété profini de $\mathbf{Z}$. On a donc $\widehat{\mathbf{Z}} = \prod_{p\in\mathscr{P}} \mathbf{Z}_p$, et $\mathbf{Q}\otimes\widehat{\mathbf{Z}}$ est l'anneau des adèles finis de $\mathbf{Q}$; c'est le produit restreint des $\mathbf{Q}_p$, $p\in\mathscr{P}$.

Si x est un objet adélique, on note x_p (resp. $x^{]p[}$) la composante de x en p (resp. en dehors de p). Soit $\widehat{\mathbf{Z}}^{]p[} = \prod_{\ell\neq p}\mathbf{Z}_\ell$. La décomposition $\widehat{\mathbf{Z}} = \mathbf{Z}_p\times\widehat{\mathbf{Z}}^{]p[}$ induit, pour $d\geq 1$, des décompositions

$$\mathbf{M}_d(\mathbf{Q}\otimes\widehat{\mathbf{Z}}) = \mathbf{M}_d(\mathbf{Q}_p)\times\mathbf{M}_d(\mathbf{Q}\otimes\widehat{\mathbf{Z}}^{]p[}) \quad\text{et}\quad \mathbf{GL}_d(\mathbf{Q}\otimes\widehat{\mathbf{Z}}) = \mathbf{GL}_d(\mathbf{Q}_p)\times\mathbf{GL}_d(\mathbf{Q}\otimes\widehat{\mathbf{Z}}^{]p[}).$$

Ceci nous permet de définir les sous-ensembles suivants de $\mathbf{Q}\otimes\widehat{\mathbf{Z}}$ et $\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})$:

$$\widehat{\mathbf{Z}}^{(p)} = \mathbf{Z}_p^*\times\widehat{\mathbf{Z}}^{]p[} \quad\text{et}\quad \mathbf{M}_2(\widehat{\mathbf{Z}})^{(p)} = \mathbf{GL}_2(\mathbf{Z}_p)\times\mathbf{M}_2(\widehat{\mathbf{Z}}^{]p[})\,,$$
$$(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^{(p)} = \mathbf{Z}_p^*\times(\mathbf{Q}\otimes\widehat{\mathbf{Z}}^{]p[}) \quad\text{et}\quad \mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^{(p)} = \mathbf{GL}_2(\mathbf{Z}_p)\times\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}}^{]p[})\,.$$

1.1.2. *Cohomologie des groupes (localement) profinis.* Si X est un espace topologique localement profini (comme tous les espaces ci-dessus) et V est un $\mathbf{Z}$-module, on note $\mathrm{LC}_c(\mathrm{X},\mathrm{V})$ le module des fonctions localement constantes à valeurs dans V dont le support est compact dans X. On note $\mathscr{D}_{\mathrm{alg}}(\mathrm{X},\mathrm{V})$ l'ensemble des applications $\mathbf{Z}$-linéaires de $\mathrm{LC}_c(\mathrm{X},\mathbf{Z})$ dans V ; un élément de $\mathscr{D}_{\mathrm{alg}}(\mathrm{X},\mathrm{V})$ est une *distribution algébrique sur* X *à valeurs dans* V. On note $\int_{\mathrm{X}} \phi\, \mu$ la valeur de μ sur ϕ.

Soit G un groupe localement profini (comme $\mathbf{GL}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})$) agissant continûment à droite sur X et V (l'action de $g\in\mathrm{G}$ sur x est notée $x\star g$, et on a $(x\star g_1)\star g_2 = x\star(g_1g_2)$). On munit $\mathrm{LC}_c(\mathrm{X},\mathbf{Z})$ et $\mathscr{D}_{\mathrm{alg}}(\mathrm{X},\mathrm{V})$ d'actions de G à droite $\phi\mapsto\phi\star g$ et $\mu\mapsto\mu\star g$, avec

$$(\phi\star g)(x) = \phi(x\star g^{-1}) \quad \text{et} \quad \int_{\mathrm{X}} \phi\,(\mu\star g) = \Big(\int_{\mathrm{X}} (\phi\star g^{-1})\,\mu\Big)\star g.$$

Si M est un G-module topologique muni d'une action à droite de G, on note $\mathrm{H}^i(\mathrm{G},\mathrm{M})$ le i-ième groupe de cohomologie continue de G à valeurs dans M. Si X est de plus muni d'une action à gauche de G (notée $(g,x)\mapsto g\cdot x$) commutant à l'action à droite de G (i.e. $g_1\cdot(x\star g_2) = (g_1\cdot x)\star g_2$), les modules $\mathrm{H}^i(\mathrm{G},\mathscr{D}_{\mathrm{alg}}(\mathrm{X},\mathrm{M}))$ sont naturellement des G-modules à gauche. Ce qui précède s'applique en particulier à $\mathrm{X} = \mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})$ et $\mathrm{G} = \mathbf{GL}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})$, les actions à gauche et à droite étant simplement données par la multiplication des matrices.

Si H est un sous-groupe fermé de G, si

$$\phi\in\mathrm{H}^0(\mathrm{H},\mathrm{LC}_c(\mathrm{X},\mathbf{Z})) \quad \text{et} \quad \mu\in\mathrm{H}^i(\mathrm{G},\mathscr{D}_{\mathrm{alg}}(\mathrm{X},\mathrm{V})),$$

le cup-produit nous définit un élément $\int_{\mathrm{X}}\phi\,\mu$ de $\mathrm{H}^i(\mathrm{H},\mathrm{V})$. Par ailleurs, si H est d'indice fini dans G, l'application de corestriction $\mathrm{H}^i(\mathrm{H},\mathrm{V})\to\mathrm{H}^i(\mathrm{G},\mathrm{V})$ envoie $\int_{\mathrm{X}}\phi\,\mu$ sur $\mathrm{cor}(\int_{\mathrm{X}}\phi\,\mu) = \int_{\mathrm{X}}\mathrm{cor}\,\phi\;\mu$, où $\mathrm{cor}\,\phi\in\mathrm{H}^0(\mathrm{G},\mathrm{LC}_c(\mathrm{X},\mathbf{Z}))$ est définie par la formule

$$(\mathrm{cor}\,\phi)(x) = \sum_{g\in\mathrm{H}\backslash\mathrm{G}} \phi(xg).$$

1.2. **Formes modulaires**

1.2.1. *Définition.* Soit $\mathscr{H} = \{x+iy,\ y>0\}$ le demi-plan de Poincaré. Si A est un sous-anneau de $\mathbf{R}$, on note $\mathbf{GL}_2(\mathrm{A})_+$, le sous-groupe de $\mathbf{GL}_2(\mathrm{A})$ des éléments de déterminant >0. Si $k\in\mathbf{N}$, on définit une action à droite $f\to f_{|_k}\gamma$ de $\mathbf{GL}_2(\mathbf{R})_+$ sur les fonctions de classe C^∞ de $\mathscr{H}$ dans $\mathbf{C}$, par la formule

$$(f_{|_k}\gamma)(\tau) = \frac{(\det\gamma)^{k-1}}{(c\tau+d)^k}\cdot f\Big(\frac{a\tau+b}{c\tau+d}\Big), \quad \text{si } \gamma = \big(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\big).$$

Si Γ est un sous-groupe d'indice fini de $\mathbf{SL}_2(\mathbf{Z})$, on note $\mathscr{M}_k(\Gamma,\mathbf{C})$, le $\mathbf{C}$-espace vectoriel des formes modulaires de poids k pour Γ, c'est-à-dire l'ensemble des $f:\mathscr{H}\to\mathbf{C}$, holomorphes sur $\mathbf{C}$, à croissance lente à l'infini, vérifiant $f_{|_k}\gamma = f$ quel que soit $\gamma\in\Gamma$. Si $f\in\mathscr{M}_k(\Gamma,\mathbf{C})$, alors f est périodique de période N pour un certain entier $\mathrm{N} \geq 1$, et f est somme de sa série de Fourier

$$f(\tau) = \sum_{n=0}^{+\infty} a_{n/\mathrm{N}} e^{2i\pi n\tau/\mathrm{N}} = \sum_{n=0}^{+\infty} a_{n/\mathrm{N}} q^{n/\mathrm{N}}, \quad \text{avec } q = e^{2i\pi\tau}.$$

La série $\sum_{n\in\mathbf{Q}_+} a_n q^n$ s'appelle le *q-développement* de f. Si A est un sous-anneau de $\mathbf{C}$, on note $\mathscr{M}_k(\Gamma, \mathrm{A})$ le sous-A-module de $\mathscr{M}_k(\Gamma, \mathbf{C})$ des formes dont le q-développement est à coefficients dans A et $\mathscr{M}(\Gamma, \mathrm{A})$ la A-algèbre des formes modulaires pour Γ à coefficients dans A, somme directe des $\mathscr{M}_k(\Gamma, \mathrm{A})$, pour $k \geq 0$. Finalement, on note $\mathscr{M}_k(\mathrm{A})$ (resp. $\mathscr{M}(\mathrm{A})$) la réunion des $\mathscr{M}_k(\Gamma, \mathrm{A})$ (resp. $\mathscr{M}(\Gamma, \mathrm{A})$), où Γ décrit l'ensemble des sous-groupes d'indice fini de $\mathbf{SL}_2(\mathbf{Z})$. L'algèbre $\mathscr{M}(\mathbf{C})$ est munie d'une action de $\mathbf{GL}_2(\mathbf{Q})_+$ notée $f \to f \star \gamma$, avec $f \star \gamma = (\det \gamma)^{1-k} f_{|_k}\gamma$, si $f \in \mathscr{M}_k(\mathbf{C})$ et $\gamma \in \mathbf{GL}_2(\mathbf{Q})_+$.

1.2.2. *Sous-groupes de congruence.* Si N est un entier ≥ 1, soit

$$\Gamma_\mathrm{N} = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbf{Z}),\ a-1, b, c, d-1 \equiv 0\ [\mathrm{N}]\right\}.$$

C'est un sous-groupe d'indice fini de $\mathbf{SL}_2(\mathbf{Z})$ et on dit qu'un sous-groupe de $\mathbf{SL}_2(\mathbf{Z})$ est *de congruence* s'il contient Γ_N, pour un certain $\mathrm{N} \geq 1$. Si A est un sous-anneau de $\mathbf{C}$, on note $\mathscr{M}_k^{\mathrm{cong}}(\mathrm{A})$ (resp. $\mathscr{M}^{\mathrm{cong}}(\mathrm{A})$) la réunion des $\mathscr{M}_k(\Gamma, \mathrm{A})$ (resp. $\mathscr{M}(\Gamma, \mathrm{A})$), où Γ décrit l'ensemble des sous-groupes de congruence de $\mathbf{SL}_2(\mathbf{Z})$.

1.2.3. *Les groupes* Π_K *et* Π'_K. Si K est un sous-corps de $\mathbf{C}$, on note Π_K le groupe des automorphismes de $\mathscr{M}(\overline{\mathrm{K}})$ au-dessus de $\mathscr{M}(\mathbf{SL}_2(\mathbf{Z}), \mathrm{K})$; c'est un groupe profini. Si K est algébriquement clos, alors Π_K est le complété profini de $\mathbf{SL}_2(\mathbf{Z})$ (qui est beaucoup plus gros que $\mathbf{SL}_2(\widehat{\mathbf{Z}})$). Dans le cas général, on dispose de la suite exacte

$$1 \to \Pi_{\overline{\mathrm{K}}} \to \Pi_\mathrm{K} \to \mathscr{G}_\mathrm{K} \to 1,$$

qui est scindée, $\mathscr{G}_\mathrm{K}$ agissant sur les coefficients du q-développement des formes modulaires. Par ailleurs, l'algèbre $\mathscr{M}(\overline{\mathrm{K}})$ est stable sous l'action de $\mathbf{GL}_2(\mathbf{Q})_+$ définie ci-dessus, et on note Π'_K le sous-groupe des automorphismes de $\mathscr{M}(\overline{\mathrm{K}})$ engendré par Π_K et $\mathbf{GL}_2(\mathbf{Q})_+$. Plus généralement, si $\mathrm{S} \subset \mathscr{P}$ est fini, on note $\Pi_\mathrm{K}^{(\mathrm{S})}$ le sous-groupe de Π'_K engendré par Π_K et $\mathbf{GL}_2(\mathbf{Z}^{(\mathrm{S})})$, où $\mathbf{Z}^{(\mathrm{S})}$ est le sous-anneau de $\mathbf{Q}$ obtenu en inversant tous les nombres premiers qui n'appartiennent pas à S.

Soit $\mathbf{Q}^{\mathrm{cycl}}$ l'extension cyclotomique de $\mathbf{Q}$ réunion des $\mathbf{Q}(\zeta_\mathrm{N})$, $\mathrm{N} \geq 1$. La sous-algèbre $\mathscr{M}^{\mathrm{cong}}(\mathbf{Q}^{\mathrm{cycl}})$ est stable par $\Pi_\mathbf{Q}$ et $\Pi'_\mathbf{Q}$ qui agissent à travers $\mathbf{GL}_2(\widehat{\mathbf{Z}})$ et $\mathbf{GL}_2(\mathbf{Q} \otimes \widehat{\mathbf{Z}})$ respectivement. On a le diagramme commutatif de groupes suivant :

$$\begin{tikzcd}
1 \arrow[r] & \Pi_{\overline{\mathrm{K}}} \arrow[r] \arrow[d] & \Pi_\mathrm{K} \arrow[r] \arrow[d] & \mathscr{G}_\mathrm{K} \arrow[r] \arrow[d, "\chi_{\mathrm{cycl}}"] & 1 \\
1 \arrow[r] & \mathbf{SL}_2(\widehat{\mathbf{Z}}) \arrow[r] & \mathbf{GL}_2(\widehat{\mathbf{Z}}) \arrow[r, "\det"] & \widehat{\mathbf{Z}}^* \arrow[r] & 1.
\end{tikzcd}$$

La section de $\mathscr{G}_{\mathbf{Q}}$ dans $\Pi_{\mathbf{Q}}$ décrite ci-dessus induit une section de l'application déterminant $\mathbf{GL}_2(\widehat{\mathbf{Z}}) \to \widehat{\mathbf{Z}}^*$; c'est celle qui envoie u sur la matrice $\left(\begin{smallmatrix} 1 & 0 \\ 0 & u \end{smallmatrix}\right)$.

1.3. Séries d'Eisenstein-Kronecker

1.3.1. *Définition.* Si $(\tau, z) \in \mathscr{H} \times \mathbf{C}$, on pose $q = e^{2i\pi\tau}$, $q_z = e^{2i\pi z}$ et on note ∂_z l'opérateur $\frac{1}{2i\pi}\frac{\partial}{\partial z} = q_z \frac{\partial}{\partial q_z}$. On pose aussi $\mathbf{e}(a) = e^{2i\pi a}$. Si $k \in \mathbf{N}$, $\tau \in \mathscr{H}$, $z, u \in \mathbf{C}$, la série d'Eisenstein-Kronecker (cf. [194] par exemple),

$$\mathrm{H}_k(s, \tau, z, u) = \frac{\Gamma(s)}{(-2i\pi)^k}\Big(\frac{\tau - \overline{\tau}}{2i\pi}\Big)^{s-k} \sum_{\omega \in \mathbf{Z} + \mathbf{Z}\tau} \frac{\overline{\omega + z}^k}{|\omega + z|^{2s}} \mathbf{e}\Big(\frac{\omega \overline{u} - u\overline{\omega}}{\tau - \overline{\tau}}\Big),$$

qui converge[55] si $\mathrm{Re}(s) > 1 + \frac{k}{2}$, possède un prolongement méromorphe à tout le plan complexe, holomorphe en dehors de pôles simples en $s = 1$ (si $k = 0$ et $u \in \mathbf{Z} + \mathbf{Z}\tau$) et $s = 0$ (si $k = 0$ et $z \in \mathbf{Z} + \mathbf{Z}\tau$) et vérifie l'équation fonctionnelle

$$\mathrm{H}_k(s, \tau, z, u) = \mathbf{e}\Big(\frac{\omega \overline{u} - u\overline{\omega}}{\tau - \overline{\tau}}\Big) \cdot \mathrm{H}_k(k - s, \tau, u, z).$$

On définit les fonctions E_k et F_k par les formules

$$\mathrm{E}_k(\tau, z) = \mathrm{H}_k(k, \tau, z, 0) \quad \text{et} \quad \mathrm{F}_k(\tau, z) = \mathrm{H}_k(k, \tau, 0, z).$$

On a

$$\mathrm{E}_{k+1}(\tau, z) = \partial_z \mathrm{E}_k(\tau, z), \text{ si } k \in \mathbf{N} \quad \text{et} \quad \mathrm{E}_0(\tau, z) = \log|\theta(\tau, z)|, \text{ si } z \notin \mathbf{Z}\tau + \mathbf{Z},$$

où $\theta(\tau, z)$ est donnée par le produit infini

$$\theta(\tau, z) = q^{1/12}(q_z^{1/2} - q_z^{-1/2}) \prod_{n \geq 1} \big((1 - q^n q_z)(1 - q^n q_z^{-1})\big).$$

On note $\Delta = \big(\partial_z \theta(\tau, z)_{|z=0}\big)^{12} = q \prod_{n \geq 1}(1 - q^n)^{24}$ la forme de poids 12 habituelle.

1.3.2. *Les formes modulaires* $\mathrm{E}^{(k)}_{\alpha,\beta}$ *et* $\mathrm{F}^{(k)}_{\alpha,\beta}$. Les fonctions $\mathrm{E}_k(\tau, z)$ et $\mathrm{F}_k(\tau, z)$ sont périodiques en z de période $\mathbf{Z}\tau + \mathbf{Z}$. Si $(\alpha, \beta) \in (\mathbf{Q}/\mathbf{Z})^2$ et si $(a, b) \in \mathbf{Q}^2$ a pour image (α, β) dans $(\mathbf{Q}/\mathbf{Z})^2$, on pose

$$\mathrm{E}^{(k)}_{\alpha,\beta} = \mathrm{E}_k(\tau, a\tau + b) \quad \text{et} \quad \mathrm{F}^{(k)}_{\alpha,\beta} = \mathrm{F}_k(\tau, a\tau + b).$$

On a les relations de distribution suivantes si e est un entier ≥ 1 :

$$\sum_{e\alpha' = \alpha,\, e\beta' = \beta} \mathrm{E}^{(k)}_{\alpha',\beta'} = e^k \mathrm{E}^{(k)}_{\alpha,\beta} \qquad \text{et} \qquad \sum_{e\alpha' = \alpha,\, e\beta' = \beta} \mathrm{F}^{(k)}_{\alpha',\beta'} = e^{2-k} \mathrm{F}^{(k)}_{\alpha,\beta}$$

$$\sum_{e\beta' = \beta} \mathrm{E}^{(k)}_{\alpha,\beta'}\Big(\frac{\tau}{e}\Big) = e^k \mathrm{E}^{(k)}_{\alpha,\beta} \qquad \text{et} \qquad \sum_{e\beta' = \beta} \mathrm{F}^{(k)}_{\alpha,\beta'}\Big(\frac{\tau}{e}\Big) = e\, \mathrm{F}^{(k)}_{\alpha,\beta}.$$

[55] Si $z \in \mathbf{Z} + \mathbf{Z}\tau$, on supprime le terme correspondant à $\omega = -z$ de la somme.

PROPOSITION 1.1. — (i) $\mathrm{E}_{0,0}^{(2)} = \mathrm{F}_{0,0}^{(2)} = \frac{-1}{24}\mathrm{E}_2^*$, *où*

$$\mathrm{E}_2^* = \frac{6}{i\pi(\tau - \overline{\tau})} + 1 - 24\sum_{n=1}^{+\infty}\sigma_1(n)q^n$$

est la série d'Eisenstein non holomorphe de poids 2 habituelle.

(ii) *Si* $\mathrm{N}\alpha = \mathrm{N}\beta = 0$, *alors*

(a) $\mathrm{E}_{\alpha,\beta}^{(2)} - \mathrm{E}_{0,0}^{(2)} \in \mathscr{M}_2(\Gamma_{\mathrm{N}}, \mathbf{Q}(\zeta_{\mathrm{N}}))$ *et* $\mathrm{E}_{\alpha,\beta}^{(k)} \in \mathscr{M}_k(\Gamma_{\mathrm{N}}, \mathbf{Q}(\zeta_{\mathrm{N}}))$ *si* $k \geq 1$, $k \neq 2$.

(b) $\mathrm{F}_{\alpha,\beta}^{(k)} \in \mathscr{M}_k(\Gamma_{\mathrm{N}}, \mathbf{Q}(\zeta_{\mathrm{N}}))$ *si* $k \geq 1$, $k \neq 2$ *ou si* $k = 2$ *et* $(\alpha, \beta) \neq (0, 0)$.

Par ailleurs, en faisant agir $\Pi_{\mathbf{Q}}$ trivialement sur $\mathrm{E}_{0,0}^{(2)}$, on obtient le résultat suivant.

PROPOSITION 1.2. — *Si* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{GL}_2(\widehat{\mathbf{Z}})$, *si* $k \geq 1$, *et si* $(\alpha, \beta) \in (\mathbf{Q}/\mathbf{Z})^2$, *alors*

$$\mathrm{E}_{\alpha,\beta}^{(k)} \star \gamma = \mathrm{E}_{a\alpha+c\beta, b\alpha+d\beta}^{(k)} \quad \text{et} \quad \mathrm{F}_{\alpha,\beta}^{(k)} \star \gamma = \mathrm{F}_{a\alpha+c\beta, b\alpha+d\beta}^{(k)}.$$

1.3.3. *Quelques q-développements.* Si $\alpha \in \mathbf{Q}/\mathbf{Z}$, posons

$$\zeta(\alpha, s) = \sum_{n \in \mathbf{Q}_+^*,\ n \equiv \alpha \bmod \mathbf{Z}} n^{-s} \quad \text{et} \quad \zeta^*(\alpha, s) = \sum_{n=1}^{+\infty} e^{2i\pi\, n\alpha}\, n^{-s}.$$

PROPOSITION 1.3. — *Si* $k \geq 1$, *et* $\alpha, \beta \in \mathbf{Q}/\mathbf{Z}$, *alors le q-développement* $\sum_{n \in \mathbf{Q}_+} a_n q^n$ *de* $\mathrm{F}_{\alpha,\beta}^{(k)}$ *est donné par*

$$\sum_{n \in \mathbf{Q}_+^*} \frac{a_n}{n^s} = \zeta(\alpha, s-k+1)\zeta^*(\beta, s) + (-1)^k\zeta(-\alpha, s-k+1)\zeta^*(-\beta, s)$$

et $a_0 = \zeta(\alpha, 1-k)$ *[resp.* $a_0 = \frac{1}{2}(\zeta^*(\beta, 0) - \zeta^*(-\beta, 0))$*] si* $k \neq 1$ *ou* $\alpha \neq 0$ *(resp. si* $k = 1$ *et* $\alpha = 0$*).*

REMARQUE 1.4. — Il y a des formules similaires pour le q-développement de $\mathrm{E}_{\alpha,\beta}^{(k)}$, mais nous n'en aurons pas besoin.

1.3.4. *Les distributions* $\mathbf{z}_{\mathrm{Eis}}(k)$ *et* $\mathbf{z}'_{\mathrm{Eis}}(k)$. Les relations de distributions et la proposition 1.2 peuvent se condenser agréablement en l'énoncé suivant[56] :

THÉORÈME 1.5. — *Si* $k \geq 1$, *il existe une distribution algébrique* $\mathbf{z}_{\mathrm{Eis}}(k)$ *(resp.* $\mathbf{z}'_{\mathrm{Eis}}(k)$*) sur* $(\mathbf{Q} \otimes \widehat{\mathbf{Z}})^2$, *à valeurs dans* $\mathscr{M}_k(\overline{\mathbf{Q}})$ *telle que, quels que soient* $r \in \mathbf{Q}^*$ *et* $(a, b) \in \mathbf{Q}^2$, *on ait*

$$\int_{(a+r\widehat{\mathbf{Z}})\times(b+r\widehat{\mathbf{Z}})} \mathbf{z}_{\mathrm{Eis}}(k) = r^{-k}\mathrm{E}_{r^{-1}a,\, r^{-1}b}^{(k)}$$

$$\Big(\text{resp.} \int_{(a+r\widehat{\mathbf{Z}})\times(b+r\widehat{\mathbf{Z}})} \mathbf{z}'_{\mathrm{Eis}}(k) = r^{k-2}\mathrm{F}_{r^{-1}a,\, r^{-1}b}^{(k)}\Big).$$

[56] L'existence des distributions $\mathbf{z}_{\mathrm{Eis}}(k)$ et $\mathbf{z}'_{\mathrm{Eis}}(k)$ est une conséquence de la première relation de distribution ; la loi de transformation sous $\mathbf{GL}_2(\mathbf{Q} \otimes \widehat{\mathbf{Z}})$ se démontre en utilisant la proposition 1.2, la seconde relation de distribution, et le fait que tout élément de $\mathbf{GL}_2(\mathbf{Q} \otimes \widehat{\mathbf{Z}})$ peut s'écrire sous la forme $g_1\left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & e \end{smallmatrix}\right)g_2$, avec $g_1, g_2 \in \mathbf{GL}_2(\widehat{\mathbf{Z}})$, $r \in \mathbf{Q}^*$ et e entier ≥ 1.

De plus, si $\gamma \in \mathbf{GL}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})$, *alors*

$$\mathbf{z}_{\mathrm{Eis}}(k)_{|_k}\gamma = |\det\gamma|^{k-1}\mathbf{z}_{\mathrm{Eis}}(k) \quad \text{et} \quad \mathbf{z}'_{\mathrm{Eis}}(k)_{|_k}\gamma = \mathbf{z}'_{\mathrm{Eis}}(k).$$

1.3.5. *La distribution* $\mathbf{z}_{\mathrm{Eis}}(k,j)$. On identifie $(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^2\times(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^2$ à $\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})$ en envoyant $((a,b),(c,d))$ sur la matrice $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$. En utilisant le fait que le produit de deux formes modulaires de poids i et j est une forme modulaire de poids $i+j$, cela nous fournit une application naturelle

$$\mathscr{D}_{\mathrm{alg}}((\mathbf{Q}\otimes\widehat{\mathbf{Z}})^2,\mathscr{M}_i(\overline{\mathbf{Q}}))\otimes\mathscr{D}_{\mathrm{alg}}((\mathbf{Q}\otimes\widehat{\mathbf{Z}})^2,\mathscr{M}_j(\overline{\mathbf{Q}}))\longrightarrow\mathscr{D}_{\mathrm{alg}}(\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}}),\mathscr{M}_{i+j}(\overline{\mathbf{Q}})).$$

Si $k\geq 2$ et $1\leq j\leq k-1$, soit

$$\mathbf{z}_{\mathrm{Eis}}(k,j)=\frac{(-1)^j}{(j-1)!}\mathbf{z}'_{\mathrm{Eis}}(k-j)\otimes\mathbf{z}_{\mathrm{Eis}}(j)\in\mathscr{D}_{\mathrm{alg}}(\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}}),\mathscr{M}_k(\overline{\mathbf{Q}})).$$

La valeur de cette distribution sur une fonction localement constante à support compact est une combinaison linéaire de produits de séries d'Eisenstein[57]. D'autre part, il résulte du théorème 1.5 que :

PROPOSITION 1.6. — *Si* $\gamma\in\mathbf{GL}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})$, *alors*

$$\mathbf{z}_{\mathrm{Eis}}(k,j)_{|_k}\gamma=|\det\gamma|^{j-1}\mathbf{z}_{\mathrm{Eis}}(k,j).$$

1.4. **Unités de Siegel et éléments de Beilinson**

1.4.1. *Unités de Siegel.* La fonction $\theta(\tau,z)$ n'est pas périodique en z de période $\mathbf{Z}\tau+\mathbf{Z}$ mais, si $c\geq 2$ est un entier premier à 6, alors la fonction $\theta(\tau,z)^{c^2}\theta(\tau,cz)^{-1}$ est périodique. Si $(\alpha,\beta)\in(\mathbf{Q}/\mathbf{Z})^2-(0,0)$, et si $(a,b)\in\mathbf{Q}^2$ a pour image $(\alpha,\beta)\in(\mathbf{Q}/\mathbf{Z})^2$, posons

$$g_{c,\alpha,\beta}=\theta(\tau,a\tau+b)^{c^2}\theta(\tau,ca\tau+cb)^{-1}.$$

PROPOSITION 1.7. — *Soient* $\alpha,\beta\in\frac{1}{\mathrm{N}}\mathbf{Z}/\mathbf{Z}$.

(i) *Si* $c\in\mathbf{N}$ *est premier à* 6 *et si* $(c\alpha,c\beta)\neq(0,0)$, *alors* $g_{c,\alpha,\beta}$ *est une unité de* $\mathscr{M}(\Gamma_{\mathrm{N}},\mathbf{Q}(\zeta_{\mathrm{N}}))[\frac{1}{\Delta}]$.

(ii) *L'élément* $g_{\alpha,\beta}=g_{c,\alpha,\beta}^{1/(c^2-1)}$ *de* $\mathbf{Q}\otimes\big(\mathscr{M}(\overline{\mathbf{Q}})[\frac{1}{\Delta}]\big)^*$ *ne dépend pas du choix de c congru à* 1 *modulo* N. *De plus, quel que soit c premier à* 6, *on a* $g_{c,\alpha,\beta}=g_{\alpha,\beta}^{c^2}g_{c\alpha,c\beta}^{-1}$.

Le théorème suivant se démontre de la même manière que le théorème 1.5

[57] Si M,N sont des entiers ≥ 1, soit $\mathrm{O}_{\mathrm{M},\mathrm{N}}=\big\{\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right),\ a-1,b\in\mathrm{M}\widehat{\mathbf{Z}},\ c,d-1\in\mathrm{N}\widehat{\mathbf{Z}}\big\}$ et soit $\phi_{\mathrm{M},\mathrm{N}}$ la fonction caractéristique de $\mathrm{O}_{\mathrm{M},\mathrm{N}}$. Par construction, on a

$$\int\phi_{\mathrm{M},\mathrm{N}}\,\mathbf{z}_{\mathrm{Eis}}(k,j)=\frac{(-1)^j}{(j-1)!}\mathrm{M}^{k-j-2}\mathrm{N}^{-j}\mathrm{F}^{(k-j)}_{\frac{1}{\mathrm{M}},0}\mathrm{E}^{(j)}_{0,\frac{1}{\mathrm{N}}}.$$

THÉORÈME 1.8. — *Il existe une distribution algébrique* $\mathbf{z}_{\mathrm{Siegel}}$ *sur* $(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^2-(0,0)$*, à valeurs dans* $\mathbf{Q}\otimes(\mathscr{M}(\overline{\mathbf{Q}})[\frac{1}{\Delta}])^*$*, telle que, quels que soient* $r\in\mathbf{Q}^*$ *et* $(a,b)\in\mathbf{Q}^2-r\mathbf{Z}^2$*, on ait*

$$\int_{(a+r\widehat{\mathbf{Z}})\times(b+r\widehat{\mathbf{Z}})}\mathbf{z}_{\mathrm{Siegel}}=g_{r^{-1}a,\,r^{-1}b}.$$

De plus, $\mathbf{z}_{\mathrm{Siegel}}$ *est invariante sous l'action de* $\Pi'_{\mathbf{Q}}$.

1.4.2. *Éléments de Beilinson.* Si A est un anneau, on dispose d'une application « symbole de Steinberg » $x\otimes y\mapsto\{x,y\}$ de $\mathrm{A}^*\otimes\mathrm{A}^*$ dans le groupe de K-théorie $\mathrm{K}_2(\mathrm{A})$. Ceci permet de construire une distribution algébrique $\mathbf{z}_{\mathrm{Bei}}=\{\mathbf{z}_{\mathrm{Siegel}},\mathbf{z}_{\mathrm{Siegel}}\}$ sur[58] $\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})$ à valeurs dans $\mathrm{K}_2(\mathscr{M}(\overline{\mathbf{Q}})[\frac{1}{\Delta}])$. Cette distribution est invariante sous l'action à droite de $\Pi'_{\mathbf{Q}}$.

1.5. La théorie p-adique

1.5.1. *Théorie de Kummer et classe de Chern p-adique.* D'après le th. 1.8, la distribution $\mathbf{z}_{\mathrm{Siegel}}$ est invariante par $\Pi'_{\mathbf{Q}}$ et on note

$$\mathbf{z}^{(p)}_{\mathrm{Siegel}}\in\mathrm{H}^1\big(\Pi'_{\mathbf{Q}},\mathscr{D}_{\mathrm{alg}}((\mathbf{Q}\otimes\widehat{\mathbf{Z}})^2-(0,0),\mathbf{Q}_p(1))\big)$$

son image par l'application de Kummer[59]. On note

$$\mathbf{z}_{\mathrm{Kato}}\in\mathrm{H}^2\big(\Pi^{(p)}_{\mathbf{Q}},\mathscr{D}_{\mathrm{alg}}\big(\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^{(p)},\mathbf{Q}_p(2)\big)\big)$$

la restriction de $\mathbf{z}^{(p)}_{\mathrm{Siegel}}\otimes\mathbf{z}^{(p)}_{\mathrm{Siegel}}$. C'est aussi, au signe près, l'image de $\mathbf{z}_{\mathrm{Bei}}$ par l'application classe de Chern, mais nous n'utiliserons pas ce fait.

Pour aller plus loin, il faut se débarrasser des dénominateurs dans la distribution $\mathbf{z}_{\mathrm{Kato}}$. Si $x\in\mathbf{Z}_p^*$, on note $\langle x\rangle$ son image dans $\widehat{\mathbf{Z}}^*$ et si $x,y\in\mathbf{Z}_p^*$, on note $\langle x,y\rangle$ l'image de $\left(\begin{smallmatrix}x&0\\0&y\end{smallmatrix}\right)$ dans $\mathbf{GL}_2(\widehat{\mathbf{Z}})$. Si $c\in\mathbf{Z}_p^*$, on déduit du (i) de la proposition 1.7 l'appartenance de $(c^2-\langle c^{-1}\rangle)\cdot\mathbf{z}^{(p)}_{\mathrm{Siegel}}$ à $\mathrm{H}^1\big(\Pi'_{\mathbf{Q}},\mathscr{D}_{\mathrm{alg}}\big((\mathbf{Q}\otimes\widehat{\mathbf{Z}})^2-(0,0),\mathbf{Z}_p(1)\big)\big)$ et donc

$$\mathbf{z}_{\mathrm{Kato},c,d}=(c^2-\langle c^{-1},1\rangle)\cdot(d^2-\langle 1,d^{-1}\rangle)\cdot\mathbf{z}_{\mathrm{Kato}}\in\mathrm{H}^2\big(\Pi^{(p)}_{\mathbf{Q}},\mathscr{D}_{\mathrm{alg}}\big(\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^{(p)},\mathbf{Z}_p(2)\big)\big).$$

[58] Elle n'est définie que sur l'ouvert $\mathbf{M}'_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})$ des matrices $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ avec $(a,b)\neq(0,0)$ et $(c,d)\neq(0,0)$. Si M, N sont des entiers ≥ 1, et si $\Gamma_{\mathrm{M,N}}=\mathbf{SL}_2(\mathbf{Z})\cap\mathrm{O}_{\mathrm{M,N}}$, alors

$$\int\phi_{\mathrm{M,N}}\,\mathbf{z}_{\mathrm{Bei}}=\{g_{\frac{1}{\mathrm{M}},0},g_{0,\frac{1}{\mathrm{N}}}\}\in\mathbf{Q}\otimes\mathrm{K}_2\Big(\mathscr{M}(\Gamma_{\mathrm{M,N}},\mathbf{Q}(\zeta_{(\mathrm{M,N})}))[\frac{1}{\Delta}]\Big)$$

est l'élément construit par Beilinson.

[59] Soit $\mathrm{Z}^0=\{(x_n)_{n\in\mathbf{N}},\ x_n\in\big(\mathscr{M}(\overline{\mathbf{Q}})[\frac{1}{\Delta}]\big)^*,\ x_{n+1}^p=x_n \text{ si } n\in\mathbf{N}\}$. Soit $\mathrm{Z}=\mathbf{Q}\otimes\mathrm{Z}^0$. Alors Z est muni d'une action de $\Pi'_{\mathbf{Q}}$ et la suite $0\to\mathbf{Q}_p(1)\to\mathrm{Z}\to\big(\mathscr{M}(\overline{\mathbf{Q}})[\frac{1}{\Delta}]\big)^*\otimes\mathbf{Q}\to 0$ est une suite exacte de $\Pi'_{\mathbf{Q}}$-modules. Posons $\mathrm{X}=(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^2-(0,0)$ et soit $(\phi_i)_{i\in\mathrm{I}}$ une base de $\mathrm{LC}_c(\mathrm{X},\mathbf{Z})$ sur $\mathbf{Z}$. On peut fabriquer une distribution algébrique μ sur X, à valeurs dans Z, en prenant pour $\int_{\mathrm{X}}\phi_i\,\mu$ n'importe quel relèvement dans Z de $\int_{\mathrm{X}}\phi_i\,\mathbf{z}_{\mathrm{Siegel}}$ et alors $\mathbf{z}^{(p)}_{\mathrm{Siegel}}$ est l'image du cocycle $\sigma\mapsto\mu\star\sigma-\mu$.

1.5.2. *Torsion à la Soulé.* L'intérêt d'avoir supprimé les dénominateurs est de pouvoir intégrer des fonctions continues à support compact et pas seulement des fonctions localement constantes (en d'autres termes, $\mathscr{D}_{\mathrm{alg}}(\mathbf{M}_2'(\mathbf{Q}\otimes\widehat{\mathbf{Z}}),\mathbf{Z}_p(2))$ est l'espace des mesures $\mathscr{D}_0(\mathbf{M}_2'(\mathbf{Q}\otimes\widehat{\mathbf{Z}}),\mathbf{Z}_p(2))$ sur $\mathbf{M}_2'(\mathbf{Q}\otimes\widehat{\mathbf{Z}})$, à valeurs dans $\mathbf{Z}_p(2)$).

On note $t=(\zeta_{p^n})_{n\in\mathbf{N}}$ le générateur canonique de $\mathbf{Z}_p(1)$ et on fait agir $\gamma\in\mathbf{GL}_2(\mathbf{Z}_p)$ sur $\mathbf{Z}_p(1)$ par multiplication par $\det\gamma$. On note $\mathrm{V}_p=\mathbf{Q}_pe_1\oplus\mathbf{Q}_pe_2$ la représentation de dimension 2 de $\mathbf{GL}_2(\mathbf{Z}_p)$ donnée par $e_1\star\gamma=ae_1+be_2$ et $e_2\star\gamma=ce_1+de_2$ si $\gamma=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathbf{GL}_2(\mathbf{Z}_p)$. Si $k\geq 2$ et $j\in\mathbf{Z}$, soit $\mathrm{V}_{k,j}=\mathrm{Sym}^{k-2}\mathrm{V}_p\otimes\mathbf{Q}_p(2-j)$. Multipliant la mesure $\mathbf{z}_{\mathrm{Kato},c,d}$ par la fonction $x\mapsto(e_1^{k-2}t^{-j})\star x_p$ qui est continue sur $\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^{(p)}$, on définit, pour $j\in\mathbf{Z}$,

$$\mathbf{z}_{\mathrm{Kato},c,d}(k,j)=\big((e_1^{k-2}t^{-j})\star x_p\big)\,\mathbf{z}_{\mathrm{Kato},c,d}\in\mathrm{H}^2\big(\Pi_{\mathbf{Q}}^{(p)},\mathscr{D}_0\big(\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^{(p)},\mathrm{V}_{k,j}\big)\big),$$

$\Pi_{\mathbf{Q}}^{(p)}$ agissant sur $\mathrm{V}_{k,j}$ à travers son quotient $\mathbf{GL}_2(\mathbf{Z}_p)$.

1.6. **Du système d'Euler de Kato aux séries d'Eisenstein**

Soit $\mathscr{K}$ le corps des fractions du séparé complété de $\mathbf{Z}_p[[q]][q^{-1}]$ pour la topologie p-adique. C'est un corps local de dimension 2 de corps résiduel $\mathbf{F}_p((q))$. On se fixe une clôture algébrique $\overline{\mathscr{K}}$ de $\mathscr{K}$, un plongement de $\overline{\mathbf{Q}}_p$ dans $\overline{\mathscr{K}}$ et un morphisme $r\mapsto q^r$ de $\mathbf{Q}$ dans $\overline{\mathscr{K}}^*$ vérifiant $q^1=q$.

Si M est un entier ≥ 1, on note q_{M} la racine M-ième $q^{1/\mathrm{M}}$ de q. Soit $\mathscr{K}_{\mathrm{M}}=\mathscr{K}[q_{\mathrm{M}},\zeta_{\mathrm{M}}]$; c'est une extension galoisienne de $\mathscr{K}$ de groupe de Galois $\mathrm{P}_{\mathrm{M}}=\{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{G}_{\mathrm{M}}=\mathbf{GL}_2(\mathbf{Z}/\mathrm{M}\mathbf{Z}),\ a=1,\ c=0\}$. On note $\mathscr{K}_\infty$ la réunion des $\mathscr{K}_{\mathrm{M}}$, $\mathrm{M}\geq 1$.

Dans le chapitre suivant, nous allons définir une application exponentielle duale

$$\exp^*:\mathrm{H}^2(\mathscr{G}_{\mathscr{K}},\mathbf{Z}_p[\mathrm{P}_{\mathrm{M}}]\otimes\mathrm{V}_{k,j})=\mathrm{H}^2(\mathscr{G}_{\mathscr{K}_{\mathrm{M}}},\mathrm{V}_{k,j})\longrightarrow\mathscr{K}_{\mathrm{M}}=\mathrm{H}^0(\mathscr{G}_{\mathscr{K}},\mathscr{K}_\infty\otimes\mathbf{Z}_p[\mathrm{P}_{\mathrm{M}}]).$$

Plus généralement, si W est une représentation de $\mathscr{G}_{\mathscr{K}}$ sur laquelle $\mathscr{G}_{\mathscr{K}}$ agit à travers un quotient fini de $\mathrm{Gal}(\mathscr{K}_\infty/\mathscr{K})$, on définit une application exponentielle duale

$$\exp^*:\mathrm{H}^2(\mathscr{G}_{\mathscr{K}},\mathrm{W}\otimes\mathrm{V}_{k,j})\longrightarrow\mathrm{H}^0(\mathscr{G}_{\mathscr{K}},\mathscr{K}_\infty\otimes\mathrm{W}).$$

Ces applications se recollent pour donner naissance à une application

$$\exp^*:\mathrm{H}^2\big(\mathscr{G}_{\mathscr{K}},\mathscr{D}_{\mathrm{alg}}\big(\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^{(p)},\mathrm{V}_{k,j}\big)\big)\longrightarrow\mathrm{H}^0\big(\mathscr{G}_{\mathscr{K}},\mathscr{D}_{\mathrm{alg}}\big(\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^{(p)},\mathscr{K}_\infty\big)\big).$$

L'application qui à une forme modulaire associe son q-développement nous fournit une injection de $\mathscr{M}(\overline{\mathbf{Q}})$ dans $\mathscr{K}_\infty$ et un morphisme de $\mathscr{G}_{\mathscr{K}}$ dans $\Pi_{\mathbf{Q}}$. Ce morphisme induit un morphisme « de localisation » $\mathrm{H}^i(\Pi_{\mathbf{Q}},\mathrm{W})\to\mathrm{H}^i(\mathscr{G}_{\mathscr{K}},\mathrm{W})$ pour tout $\Pi_{\mathbf{Q}}$-module W et tout $i\in\mathbf{N}$. On note $\mathbf{z}_{\mathrm{Eis}}^{(p)}(k,j)$ l'élément de

$$\mathrm{H}^0\big(\mathscr{G}_{\mathscr{K}},\mathscr{D}_{\mathrm{alg}}\big(\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^{(p)},\mathscr{K}_\infty\big)\big)$$

obtenu en localisant la restriction de $\mathbf{z}_{\mathrm{Eis}}(k,j)$ à $\mathbf{M}_2(\mathbf{Q}\otimes\widehat{\mathbf{Z}})^{(p)}$, et en utilisant l'injection de $\mathscr{M}(\overline{\mathbf{Q}})$ dans $\mathscr{K}_\infty$.

Le résultat suivant permet de faire le lien entre le système d'Euler de Kato et les fonctions L ; c'est la clef de voûte de tout l'édifice. Sa démonstration est un long calcul délicat dans les anneaux de Fontaine auquel le chapitre suivant est consacré.

THÉORÈME 1.9. — *Si* $k \geq 2$, *et* $1 \leq j \leq k-1$, *et si* $c, d \in \mathbf{Z}_p^*$, *alors*

$$\exp^*(\mathbf{z}_{\mathrm{Kato},c,d}(k,j)) = (c^2 - \langle c^{-1}, 1\rangle) \cdot (d^2 - \langle 1, d^{-1}\rangle) \cdot \mathbf{z}_{\mathrm{Eis}}^{(p)}(k,j).$$

1.7. Opérateurs de Hecke

1.7.1. *Définition.* Si Γ est un sous-groupe ouvert de $\mathbf{GL}_2(\widehat{\mathbf{Z}})$, on note $\widetilde{\Gamma}$ l'image inverse de Γ dans $\Pi_{\mathbf{Q}}$. Si $g \in \mathbf{GL}_2(\mathbf{Q})$ est tel que $g^{-1}\Gamma g \subset \mathbf{GL}_2(\widehat{\mathbf{Z}})$, alors le sous-groupe $g^{-1}\widetilde{\Gamma} g$ de $\Pi'_{\mathbf{Q}}$ est inclus dans $\Pi_{\mathbf{Q}}$ et est l'image inverse de $g^{-1}\Gamma g$ dans $\Pi_{\mathbf{Q}}$. On en déduit, si V est un $\Pi'_{\mathbf{Q}}$-module, un isomorphisme[60] $c \mapsto c \star g$ de $\mathrm{H}^i(\widetilde{\Gamma}, \mathrm{V})$ sur $\mathrm{H}^i(g^{-1}\widetilde{\Gamma} g, \mathrm{V})$.

Si ℓ est un nombre premier, et M, N sont des entiers ≥ 1, on définit le sous-groupe $\widehat{\Gamma}_{\mathrm{M}(\ell),\mathrm{N}}$ (resp. $\widehat{\Gamma}_{\mathrm{M},\mathrm{N}(\ell)}$) comme l'intersection de $\mathbf{GL}_2(\widehat{\mathbf{Z}})$ avec l'ensemble des matrices $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$ de $\mathrm{M}_2(\widehat{\mathbf{Z}})$ vérifiant $a - 1 \in \mathrm{M}\widehat{\mathbf{Z}}$, $b \in \mathrm{M}\ell\widehat{\mathbf{Z}}$ (resp. $b \in \mathrm{M}\widehat{\mathbf{Z}}$), $c \in \mathrm{N}\widehat{\mathbf{Z}}$ (resp. $c \in \mathrm{N}\ell\widehat{\mathbf{Z}}$), $d - 1 \in \mathrm{N}\widehat{\mathbf{Z}}$. On définit[61] les opérateurs de Hecke $\mathrm{T}(\ell)$ et $\mathrm{T}'(\ell)$ comme les composés :

$$\mathrm{T}(\ell) : \mathrm{H}^i(\widetilde{\Gamma}_{\mathrm{M},\mathrm{N}}, \mathrm{V}) \xrightarrow{\mathrm{res}} \mathrm{H}^i(\widetilde{\Gamma}_{\mathrm{M}(\ell),\mathrm{N}}, \mathrm{V}) \xrightarrow{\star(1,\ell)} \mathrm{H}^i(\widetilde{\Gamma}_{\mathrm{M},\mathrm{N}(\ell)}, \mathrm{V}) \xrightarrow{\mathrm{cor}} \mathrm{H}^i(\widetilde{\Gamma}_{\mathrm{M},\mathrm{N}}, \mathrm{V}) \ ,$$

$$\mathrm{T}'(\ell) : \mathrm{H}^i(\widetilde{\Gamma}_{\mathrm{M},\mathrm{N}}, \mathrm{V}) \xrightarrow{\mathrm{res}} \mathrm{H}^i(\widetilde{\Gamma}_{\mathrm{M},\mathrm{N}(\ell)}, \mathrm{V}) \xrightarrow{\star(\ell,1)} \mathrm{H}^i(\widetilde{\Gamma}_{\mathrm{M}(\ell),\mathrm{N}}, \mathrm{V}) \xrightarrow{\mathrm{cor}} \mathrm{H}^i(\widetilde{\Gamma}_{\mathrm{M},\mathrm{N}}, \mathrm{V}) \ .$$

Si $(\ell, \mathrm{MN}) = 1$, on a $\mathrm{T}'(\ell)(\ell^{-1}, 1)^{]\ell[} = \mathrm{T}(\ell)(1, \ell^{-1})^{]\ell[}$.

1.7.2. *Corestriction et opérateurs de Hecke.* Soit $\mathrm{S} \subset \mathscr{P}$ un ensemble fini, soit V un $\Pi_{\mathbf{Q}}^{(\mathrm{S})}$-module (cf. nº 1.2.3), soit $i \in \mathbf{N}$ et soit $\mu \in \mathrm{H}^i(\Pi_{\mathbf{Q}}^{(\mathrm{S})}, \mathscr{D}_{\mathrm{alg}}(\mathbf{M}_2(\mathbf{Z}^{(\mathrm{S})} \otimes \widehat{\mathbf{Z}}), \mathrm{V}))$. Soient A, M, N des entiers ≥ 1, et soit ϕ une fonction sur $\mathbf{M}_2(\widehat{\mathbf{Z}})$, constante modulo A, invariante par $\widetilde{\Gamma}_{\mathrm{M},\mathrm{N}}$. Si ℓ est un nombre premier ne divisant pas AMN, soit ϕ_ℓ la fonction définie par

$$\phi_\ell(x) = \phi(x) \cdot \mathbf{1}_{1+\ell\mathbf{M}_2(\mathbf{Z}_\ell)}(x_\ell);$$

cette fonction est invariante par $\widetilde{\Gamma}_{\mathrm{M}\ell,\mathrm{N}\ell}$.

PROPOSITION 1.10. — *Si* $\ell \notin \mathrm{S}$, *alors*

(i) $\int \phi\, \mu \in \mathrm{H}^i(\widetilde{\Gamma}_{\mathrm{M},\mathrm{N}}, \mathrm{V})$ *et* $\int \phi_\ell\, \mu \in \mathrm{H}^i(\widetilde{\Gamma}_{\mathrm{M}\ell,\mathrm{N}\ell}, \mathrm{V})$ *;*

(ii) $\mathrm{cor}(\int \phi_\ell\, \mu) = (\int \phi\, \mu) \star \big(1 - \mathrm{T}'(\ell) \star (\ell^{-1}, 1)^{]\ell[} + \ell(\ell,\ell) \star (\ell^{-1}, \ell^{-1})^{]\ell[}\big)$.

Démonstration. — Le (i) est immédiat. Pour démontrer le (ii), on part des formules

$$\mathrm{cor}\Big(\int \phi_\ell\, \mu\Big) = \int \mathrm{cor}(\phi_\ell)\, \mu \quad \text{et} \quad (\mathrm{cor}(\phi_\ell))(x) = \phi(x) \cdot \mathbf{1}_{\mathbf{GL}_2(\mathbf{Z}_\ell)}.$$

[60] Le cocycle $(\sigma_1, \ldots, \sigma_i) \mapsto c_{\sigma_1,\ldots,\sigma_i}$ est envoyé sur $(\sigma_1, \ldots, \sigma_i) \mapsto (c_{g\sigma_1 g^{-1},\ldots,g\sigma_i g^{-1}}) \star g$.

[61] Cette définition est la traduction, en termes de cohomologie des groupes, de la définition usuelle via les correspondances sur les courbes modulaires.

On est donc ramené à relier les fonctions caractéristiques de $\mathbf{GL}_2(\mathbf{Z}_\ell)$ et $\mathbf{M}_2(\mathbf{Z}_\ell)$. Plus généralement[62], soient $0 \leq r \leq s$ des entiers, et soient $\mathrm{O}_{r,s}$ et $\mathrm{G}_{r,s}$ les sous-ensembles de $\mathbf{M}_2(\mathbf{Z}_\ell)$ définis par

$$\mathrm{O}_{r,s} = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right),\ a-1 \equiv b \equiv 0\ [\ell^r],\ c \equiv d-1 \equiv 0\ [\ell^s] \right\} \quad \text{et} \quad \mathrm{G}_{r,s} = \mathrm{GL}_2(\mathbf{Z}_\ell) \cap \mathrm{O}_{r,s}.$$

Soient $\alpha_{s,i} = \left(\begin{smallmatrix} 1 & 0 \\ i\ell^s & 1 \end{smallmatrix}\right)$ si $0 \leq i \leq \ell - 1$ et $\alpha_{0,\ell} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Les fonctions caractéristiques de $\mathrm{O}_{r,s}$ et $\mathrm{G}_{r,s}$ sont reliées de la manière suivante :

$$\mathbf{1}_{\mathrm{G}_{r,s}} = \begin{cases} \mathbf{1}_{\mathrm{O}_{r,s}} & \text{si } r \geq 1 \text{ et } s \geq 1, \\ \mathbf{1}_{\mathrm{O}_{r,s}} \star \left(1 - \sum_{i=0}^{\ell-1} \left((\ell,1)_\ell \alpha_{s,i}\right)\right) & \text{si } r = 0 \text{ et } s \geq 1, \\ \mathbf{1}_{\mathrm{O}_{r,s}} \star \left(1 - \sum_{i=0}^{\ell} \left((\ell,1)_\ell \alpha_{0,i}\right) + \ell(\ell,\ell)_\ell\right) & \text{si } r = s = 0. \end{cases}$$

La proposition se déduit alors de la troisième de ces relations, du fait que, si $(\ell, \mathrm{M}) = 1$, les $\alpha_{s,i}$ forment un système de représentants de $\widetilde{\Gamma}_{\mathrm{M}(\ell),\mathrm{N}} \backslash \widetilde{\Gamma}_{\mathrm{M},\mathrm{N}}$, et de la formule $\int (\phi \star g)\, \mu = (\int \phi \mu) \star g$ qui se démontre à partir du cas $i = 0$ par « décalage » de dimension.

2. LA LOI DE RÉCIPROCITÉ EXPLICITE DE KATO

Ce chapitre est consacré à la définition de l'application $\exp^*$ et au calcul de l'image du système d'Euler de Kato par cette application. Les techniques sont celles introduites par Tate [185] pour calculer la cohomologie galoisienne de $\mathbf{C}_p$ et étendues par Hyodo [92] dans le cas de corps locaux de corps résiduel non parfait.

2.1. L'anneau $\mathbb{B}_{\mathrm{dR}}^+$

2.1.1. *Définition.* Soit L un corps de caractéristique 0 muni d'une extension v_p de la valuation p-adique normalisée par $v_p(p) = 1$. On note $\mathbb{C}(\mathrm{L})$ le complété de L pour la valuation v_p.

Soit

$$\mathbb{R}(\mathrm{L}) = \{(x_n)_{n \in \mathbf{N}},\ x_n \in \mathscr{O}_\mathrm{L}/p\mathscr{O}_\mathrm{L} \text{ et } x_{n+1}^p = x_n \text{ si } n \in \mathbf{N}\}.$$

Si $x = (x_n)_{n \in \mathbf{N}} \in \mathbb{R}(\mathrm{L})$ et si $\hat{x}_n \in \mathscr{O}_\mathrm{L}$ a pour image x_n modulo p, alors la suite $\hat{x}_{n+k}^{p^k}$ converge, quand k tend vers $+\infty$, vers un élément $x^{(n)}$ de $\mathscr{O}_{\mathbb{C}(\mathrm{L})}$ qui ne dépend que de x. Ceci permet de mettre $\mathbb{R}(\mathrm{L})$ en bijection avec l'ensemble des suites $x = (x^{(n)})_{n \in \mathbf{N}}$, avec $x^{(n)} \in \mathscr{O}_{\mathbb{C}(\mathrm{L})}$ et $(x^{(n+1)})^p = x^{(n)}$ si $n \in \mathbf{N}$.

L'anneau $\mathbb{R}(\mathrm{L})$ est un anneau parfait de caractéristique p et on note $\mathbb{A}_{\mathrm{inf}}(\mathrm{L}) = \mathrm{W}(\mathbb{R}(\mathrm{L}))$ l'anneau des vecteurs de Witt à coefficients dans $\mathbb{R}(\mathrm{L})$. Si $x \in \mathbb{R}(\mathrm{L})$, on note $[x] \in \mathbb{A}_{\mathrm{inf}}(\mathrm{L})$ son représentant de Teichmüller, et tout élément de $\mathbb{A}_{\mathrm{inf}}(\mathrm{L})$ peut s'écrire de manière unique sous la forme $\sum_{k=0}^{+\infty} p^k[x_k]$, où $(x_k)_{k \in \mathbf{N}}$ est une suite d'éléments de $\mathbb{R}(\mathrm{L})$. On définit un

[62]Cela peut être utile pour calculer des corestrictions de $\widetilde{\Gamma}_{\mathrm{M}\ell,\mathrm{N}\ell}$ à $\widetilde{\Gamma}_{\mathrm{M},\mathrm{N}}$ dans le cas où ℓ divise N par exemple.

morphisme d'anneaux $\theta : \mathbb{A}_{\inf}(\mathrm{L}) \to \mathscr{O}_{\mathbb{C}(\mathrm{L})}$ par la formule $\theta(\sum_{k=0}^{+\infty} p^k[x_k]) = \sum_{k=0}^{+\infty} p^k x_k^{(0)}$. On note $\mathbb{B}_{\inf}(\mathrm{L})$ l'anneau $\mathbb{A}_{\inf}(\mathrm{L})[\frac{1}{p}]$ et on étend θ en un morphisme de $\mathbb{B}_{\inf}(\mathrm{L})$ dans $\mathbb{C}(\mathrm{L})$. Si $m \geq 1$ est un entier, on note $\mathbb{B}_m(\mathrm{L})$ l'anneau $\mathbb{B}_{\inf}(\mathrm{L})/(\ker\theta)^m$. On fait de $\mathbb{B}_m(\mathrm{L})$ un anneau de Banach en prenant l'image de $\mathbb{A}_{\inf}(\mathrm{L})$ comme anneau d'entiers.

On définit l'anneau $\mathbb{B}_{\mathrm{dR}}^+(\mathrm{L})$ comme la limite projective des $\mathbb{B}_m(\mathrm{L})$ que l'on munit de la topologie de la limite projective, ce qui en fait un anneau de Fréchet. Par construction, θ s'étend en un morphisme continu d'anneaux topologiques de $\mathbb{B}_{\mathrm{dR}}^+(\mathrm{L})$ dans $\mathbb{C}(\mathrm{L})$ et on a $\mathbb{B}_m(\mathrm{L}) = \mathbb{B}_{\mathrm{dR}}^+(\mathrm{L})/(\ker\theta)^m$ quel que soit $m \in \mathbf{N}$.

2.1.2. *L'anneau* $\mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}})$. Le groupe $\mathscr{G}_{\mathscr{K}}$ agit continûment sur les anneaux $\mathbb{C}(\overline{\mathscr{K}})$ et $\mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}})$ et la définition de l'application $\exp^*$ repose sur l'étude de la cohomologie de $\mathscr{G}_{\mathscr{K}}$ à valeurs dans ces anneaux. Si M est un entier, on note $\mathscr{K}_{\mathrm{M}p^\infty}$ la réunion des $\mathscr{K}_{\mathrm{M}p^n}$, $n \in \mathbf{N}$. L'extension $\overline{\mathscr{K}}/\mathscr{K}_{\mathrm{M}p^\infty}$ est presque étale, ce qui se traduit par la nullité de $\mathrm{H}^i(\mathscr{G}_{\mathscr{K}_{\mathrm{M}p^\infty}}, \mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}}) \otimes \mathrm{V})$ quelle que soit la $\mathbf{Q}_p$-représentation V de $\mathscr{G}_{\mathscr{K}_\mathrm{M}}$ et quel que soit $i \geq 1$. On est donc ramené à étudier de près l'extension $\mathscr{K}_{\mathrm{M}p^\infty}/\mathscr{K}_\mathrm{M}$ dont le groupe de Galois $\mathrm{P}_{\mathscr{K}_\mathrm{M}}$ est un groupe de Lie de dimension 2 isomorphe au groupe P_m $[m = v_p(\mathrm{M})]$ des matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de $\mathbf{GL}_2(\mathbf{Z}_p)$ vérifiant $a = 1$, $c = 0$, $b \in p^m\mathbf{Z}_p$, $d \in 1 + p^m\mathbf{Z}_p$. Cette étude repose sur la construction (prop. 2.1) de « traces de Tate normalisées » et des résultats généraux concernant la cohomologie des groupes de Lie p-adiques.

2.1.3. *Traces de Tate normalisées.* Soit $\tilde\zeta$ [resp. $\tilde\zeta_\mathrm{M}$, si M est un entier ≥ 1] le représentant de Teichmüller dans $\mathbb{A}_{\inf}(\overline{\mathscr{K}})$ de $(1, \zeta_p, \dots, \zeta_{p^n}, \dots)$ [resp. $(\zeta_\mathrm{M}, \dots, \zeta_{\mathrm{M}p^n}, \dots)$]. Si M|N, on a $\tilde\zeta_\mathrm{N}^{\mathrm{N}/\mathrm{M}} = \tilde\zeta_\mathrm{M}$.

Soit $t = \log\tilde\zeta = -\sum_{n=1}^{+\infty} \frac{(1-\tilde\zeta)^n}{n} \in \mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}})$ le $2i\pi$ p-adique de Fontaine. C'est un générateur du noyau de $\theta : \mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}}) \to \mathbb{C}(\overline{\mathscr{K}})$ sur lequel $\mathscr{G}_{\mathscr{K}}$ agit par multiplication par χ_{cycl}.

Soit $\tilde q$ [resp. $\tilde q_\mathrm{M}$, si M est un entier ≥ 1] le représentant de Teichmüller dans $\mathbb{A}_{\inf}(\overline{\mathscr{K}})$ de $(q, q_p, \dots, q_{p^n}, \dots)$ [resp. $(q_\mathrm{M}, \dots, q_{\mathrm{M}p^n}, \dots)$]. Si M|N, on a $\tilde q_\mathrm{N}^{\mathrm{N}/\mathrm{M}} = \tilde q_\mathrm{M}$. L'application $f(q) \mapsto f(\tilde q)$ permet d'identifier $\mathscr{K}$ à un sous-anneau de $\mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}})$, mais il faut faire attention au fait que $\mathscr{K}$ n'est pas stable par $\mathscr{G}_{\mathscr{K}}$ car $\tilde q \star \sigma = \tilde q \tilde\zeta^{c_q(\sigma)}$ si $\sigma \in \mathscr{G}_{\mathscr{K}}$, où $\sigma \mapsto c_q(\sigma)$ est le cocycle à valeurs dans $\mathbf{Z}_p(1) = \mathbf{Z}_p(\chi_{\mathrm{cycl}})$ associé à q par la théorie de Kummer. Par contre l'anneau $\widetilde{\mathscr{K}} = \mathscr{K}[[t]]$ est stable par $\mathscr{G}_{\mathscr{K}}$.

Si M est un entier ≥ 1, on note $\widetilde{\mathscr{K}_\mathrm{M}}$ l'anneau $\widetilde{\mathscr{K}}[\tilde q_\mathrm{M}, \tilde\zeta_\mathrm{M}]$; on a aussi $\widetilde{\mathscr{K}_\mathrm{M}} = \mathscr{K}_\mathrm{M}[[t]]$. On définit, si $v_p(\mathrm{M}) \geq v_p(2p)$, une application R_M de la sous-$\mathbf{Q}_p$-algèbre $\widetilde{\mathscr{K}_{\mathrm{M}p^\infty}}$ de $\mathbb{B}_{\mathrm{dR}}^+(\mathscr{K}_{\mathrm{M}p^\infty})$ engendrée par les $\tilde\zeta_{\mathrm{M}p^n}$ et les $\tilde q_{\mathrm{M}p^n}$, $n \in \mathbf{N}$, dans $\widetilde{\mathscr{K}_\mathrm{M}}$ en envoyant $\tilde\zeta_{\mathrm{M}p^n}^a \tilde q_{\mathrm{M}p^n}^b$ sur $\tilde\zeta_{\mathrm{M}p^n}^a \tilde q_{\mathrm{M}p^n}^b$ (resp. sur 0) si p^n divise a et b (resp. p^n ne divise pas a ou b).

Proposition 2.1. — *Si* M *est un entier* ≥ 1*, alors*

(i) $\mathrm{H}^0(\mathscr{G}_{\mathscr{K}_{\mathrm{M}p^\infty}}, \mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}})) = \mathbb{B}_{\mathrm{dR}}^+(\mathscr{K}_{\mathrm{M}p^\infty})$.

(ii) $\widetilde{\mathscr{K}_{\mathrm{M}p^\infty}}$ *est dense dans* $\mathbb{B}_{\mathrm{dR}}^+(\mathscr{K}_{\mathrm{M}p^\infty})$.

(iii) *Si* $v_p(\mathrm{M}) \geq v_p(2p)$, *alors* $\mathrm{R_M}$ *s'étend par continuité en une application* $\mathscr{K}$*-linéaire* $\mathrm{R_M} : \mathbb{B}^+_{\mathrm{dR}}(\mathscr{K}_{\mathrm{M}p^\infty}) \to \widetilde{\mathscr{K}_\mathrm{M}}$ *qui commute à l'action de* $\mathscr{G}_\mathscr{K}$.

Proposition 2.2. — *Si* $v_p(\mathrm{M}) \geq v_p(2p)$, *si* V *est une* $\mathbf{Q}_p$*-représentation de* $\mathrm{P}_{\mathscr{K}_\mathrm{M}}$ *possédant un* $\mathbf{Z}_p$*-réseau* T *tel que* $\mathrm{P}_{\mathscr{K}_\mathrm{M}}$ *agisse trivialement sur* $\mathrm{T}/2p\mathrm{T}$, *et si* $i \in \mathbf{N}$, *alors* $\mathrm{R_M}$ *induit un isomorphisme*

$$\mathrm{R_M} : \mathrm{H}^i(\mathrm{P}_{\mathscr{K}_\mathrm{M}}, \mathbb{B}^+_{\mathrm{dR}}(\mathscr{K}_{\mathrm{M}p^\infty}) \otimes \mathrm{V}) \cong \mathrm{H}^i(\mathrm{P}_{\mathscr{K}_\mathrm{M}}, \widetilde{\mathscr{K}_\mathrm{M}} \otimes \mathrm{V}).$$

Le gros intérêt de descendre de $\mathbb{B}^+_{\mathrm{dR}}(\mathscr{K}_{\mathrm{M}p^\infty})$ à $\widetilde{\mathscr{K}_\mathrm{M}}$ est que l'action de $\mathrm{P}_{\mathscr{K}_\mathrm{M}}$ devient analytique, ce qui permet d'utiliser les techniques du § 2.2.

2.2. Cohomologie de P_m

Si $m \geq v_p(2p)$, soit $\mathrm{P}_m = \{\left(\begin{smallmatrix} 1 & b \\ 0 & d \end{smallmatrix}\right),\ b \in p^m\mathbf{Z}_p,\ d \in 1+p^m\mathbf{Z}_p\}$. C'est un groupe analytique p-adique compact et, si $u, v \in p^m\mathbf{Z}_p$, on note (u,v) l'élément $\left(\begin{smallmatrix} 1 & u \\ 0 & e^v \end{smallmatrix}\right)$ de P_m. La loi de groupe s'écrit alors sous la forme

$$(u_1, v_1)(u_2, v_2) = (e^{v_2}u_1 + u_2, v_1 + v_2).$$

Soient U_m et Γ_m les sous-groupes de P_m topologiquement engendrés par $(p^m, 0)$ et $(0, p^m)$ respectivement. Ces deux sous-groupes sont isomorphes à $\mathbf{Z}_p$, U_m est distingué dans P_m et on a $\mathrm{P}_m/\mathrm{U}_m \cong \Gamma_m$. En particulier, U_m et Γ_m n'ayant pas de H^2, la suite spectrale de Hochschild-Serre nous fournit, si V est une représentation[63] de P_m, un isomorphisme[64]

$$\mathrm{H}^2(\mathrm{P}_m, \mathrm{V}) \cong \mathrm{H}^1(\Gamma_m, \mathrm{H}^1(\mathrm{U}_m, \mathrm{V})) \cong \mathrm{V}/\big((p^m, 0) - 1, (0, p^m) - e^{p^m}\big).$$

Soit V une représentation analytique[65] de P_m. Soient $\partial_i : \mathrm{V} \to \mathrm{V}$, $i = 1, 2$ les opérateurs définis par

$$x \star (u, v) = x + u\partial_1 x + v\partial_2 x + \mathrm{O}((u, v)^2).$$

Ces opérateurs se comportent comme des dérivations : si $x_1 \in \mathrm{V}_1$ et $x_2 \in \mathrm{V}_2$ et si $i = 1, 2$, alors $\partial_i(x_1 \otimes x_2) = (\partial_i x_1) \otimes x_2 + x_1 \otimes \partial_i x_2$. Comme $\partial_1 = \log(p^m, 0)$ et $\partial_2 - 1 = \log(e^{-p^m}(0, p^m))$ sont divisibles par $(p^m, 0) - 1$ et $(0, p^m) - e^{p^m}$ respectivement, on dispose d'une application naturelle de $\mathrm{V}/(\partial_1, \partial_2 - 1)$ dans $\mathrm{V}/\big((p^m, 0) - 1, (0, p^m) - e^{p^m}\big)$ qui est un isomorphisme car V est supposée analytique. On en déduit un isomorphisme

$$\mathrm{H}^2(\mathrm{P}_m, \mathrm{V}) \cong \mathrm{V}/(\partial_1, \partial_2 - 1).$$

[63] i.e. un espace vectoriel de dimension finie sur $\mathbf{Q}_p$ ou $\mathscr{K}$ muni d'une action continue de P_m agissant de manière linéaire.

[64] Le groupe $\mathrm{H}^1(\mathrm{U}_m, \mathrm{V})$ est isomorphe, en tant que groupe, à $\mathrm{V}/((p^m, 0) - 1)$ mais, comme $(0, v)(u, 0)(0, v)^{-1} = (e^{-v}u, 0)$, l'action de $(0, v) \in \Gamma_m$ sur $\mathrm{H}^1(\mathrm{U}_m, \mathrm{V})$ est celle sur $\mathrm{V}/((p^m, 0) - 1)$ multipliée par e^{-v}, d'où l'apparition de e^{p^m} dans l'explicitation du groupe $\mathrm{H}^1(\Gamma_m, \mathrm{H}^1(\mathrm{U}_m, \mathrm{V}))$.

[65] i.e. une représentation de P_m telle que les coordonnées de la matrice de (u, v) dans une base de V soient les restrictions à $p^m\mathbf{Z}_p \times p^m\mathbf{Z}_p$ de fonctions analytiques sur $\{v_p(u), v_p(v) > s\}$, avec $s < m$.

PROPOSITION 2.3. — *Si* V *est une représentation analytique de* P_m*, alors*

(i) *tout élément de* $\mathrm{H}^2(\mathrm{P}_m, \mathrm{V})$ *est représentable par un 2-cocycle analytique ;*

(ii) *l'image, dans* $\mathrm{H}^2(\mathrm{P}_m, \mathrm{V}) \cong \mathrm{V}/(\partial_1, \partial_2 - 1)$*, d'un 2-cocycle analytique*

$$((u,v),(x,y)) \mapsto c_{(u,v),(x,y)} = \sum_{i+j+k+\ell \geq 2} c_{i,j,k,\ell} \cdot u^i v^j x^k y^\ell$$

est aussi celle de $\delta^{(2)}(c_{(u,v),(x,y)}) = c_{1,0,0,1} - c_{0,1,1,0}$ *dans* $\mathrm{V}/(\partial_1, \partial_2 - 1)$.

2.3. L'application $\exp^*$ pour la représentation $\mathrm{V}_{k,j}$

La construction[66] de l'application $\exp^*$ repose sur le résultat suivant qui se démontre en constatant que $e_1^i e_2^{k-2-i} t^\ell f(\tilde{q})$ est vecteur propre de $\partial_2 - 1$ pour la valeur propre $(k-3-i+\ell)$ et en calculant son image par ∂_1.

PROPOSITION 2.4. — *Si* $v_p(\mathrm{M}) \geq v_p(2p)$*, et si* $1 \leq j \leq k-1$*, alors l'application* $f \mapsto t e_1^{k-2} f$ *induit un isomorphisme de* $\mathscr{K}_\mathrm{M}$ *sur* $(\mathscr{K}_\mathrm{M} \otimes \mathrm{V}_{k,j})/(\partial_1, \partial_2 - 1)$.

On note $\mathrm{res}_{k,j} : \mathscr{K}_\mathrm{M} \otimes \mathrm{V}_{k,j} \to \mathscr{K}_\mathrm{M}$ l'application obtenue en composant la projection de $\mathscr{K}_\mathrm{M} \otimes \mathrm{V}_{k,j}$ sur $(\mathscr{K}_\mathrm{M} \otimes \mathrm{V}_{k,j})/(\partial_1, \partial_2 - 1)$ avec l'inverse de l'isomorphisme précédent.

Maintenant, soit $\mathrm{M} \geq 1$ avec $v_p(\mathrm{M}) \geq v_p(2p)$, soit $c \in \mathrm{H}^2(\mathscr{G}_{\mathscr{K}_\mathrm{M}}, \mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}}) \otimes \mathrm{V}_{k,j})$ et soit $(\sigma, \tau) \mapsto c_{\sigma,\tau}$ un 2-cocycle continu sur $\mathscr{G}_{\mathscr{K}_\mathrm{M}}$, à valeurs dans $\mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}}) \otimes \mathrm{V}_{k,j}$, représentant c. L'extension $\overline{\mathscr{K}}/\mathscr{K}_{\mathrm{M}p^\infty}$ étant presque étale, l'application d'inflation induit un isomorphisme

$$\mathrm{H}^2(\mathrm{P}_{\mathscr{K}_\mathrm{M}}, \mathbb{B}_{\mathrm{dR}}^+(\mathscr{K}_{\mathrm{M}p^\infty}) \otimes \mathrm{V}_{k,j}) \cong \mathrm{H}^2(\mathscr{G}_{\mathscr{K}_\mathrm{M}}, \mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}}) \otimes \mathrm{V}),$$

et il existe un 2-cocycle continu $(\sigma, \tau) \mapsto c'_{\sigma,\tau}$ sur $\mathrm{P}_{\mathscr{K}_\mathrm{M}}$, à valeurs dans $\mathbb{B}_{\mathrm{dR}}^+(\mathscr{K}_{\mathrm{M}p^\infty})$ dont l'inflation a pour image c dans $\mathrm{H}^2(\mathscr{G}_{\mathscr{K}_\mathrm{M}}, \mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}}) \otimes \mathrm{V}_{k,j})$.

Comme $v_p(\mathrm{M}) \geq v_p(2p)$, on est dans les conditions d'application de la prop. 2.2, et R_M induit un isomorphisme

$$\mathrm{R}_\mathrm{M} : \mathrm{H}^2(\mathrm{P}_{\mathscr{K}_\mathrm{M}}, \mathbb{B}_{\mathrm{dR}}^+(\mathscr{K}_{\mathrm{M}p^\infty}) \otimes \mathrm{V}_{k,j}) \cong \mathrm{H}^2(\mathrm{P}_{\mathscr{K}_\mathrm{M}}, \widetilde{\mathscr{K}_\mathrm{M}} \otimes \mathrm{V}_{k,j}).$$

Il existe donc (cf. [67] prop. 2.3 (i)), un 2-cocycle analytique $(\sigma, \tau) \mapsto c''_{\sigma,\tau}$ sur $\mathrm{P}_{\mathscr{K}_\mathrm{M}}$, à valeurs dans $\widetilde{\mathscr{K}_\mathrm{M}} \otimes \mathrm{V}_{k,j}$, ayant même image que $(\sigma, \tau) \mapsto c'_{\sigma,\tau}$ dans $\mathrm{H}^2(\mathrm{P}_{\mathscr{K}_\mathrm{M}}, \mathbb{B}_{\mathrm{dR}}^+(\mathscr{K}_{\mathrm{M}p^\infty}) \otimes \mathrm{V}_{k,j})$.

L'élément $\mathrm{res}_{k,j}(\delta^{(2)}(c''_{\sigma,\tau}))$ de $\mathscr{K}_\mathrm{M}$ ne dépend d'aucun des choix que l'on a faits ; on le note $\exp^*(c)$, et l'application $\exp^*$ induit un isomorphisme

$$\exp^* : \mathrm{H}^2(\mathscr{G}_{\mathscr{K}_\mathrm{M}}, \mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}}) \otimes \mathrm{V}_{k,j}) \to \mathscr{K}_\mathrm{M}.$$

[66] La construction qui suit est un peu ad hoc, mais elle a le mérite de coller aux calculs du paragraphe suivant. On peut définir une application $\exp^*$ pour toute représentation de de Rham de $\mathscr{G}_\mathrm{L}$, L extension finie de $\mathscr{K}$; la définition de cette application ainsi que celle de représentation de de Rham utilise l'anneau $\mathbb{B}_{\mathrm{dR}}(\overline{\mathscr{K}}/\mathscr{K})$ obtenu en complétant $\mathscr{K} \otimes_{\mathbf{Q}_p} \mathbb{B}_{\mathrm{dR}}(\overline{\mathscr{K}})$. (On a $\mathbb{B}_{\mathrm{dR}}(\overline{\mathscr{K}}/\mathscr{K})^{\mathscr{G}_\mathscr{K}} = \mathscr{K}$, alors que $\mathbb{B}_{\mathrm{dR}}(\overline{\mathscr{K}})^{\mathscr{G}_\mathscr{K}} = \mathbf{Q}_p$.)

[67] $\widetilde{\mathscr{K}_\mathrm{M}} \otimes \mathrm{V}_{k,j}$ n'est pas une représentation analytique de $\mathrm{P}_{\mathscr{K}_\mathrm{M}}$, mais c'est la limite projective des $(\widetilde{\mathscr{K}_\mathrm{M}}/t^n) \otimes \mathrm{V}_{k,j}$ qui sont des représentations analytiques de $\mathrm{P}_{\mathscr{K}_\mathrm{M}}$.

Plus généralement, si W est une représentation de $\mathrm{Gal}(\mathscr{K}_\infty/\mathscr{K})$ d'image finie, on définit un isomorphisme

$$\exp^* : \mathrm{H}^2(\mathscr{G}_{\mathscr{K}}, \mathbb{B}^+_{\mathrm{dR}}(\overline{\mathscr{K}}) \otimes \mathrm{W} \otimes \mathrm{V}_{k,j}) \to \mathrm{H}^0(\mathscr{G}_{\mathscr{K}}, \mathscr{K}_\infty \otimes \mathrm{W})$$

en choisissant un entier $\mathrm{M} \geq 1$, $v_p(\mathrm{M}) \geq v_p(2p)$, tel que $\mathscr{G}_{\mathscr{K}_\mathrm{M}}$ agisse trivialement sur W, et en restreignant l'application $\exp^*$

$$\exp^* : \mathrm{H}^2(\mathscr{G}_{\mathscr{K}_\mathrm{M}}, \mathbb{B}^+_{\mathrm{dR}}(\overline{\mathscr{K}}) \otimes \mathrm{W} \otimes \mathrm{V}_{k,j}) \to \mathscr{K}_\mathrm{M} \otimes \mathrm{W}$$

précédemment définie à la partie fixe par $\mathrm{Gal}(\mathscr{K}_\mathrm{M}/\mathscr{K})$.

2.4. Image du système d'Euler de Kato par l'exponentielle duale

2.4.1. *Préliminaires.* Si M est un entier ≥ 1, et $\mathrm{A} = \left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right)$, avec $\alpha, \beta, \gamma, \delta \in \{1, \dots, \mathrm{M}\}$, on note $\psi_{\mathrm{M,A}}$ la fonction caractéristique de $\mathrm{A} + \mathrm{M}\mathbf{M}_2(\widehat{\mathbf{Z}})$. C'est une fonction invariante sous l'action de $\mathscr{G}_{\mathscr{K}_\mathrm{M}}$ et $\int \psi_{\mathrm{M,A}}\, \mathbf{z}_{\mathrm{Kato}}(k,j)$ est[68] un élément de $\mathrm{H}^2(\mathscr{G}_{\mathscr{K}_\mathrm{M}}, \mathrm{V}_{k,j})$ dont on note $z_{\mathrm{M,A}}$ l'image dans $\mathrm{H}^2(\mathscr{G}_{\mathscr{K}_\mathrm{M}}, \mathbb{B}^+_{\mathrm{dR}}(\overline{\mathscr{K}}) \otimes \mathrm{V}_{k,j})$. Pour démontrer le théorème 1.9, il suffit[69] de démontrer le résultat suivant

Proposition 2.5. — *Pour tout couple* M, A *comme ci-dessus avec* $v_p(\mathrm{M}) \geq v_p(2p)$ *et* $\det \mathrm{A} \in \mathbf{Z}_p^*$, *on a*

$$\exp^*(z_{\mathrm{M,A}}) = \frac{(-1)^j}{(j-1)!} \mathrm{M}^{k-2-2j} \mathrm{F}^{(k-j)}_{\alpha/\mathrm{M},\, \beta/\mathrm{M}} \mathrm{E}^{(j)}_{\gamma/\mathrm{M},\, \delta/\mathrm{M}}.$$

Pour démontrer ceci, nous allons avoir besoin d'écrire un 2-cocycle explicite représentant $z_{\mathrm{M,A}}$ et le suivre à travers les étapes de la construction de l'application $\exp^*$. Il y a deux petits miracles qui permettent de mener le calcul à bien (cf. lemme 2.9 et apparition de $ad - bc$ dans le lemme 2.12).

Comme $z_{\mathrm{M,A}}$ est fabriqué à partir d'unités de Siegel que l'on peut voir comme éléments de $\overline{\mathscr{K}}$ et même de $\mathscr{K}_\infty \subset \overline{\mathscr{K}}$, nous allons choisir des relèvements privilégiés de ces unités dans $\mathbb{B}^+_{\mathrm{dR}}(\overline{\mathscr{K}})$. Si N est un entier ≥ 1, si $a, b \in \mathbf{Z}^2 - \mathrm{N}\mathbf{Z}^2$, soit $[\theta(q, q_\mathrm{N}^a \zeta_\mathrm{N}^b)] \in \mathbb{A}_{\mathrm{inf}}(\overline{\mathscr{K}})$ un représentant de Teichmüller dont l'image dans $\mathbb{C}(\overline{\mathscr{K}})$ est $\theta(q, q_\mathrm{N}^a \zeta_\mathrm{N}^b)$ (on note $\theta(q, q_z)$, ce qui est noté $\theta(\tau, z)$ dans le n° 1.3.1 ; même chose pour les séries d'Eisenstein). Ceci détermine $[\theta(q, q_\mathrm{N}^a \zeta_\mathrm{N}^b)]$ à multiplication près par $\tilde{\zeta}^u$, $u \in \mathbf{Z}_p$.

---

[68] Nous allons faire comme s'il existait une distribution $\mathbf{z}_{\mathrm{Kato}}(k,j)$ telle que l'on ait (cf. th. 1.9)

$$\mathbf{z}_{\mathrm{Kato},c,d}(k,j) = (c^2 - \langle c^{-1}, 1\rangle) \cdot (d^2 - \langle 1, d^{-1}\rangle) \cdot \mathbf{z}_{\mathrm{Kato}}(k,j).$$

Les calculs montrent que l'existence d'une telle distribution est plus que probable, et pour les transformer en une « vraie » démonstration, il suffit d'appliquer l'opérateur $(c^2 - \langle c^{-1}, 1\rangle) \cdot (d^2 - \langle 1, d^{-1}\rangle)$ à tous les objets en présence, ce qui ne fait que compliquer les formules sans modifier les arguments.

[69] Par linéarité, on en déduit le résultat pour toute fonction à support dans $\mathbf{M}_2(\widehat{\mathbf{Z}})^{(p)}$ et on en déduit le cas général en utilisant l'action des homothéties.

2.4.2. *Construction d'un 2-cocycle.* Si $a,b,c,d\in\{1,\dots,p^n\mathrm{M}\}$ vérifient $a\equiv\alpha$, $b\equiv\beta$ $c\equiv\gamma$ et $d\equiv\delta$ modulo M, soient $\psi_{a,b}^{(n)}$, $\psi_{c,d}^{(n)}$ et $\psi_{a,b,c,d}^{(n)}$ les fonctions caractéristiques de $(a+\mathrm{M}p^n\mathbf{Z}_p)\times(b+\mathrm{M}p^n\mathbf{Z}_p)$, $(c+\mathrm{M}p^n\mathbf{Z}_p)\times(d+\mathrm{M}p^n\mathbf{Z}_p)$ et $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)+\mathrm{M}p^n\mathbf{M}_2(\mathbf{Z}_p)$ respectivement. Notons U_1 et U_2 respectivement les ouverts $(\alpha+\mathrm{M}\mathbf{Z}_p)\times(\beta+\mathrm{M}\mathbf{Z}_p)$ et $(\gamma+\mathrm{M}\mathbf{Z}_p)\times(\delta+\mathrm{M}\mathbf{Z}_p)$ de $\mathbf{Z}_p^2$, et $\mathrm{U}=\mathrm{U}_1\times\mathrm{U}_2$ que l'on voit comme un ouvert de $\mathbf{M}_2(\mathbf{Z}_p)$ et même de $\mathbf{GL}_2(\mathbf{Z}_p)$ puisque $\det\mathrm{A}\in\mathbf{Z}_p^*$ et $p|\mathrm{M}$.

Si $i=1,2$, soit $\mu_i\in\mathrm{H}^1\big(\mathscr{G}_{\mathscr{K}_\mathrm{M}},\mathscr{D}_0\big(\mathrm{U}_i,\mathbf{Z}_p(1)\big)\big)$ la mesure définie par

$$\int\psi_{a,b}^{(n)}\,\mu_1=\int_{(a+\mathrm{M}p^n\widehat{\mathbf{Z}})\times(b+\mathrm{M}p^n\widehat{\mathbf{Z}})}\mathbf{z}_{\mathrm{Siegel}}^{(p)}\ \text{ et }\ \int\psi_{c,d}^{(n)}\,\mu_2=\int_{(c+\mathrm{M}p^n\widehat{\mathbf{Z}})\times(d+\mathrm{M}p^n\widehat{\mathbf{Z}})}\mathbf{z}_{\mathrm{Siegel}}^{(p)}.$$

Soit $\nu=\mu_1\otimes\mu_2\in\mathrm{H}^2\big(\mathscr{G}_{\mathscr{K}_\mathrm{M}},\mathscr{D}_0\big(\mathrm{U},\mathbf{Z}_p(2)\big)\big)$.

Si $i=1,2$, soit Ψ_i une base du $\mathbf{Z}$-module des fonctions localement constantes sur U_i constituée de fonctions du type $\psi_{a,b}^{(n)}$ (resp. $\psi_{c,d}^{(n)}$), avec $n\in\mathbf{N}$ et a,b (resp. c,d) comme ci-dessus. Soit μ_{1,Ψ_1} (resp. μ_{2,Ψ_2}) la distribution algébrique sur U_1 (resp. U_2) définie[70] par

$$\int\psi_{a,b}^{(n)}\,\mu_{1,\Psi_1}=\log[\theta(q,q_{\mathrm{M}p^n}^a\zeta_{\mathrm{M}p^n}^b)]\quad\text{et}\quad\int\psi_{c,d}^{(n)}\,\mu_{2,\Psi_2}=\log[\theta(q,q_{\mathrm{M}p^n}^c\zeta_{\mathrm{M}p^n}^d)],$$

si $\psi_{a,b}^{(n)}$ (resp. $\psi_{c,d}^{(n)}$) appartient à Ψ_1 (resp. Ψ_2).

Lemme 2.6. — Si $i=1,2$, alors μ_i est représenté par le cocycle $\sigma\mapsto\mu_{i,\Psi_i}\star(\sigma-1)$ pour tout choix de Ψ_i.

Démonstration. — Il suffit de revenir à la définition de l'application de Kummer (note 59).

2.4.3. *Descente de $\overline{\mathscr{K}}$ à $\mathscr{K}_{\mathrm{M}p^\infty}$.* Si $i=1,2$, soit $\tilde\mu_{i,\Psi_i}$ la distribution algébrique sur U_i définie par

$$\int\psi_{a,b}^{(n)}\,\tilde\mu_{1,\Psi_1}=\log\theta(\tilde q,\tilde q_{\mathrm{M}p^n}^a\tilde\zeta_{\mathrm{M}p^n}^b)\quad\text{et}\quad\int\psi_{c,d}^{(n)}\,\tilde\mu_{2,\Psi_2}=\log\theta(\tilde q,\tilde q_{\mathrm{M}p^n}^c\tilde\zeta_{\mathrm{M}p^n}^d),$$

si $\psi_{a,b}^{(n)}$ (resp. $\psi_{c,d}^{(n)}$) appartient à Ψ_1 (resp. Ψ_2).

Lemme 2.7. — Si $i=1,2$, alors

(i) $\tilde\mu_{i,\Psi_i}-\mu_{i,\Psi_i}$ est une mesure à valeurs dans $t\mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}})$.

(ii) L'image de μ_i dans $\mathrm{H}^1\big(\mathscr{G}_{\mathscr{K}_\mathrm{M}},\mathscr{D}_0\big(\mathrm{U}_i,t\mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}})\big)\big)$ est représentée par le cocycle $\sigma\mapsto\tilde\mu_{i,\Psi_i}\star(\sigma-1)$ qui est l'inflation d'un cocycle sur $\mathrm{P}_{\mathscr{K}_\mathrm{M}}$ à valeurs dans $\mathscr{D}_0\big(\mathrm{U}_i,t\mathbb{B}_{\mathrm{dR}}^+(\mathscr{K}_{\mathrm{M}p^\infty})\big)$.

[70] $\log[\theta(q,q_\mathrm{M}^a,\zeta_\mathrm{M}^b)]$ et $\log\theta(\tilde q,\tilde q_\mathrm{M}^a\tilde\zeta_\mathrm{M}^b)$ sont des notations commodes, mais ne correspondent pas à des éléments de $\mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}})$; le principal problème est que le q-développement de $\log\theta(q,q_\mathrm{M}^a\zeta_\mathrm{M}^b)$ admet des dénominateurs non bornés et donc ne définit pas un élément de $\mathscr{K}_\mathrm{M}$. Par contre,

- $\log[\theta(q,q_\mathrm{M}^a,\zeta_\mathrm{M}^b)]\star(\sigma-1)=\log\frac{[\theta(q,q_\mathrm{M}^a,\zeta_\mathrm{M}^b)]\star\sigma}{[\theta(q,q_\mathrm{M}^a,\zeta_\mathrm{M}^b)]}\in\mathbf{Q}_p\cdot t$, si $\sigma\in\mathscr{G}_{\mathscr{K}_\mathrm{M}}$,
- $\log\theta(\tilde q,\tilde q_\mathrm{M}^a\tilde\zeta_\mathrm{M}^b)-\log[\theta(q,q_\mathrm{M}^a,\zeta_\mathrm{M}^b)]=\log\frac{\theta(\tilde q,\tilde q_\mathrm{M}^a\tilde\zeta_\mathrm{M}^b)}{[\theta(q,q_\mathrm{M}^a,\zeta_\mathrm{M}^b)]}\in t\mathbb{B}_{\mathrm{dR}}^+(\overline{\mathscr{K}})$,
- $\log\theta(\tilde q\tilde\zeta^x,\tilde q_\mathrm{M}^a\tilde\zeta_\mathrm{M}^{b+y})-\log\theta(\tilde q,\tilde q_\mathrm{M}^a\tilde\zeta_\mathrm{M}^b)\in t\mathscr{O}_{\mathscr{K}_\mathrm{M}}[[\frac{t}{p}]]$, si $x,y\in\mathbf{Z}_p$,

sont bien définis ; c'est toujours ce type d'expression qui intervient dans les calculs.

Démonstration. — Le (ii) est une conséquence immédiate du (i) qui, quant à lui, résulte de ce que $[\theta(q, q^a_{\mathrm{M}p^n}\zeta^b_{\mathrm{M}p^n})]^{-1}\theta(\tilde{q}, \tilde{q}^a_{\mathrm{M}p^n}\tilde{\zeta}^b_{\mathrm{M}p^n})$ appartient à $1+\tilde{q}^{-1}\mathbb{A}_{\mathrm{inf}}(\overline{\mathscr{K}})$ et a pour image 1 dans $\mathbb{C}(\overline{\mathscr{K}})$, et donc que l'ensemble des $\log\theta(\tilde{q}, \tilde{q}^a_{\mathrm{M}p^n}\tilde{\zeta}^b_{\mathrm{M}p^n}) - \log[\theta(q, q^a_{\mathrm{M}p^n}\zeta^b_{\mathrm{M}p^n})]$ est borné dans $t\mathbb{B}^+_{\mathrm{dR}}(\overline{\mathscr{K}})$ quand n décrit $\mathbf{N}$ et a, b décrivent $\mathbf{Z}$.

Si Λ_1 et Λ_2 sont deux G-modules à droite, si $x_1 \in \Lambda_1$ et $x_2 \in \Lambda_2$, et si $\sigma, \tau \in \mathrm{G}$, on note $\{x_1 \otimes x_2\}_{\sigma,\tau}$ l'élément de $\Lambda_1 \otimes \Lambda_2$ défini par

$$\{x_1 \otimes x_2\}_{\sigma,\tau} = \big(x_1 \star (\tau\sigma - \sigma)\big) \otimes \big(x_2 \star (\sigma - 1)\big).$$

Corollaire 2.8. — *L'image de* $\nu = \mu_1 \otimes \mu_2$ *dans* $\mathrm{H}^2\big(\mathscr{G}_{\mathscr{K}_\mathrm{M}}, \mathscr{D}_0\big(\mathrm{U}, t^2\mathbb{B}^+_{\mathrm{dR}}(\overline{\mathscr{K}})\big)\big)$ *peut se représenter par l'inflation de* $\mathrm{P}_{\mathscr{K}_\mathrm{M}}$ *à* $\mathscr{G}_{\mathscr{K}_\mathrm{M}}$ *du 2-cocycle* $(\sigma, \tau) \mapsto \{\mu_{1,\Psi_1} \otimes \mu_{2,\Psi_2}\}_{\sigma,\tau}$.

2.4.4. *Descente de* $\mathscr{K}_{\mathrm{M}p^\infty}$ *à* $\mathscr{K}_\mathrm{M}$. Par définition de $\mathbf{z}_{\mathrm{Kato},c,d}(k,j)$ et de ν, on a $z_{\mathrm{M,A}} = \int_\mathrm{U} \big((e_1^{k-2}t^{-j}) \star g\big)\ \nu$ et, d'après ce qui précède, $z_{\mathrm{M,A}}$ est la classe du 2-cocycle

$$(\sigma, \tau) \mapsto \int_\mathrm{U} \big((e_1^{k-2}t^{-j}) \star g\big)\ \{\mu_{1,\Psi_1} \otimes \mu_{2,\Psi_2}\}_{\sigma,\tau},$$

qui est aussi, d'après la proposition 2.2, la classe du 2-cocycle

$$(\sigma, \tau) \mapsto \mathrm{R_M}\Big(\int_\mathrm{U} \big((e_1^{k-2}t^{-j}) \star g\big)\ \{\mu_{1,\Psi_1} \otimes \mu_{2,\Psi_2}\}_{\sigma,\tau}\Big)$$
$$= \int_\mathrm{U} \big((e_1^{k-2}t^{-j}) \star g\big)\ \mathrm{R_M}(\{\mu_{1,\Psi_1} \otimes \mu_{2,\Psi_2}\}_{\sigma,\tau}).$$

Lemme 2.9. — Si $ad - bc \in \mathbf{Z}_p^*$, alors

$$\mathrm{R_M}\big(\log\theta(\tilde{q}, \tilde{q}^a_{\mathrm{M}p^n}\tilde{\zeta}^b_{\mathrm{M}p^n}) \cdot \log\theta(\tilde{q}, \tilde{q}^c_{\mathrm{M}p^n}\tilde{\zeta}^d_{\mathrm{M}p^n})\big) = p^{-2n}\log\theta(\tilde{q}^{p^n}, \tilde{q}^a_\mathrm{M}\tilde{\zeta}^b_\mathrm{M}) \cdot \log\theta(\tilde{q}^{p^n}, \tilde{q}^c_\mathrm{M}\tilde{\zeta}^d_\mathrm{M}).$$

Démonstration. — Ce lemme se démontre en regardant les q-développements des logarithmes des unités de Siegel et en utilisant le fait que

$$\mathrm{R_M}\big((\tilde{q}^a_{\mathrm{M}p^n}\tilde{\zeta}^b_{\mathrm{M}p^n})^i(\tilde{q}^c_{\mathrm{M}p^n}\tilde{\zeta}^d_{\mathrm{M}p^n})^j\big) = \begin{cases} (\tilde{q}^a_{\mathrm{M}p^n}\tilde{\zeta}^b_{\mathrm{M}p^n})^i(\tilde{q}^c_{\mathrm{M}p^n}\tilde{\zeta}^d_{\mathrm{M}p^n})^j & \text{si } p^n | ai + cj \text{ et } p^n | bi + dj, \\ 0 & \text{sinon,} \end{cases}$$

la condition $ad - bc \in \mathbf{Z}_p^*$ entraînant miraculeusement que $ai + cj$ et $bi + dj$ sont divisibles par p^n si et seulement si i et j le sont.

Corollaire 2.10. — *On peut représenter* $z_{\mathrm{M,A}}$ *par le 2-cocycle*

$$(\sigma, \tau) \mapsto \lim_{n\to+\infty} p^{-2n} \sum \frac{(ae_1 + be_2)^{k-2}}{(ad - bc)^j t^j} \big\{\log\theta(\tilde{q}^{p^n}, \tilde{q}^a_\mathrm{M}\tilde{\zeta}^b_\mathrm{M}) \otimes \log\theta(\tilde{q}^{p^n}, \tilde{q}^c_\mathrm{M}\tilde{\zeta}^d_\mathrm{M})\big\}_{\sigma,\tau},$$

la somme portant sur les quadruplets a, b, c, d *d'entiers* $\in \{1, \ldots \mathrm{M}p^n\}$, *avec* $a \equiv \alpha$, $b \equiv \beta$, $c \equiv \gamma$, $d \equiv \delta$ *modulo* M.

2.4.5. *Passage à l'agèbre de Lie.* Le cocycle ci-dessus est un 2-cocycle analytique, à valeurs dans $\widetilde{\mathscr{K}_{\mathrm{M}}} \otimes \mathrm{V}_{k,j}$; son image dans $\mathscr{K}_{\mathrm{M}}$ par l'application $\exp^*$ peut donc se calculer en utilisant les techniques différentielles du § 2.2.

Remarquons que les rôles de a, b, c et d ne sont pas tout à fait symétriques car $\tilde{\zeta}^x$ est analytique en x, alors que $\tilde{q}^x$ n'est défini que pour les valeurs entières de x. On dit que $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \mathrm{F}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ est p^n-négligeable si, à a et c fixés, la fonction $(x,y) \mapsto \mathrm{F}\left(\begin{smallmatrix} a & \beta+\mathrm{M}x \\ c & \beta+\mathrm{M}y \end{smallmatrix}\right)$ est élément de $p^n\mathscr{O}_{\mathscr{K}_{\mathrm{M}}}[[\mathrm{M}x, \mathrm{M}y, \frac{tx}{p}, \frac{ty}{p}]]$. On a alors

$$p^{-2n} \sum_{\substack{b\equiv\beta\,[\mathrm{M}] \\ d\equiv\delta\,[\mathrm{M}] \\ 1\leq b,d\leq \mathrm{M}p^n}} \mathrm{F}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in p^n\mathscr{O}_{\mathscr{K}_{\mathrm{M}}}[[p^{-1}t]].$$

Si $f(x_1,x_2)$ est une fonction de deux variables, on note D_1 et D_2 respectivement les opérateurs $x_1\frac{d}{dx_1}$ et $x_2\frac{d}{dx_2}$. Si $n\in\mathbf{N}$ et si a,b sont deux entiers, on pose $f_{a,b}^{(n)} = f(\tilde{q}^{p^n}, \tilde{q}_{\mathrm{M}}^a\tilde{\zeta}_{\mathrm{M}}^b)$.

Lemme 2.11. — A addition près d'un élément p^n-négligeable près, on a

$$\delta^{(2)}\Big(\big\{\log\theta_{a,b}^{(n)}\otimes\log\theta_{c,d}^{(n)}\big\}_{\sigma,\tau}\Big) = \frac{(ad-bc)t^2}{\mathrm{M}^2}\cdot \mathrm{D}_2\log\theta_{a,b}^{(n)}\cdot \mathrm{D}_2\log\theta_{c,d}^{(n)}.$$

Démonstration. — Cela résulte du développement limité

$$\log\theta_{a,b}^{(n)}\star\Big(\left(\begin{smallmatrix} 1 & u \\ 0 & e^v \end{smallmatrix}\right)-1\Big) = p^nt\cdot \mathrm{D}_1\log\theta_{a,b}^{(n)} + \frac{(au+bv)t}{\mathrm{M}}\cdot \mathrm{D}_2\log\theta_{a,b}^{(n)} + \mathrm{O}((u,v)^2),$$

et de ce que $\mathrm{D}_1\log\theta$ et $\mathrm{D}_2\log\theta$ ont des développements à coefficients entiers.

Lemme 2.12. — Si f et g sont à coefficients entiers, si $s\geq 2-j$ et $a,b,c,d\in\mathbf{Z}$, alors

$$(ae_1+be_2)^{k-2}t^sf_{a,b}^{(n)}\Big(a\cdot g_{c,d}^{(n)} + \frac{1}{1-s}\cdot(ad-bc)\cdot\frac{t}{\mathrm{M}}\cdot \mathrm{D}_2g_{c,d}^{(n)}\Big)$$

est p^n-négligeable dans $(\widetilde{\mathscr{K}_{\mathrm{M}}}\otimes\mathrm{V}_{k,j})/(\partial_1, 1-\partial_2)$.

Démonstration. — Cela résulte du calcul de $(a(1-\partial_2)+b\partial_1)\big((ae_1+be_2)^{k-2}t^sf_{a,b}^{(n)}g_{c,d}^{(n)}\big)$ qui peut se faire en utilisant les formules

$$\partial_1t=0,\ \partial_2t=t \qquad \partial_1e_1=e_2,\ \partial_2e_1=0 \qquad \partial_1e_2=0,\ \partial_2e_2=e_2$$
$$\partial_1f_{a,b}^{(n)} = p^nt\cdot \mathrm{D}_1f_{a,b}^{(n)} + \frac{at}{\mathrm{M}}\cdot \mathrm{D}_2f_{a,b}^{(n)}, \qquad \partial_2f_{a,b}^{(n)} = \frac{bt}{\mathrm{M}}\cdot \mathrm{D}_2f_{a,b}^{(n)},$$

en modifiant de manière évidente la dernière ligne pour caluler $\partial_1g_{c,d}^{(n)}$ et $\partial_2g_{c,d}^{(n)}$.

Corollaire 2.13. — *A addition d'un élément p^n-négligeable près, on a*

$$\mathrm{res}_{k,j}\Big(\frac{(ae_1+be_2)^{k-2}}{(ad-bc)^jt^j}\cdot\delta^{(2)}\big(\big\{\log\theta_{a,b}^{(n)}\otimes\log\theta_{c,d}^{(n)}\big\}_{\sigma,\tau}\big)\Big)$$
$$= \mathrm{M}^{-1-j}\cdot\frac{(-1)^{j-1}}{(j-1)!}\cdot a^{k-1-j}\cdot \mathrm{D}_2\log\theta_{a,b}^{(n)}\cdot \mathrm{D}_2^j\log\theta_{c,d}^{(n)}.$$

Démonstration. — Cela résulte du lemme 2.11, d'une récurrence utilisant le lemme 2.12, de la définition de l'application $\mathrm{res}_{k,j}$ (cf. prop. 2.4), et de ce que $\mathrm{res}_{k,j}(t^s e_1^i e_2^{k-2-i} f(\tilde{q})) = 0$ si $s \geq 2$.

Comme $\mathrm{D}_2^r \log\theta(x_1, x_2) = \mathrm{E}_r(x_1, x_2)$, et comme $\zeta_{\mathrm{M}}^b = \zeta_{\mathrm{M}}^\beta$ si $b \equiv \beta\,[\mathrm{M}]$ et $\zeta_{\mathrm{M}}^d = \zeta_{\mathrm{M}}^\delta$ si $d \equiv \delta\,[\mathrm{M}]$, on en déduit la formule

$$\exp^*(z_{\mathrm{M,A}}) = \mathrm{M}^{-3-j}\frac{(-1)^{j-1}}{(j-1)!}\lim_{n\to+\infty}\sum_{\substack{a\equiv\alpha\,[\mathrm{M}]\\ c\equiv\gamma\,[\mathrm{M}]\\ 1\leq a,c\leq \mathrm{M}p^n}} a^{k-1-j}\mathrm{E}_1(q^{p^n}, q_{\mathrm{M}}^a\zeta_{\mathrm{M}}^\beta)\mathrm{E}_j(q^{p^n}, q_{\mathrm{M}}^c\zeta_{\mathrm{M}}^\delta).$$

On termine la démonstration de la proposition 2.5, en utilisant le lemme suivant :

Lemme 2.14. — (i) $\sum_{c\equiv\gamma\,[\mathrm{M}],\ 1\leq c\leq \mathrm{M}p^n} \mathrm{E}_j(q^{p^n} q_{\mathrm{M}}^c\zeta_{\mathrm{M}}^\delta) = \mathrm{E}_j(q, q_{\mathrm{M}}^\gamma\zeta_{\mathrm{M}}^\delta) = \mathrm{E}^{(j)}_{\gamma/\mathrm{M},\,\delta/\mathrm{M}}$

(ii) Si $r \in \mathbf{N}$, alors

$$\lim_{n\to\infty}\sum_{a\equiv\alpha\,[\mathrm{M}],\ 1\leq a\leq \mathrm{M}p^n} a^r\mathrm{E}_1(q^{p^n}, q_{\mathrm{M}}^a\zeta_{\mathrm{M}}^\beta) = \mathrm{M}^r\mathrm{F}_{r+1}(q, q_{\mathrm{M}}^\alpha, \zeta_{\mathrm{M}}^\beta) = \mathrm{M}^r\mathrm{F}^{(r+1)}_{\alpha/\mathrm{M},\,\beta/\mathrm{M}}.$$

Démonstration. — Le (i) se démontre en revenant à la définition. Pour démontrer le (ii), on part de la formule

$$\mathrm{E}_1(q^{p^n}, q_{\mathrm{M}}^a\zeta_{\mathrm{M}}^\beta) = \mathrm{F}_1(q^{p^n}, q_{\mathrm{M}}^a\zeta_{\mathrm{M}}^\beta) = \mathrm{F}^{(1)}_{a/\mathrm{M}p^n,\,\beta/\mathrm{M}}(q^{p^n}),$$

et on utilise la formule pour le q-développement de $\mathrm{F}^{(k)}_{\alpha,\beta}$ donnée dans la prop. 1.3.

3. FORMES PROPRES POUR LES OPÉRATEURS DE HECKE

Ce chapitre est consacré à la construction (th. 3.1) d'un système d'Euler pour la représentation p-adique associée à une forme primitive, et aux résultats de théorie d'Iwasawa que l'on peut en tirer (th. 3.2). Nous renvoyons au (v) de la remarque 3.3 pour des commentaires sur l'articulation des arguments.

3.1. Le système d'Euler de Kato associé à une forme primitive

3.1.1. *Projection sur un espace propre.* Soient $\mathrm{N} \geq 1$ et $k \geq 2$ des entiers, et ε un caractère de Dirichlet modulo N (pas nécessairement primitif). Soit $f = \sum_{n=1}^{+\infty} a_n q^n \in \mathrm{S}_k(\Gamma_0(\mathrm{N}), \varepsilon)$ une forme primitive. En particulier, $a_1 = 1$ et $\mathbf{Q}(f) = \mathbf{Q}(a_2, \ldots, a_n, \ldots)$ est une extension finie de $\mathbf{Q}$. De plus, on a $\overline{a_n} = \varepsilon^{-1}(n)a_n$ quel que soit $n \in \mathbf{N}$ premier à N, et

$$f \star \mathrm{T}(\ell) = a_\ell f, \quad f \star \mathrm{T}'(\ell) = \overline{a_\ell} f, \quad f \star \left(\begin{smallmatrix} u^{-1} & 0 \\ 0 & u \end{smallmatrix}\right) = \varepsilon(u)f,$$

si $\ell \nmid \mathrm{N}$ est un nombre premier et $u \in \widehat{\mathbf{Z}}^*$.

Si S est un sous-ensemble fini de $\mathscr{P}$, et si M est un $\mathbf{Q}(f)$-espace vectoriel muni d'actions des $\mathrm{T}(\ell), \mathrm{T}'(\ell)$, $\ell \notin \mathrm{S}$ et $\left(\begin{smallmatrix} u^{-1} & 0 \\ 0 & u \end{smallmatrix}\right)$, pour $u \in \mathrm{U}$ sous-groupe ouvert de $\widehat{\mathbf{Z}}^*$, on note M_{π_f} le quotient de M par le sous-$\mathbf{Q}(f)$-espace vectoriel engendré par les $x \star \mathrm{T}(\ell) - a_\ell x$, $x \in \mathrm{M}$ et

$\ell \notin \mathrm{S}$. Dans tous les cas que nous aurons à considérer, le théorème de multiplicité 1 fort entraîne que l'on a $x \star \mathrm{T}'(\ell) = \overline{a_\ell} x$ et $x \star \left(\begin{smallmatrix} u^{-1} & 0 \\ 0 & u \end{smallmatrix}\right) = \varepsilon(u) x$, si $x \in \mathrm{M}$, et si $\ell \notin \mathrm{S}$ et $u \in \mathrm{U}$.

3.1.2. *La représentation p-adique associée à une forme primitive.* Un exemple d'utilisation de la construction précédente est la définition de la représentation p-adique associée à f. Notons $\widehat{\Gamma}_{1,\mathrm{N}}$ le sous-groupe de $\mathbf{SL}_2(\widehat{\mathbf{Z}})$ des matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ avec $c \equiv d-1 \equiv 0$ modulo N. Soit $\widetilde{\Gamma}_{1,\mathrm{N}}$ l'image inverse de $\widehat{\Gamma}_{1,\mathrm{N}}$ dans $\Pi_{\mathbf{Q}}$ et soit $\overline{\Gamma}_{1,\mathrm{N}}$ l'intersection[71] de $\widetilde{\Gamma}_{1,\mathrm{N}}$ et $\Pi_{\overline{\mathbf{Q}}}$. On définit[72] alors la représentation V_f associée à f par

$$\mathrm{V}_f = \big(\mathrm{H}^1(\overline{\Gamma}_{1,\mathrm{N}}, \mathrm{Sym}^{k-2}\mathrm{V}_p) \otimes_{\mathbf{Q}_p} \mathbf{Q}_p(f)\big)_{\pi_f} \otimes_{\mathbf{Q}_p} \mathbf{Q}_p(2-k).$$

C'est une $\mathbf{Q}_p(f)$-représentation de $\mathscr{G}_{\mathbf{Q}}$ de dimension 2, non ramifiée en dehors de Np. Si $\ell \nmid p\mathrm{N}$, le déterminant de $1-\mathrm{Frob}_\ell^{-1}\mathrm{X}$ agissant sur V_f est $1-a_\ell\mathrm{X}+\varepsilon(\ell)\ell^{k-1}\mathrm{X}^2$. La restriction de V_f à $\mathscr{G}_{\mathbf{Q}_p}$ est de de Rham, de poids de Hodge-Tate 0 et $1-k$; elle est cristalline si $p \nmid \mathrm{N}$ et le polynôme caractéristique de φ sur $\mathbf{D}_{\mathrm{cris}}(\mathrm{V}_f)$ est $\mathrm{X}^2 - a_p\mathrm{X} + \varepsilon(p)p^{k-1}$; elle est semi-stable si $p|\mathrm{N}$ et $a_p \neq 0$ (auquel cas, a_p est la valeur propre de φ sur $\mathbf{D}_{\mathrm{cris}}(\mathrm{V}_f)$) et seulement potentiellement semi-stable si $p|\mathrm{N}$ et $a_p = 0$.

3.1.3. *La fonction* L *de f et ses tordues.* Si ϕ est une fonction localement constante sur $\widehat{\mathbf{Z}}$ à valeurs dans $\mathbf{Q}(f)$, on définit la fonction $\mathrm{L}(f,\phi,s)$ par la formule

$$\mathrm{L}(f,\phi,s) = \sum_{n\geq 1} \phi(n)\, a_n\, n^{-s}.$$

Cette fonction possède un prolongement analytique à tout le plan complexe et il existe des nombres complexes non nuls Ω_f^+ et Ω_f^-, tels que, si ϕ est constante modulo $\mathrm{N}\widehat{\mathbf{Z}}$, alors

$$\frac{\Gamma(j)}{(2i\pi)^j}\mathrm{L}(f,\phi,j) \in \begin{cases} \mathbf{Q}(f,\zeta_{\mathrm{N}}) \cdot \Omega_f^+ & \text{si } 1 \leq j \leq k-1 \text{ et } \phi(-x) = (-1)^j\phi(x), \\ \mathbf{Q}(f,\zeta_{\mathrm{N}}) \cdot \Omega_f^- & \text{si } 1 \leq j \leq k-1 \text{ et } \phi(-x) = (-1)^{j+1}\phi(x). \end{cases}$$

Si $\phi \in \mathrm{LC}(\widehat{\mathbf{Z}}, \mathbf{Q}(f))$, on définit la fonction $\phi \circ (-1)$ par $(\phi\circ(-1))(x) = \phi(-x)$ et on modifie $\mathrm{L}(f,\phi,j)$ de manière à le rendre algébrique en posant

$$\widetilde{\mathrm{L}}(f,\phi,j) = \frac{1}{2}\cdot\frac{\Gamma(j)}{(2i\pi)^j}\Big(\frac{\mathrm{L}(f,\phi+(-1)^j\phi\circ(-1),j)}{\Omega_f^+} + \frac{\mathrm{L}(f,\phi-(-1)^j\phi\circ(-1),j)}{\Omega_f^-}\Big),$$

ce qui permet d'étendre $\phi \mapsto \widetilde{\mathrm{L}}(f,\phi,j)$ par linéarité à $\mathrm{LC}(\widehat{\mathbf{Z}}, \mathrm{A})$ pour toute $\mathbf{Q}(f)$-algèbre A.

[71]Si $\mathrm{N} \geq 5$, c'est le complété profini du groupe fondamental de la surface de Riemann $\mathrm{Y}_1(\mathrm{N})$.

[72]V_p est la représentation apparaissant au n° 1.5.2 ; c'est le module de Tate de la courbe elliptique universelle.

3.1.4. *Caractérisation du système d'Euler de Kato et applications.* On note f^* la conjuguée complexe de f (i.e. $f^*(z) = \overline{f(\overline{z})} = \sum \overline{a_n} q^n$).

Théorème 3.1. — *Il existe un unique élément* $\mathbf{z}_{\mathrm{Kato}}(f)$ *de* $\mathrm{H}^1(\mathscr{G}_{\mathbf{Q}}, \mathscr{D}_0(\widehat{\mathbf{Z}}^{(p)}, \mathrm{V}_f))$ *tel que, quels que soient* $j \in \{0, \dots, k-2\}$ *et* $\phi \in \mathrm{LC}(\widehat{\mathbf{Z}}^{(p)}, \mathbf{Q}(f))$, *on ait*[73]

$$\exp^*\Big(\int_{\widehat{\mathbf{Z}}^{(p)}} \phi(x)\ (t\cdot x_p)^{k-1-j}\ \mathbf{z}_{\mathrm{Kato}}(f)\Big) = \frac{1}{j!}\widetilde{\mathrm{L}}(f^*, \phi, j+1)\cdot f.$$

Soit Λ l'algèbre de groupe complétée de $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q})$ identifié à $\mathbf{Z}_p^*$. Si E est une extension finie de $\mathbf{Q}_p$, alors $\mathrm{E}\otimes_{\mathbf{Z}_p}\Lambda = \mathscr{D}_0(\mathbf{Z}_p^*, \mathrm{E})$ est un produit[74] d'anneaux principaux, ce qui permet d'associer à un module M de torsion sur $\mathrm{E}\otimes_{\mathbf{Z}_p}\Lambda$ sa mesure caractéristique $|\mathrm{M}|_\Lambda$ définie, composante par composante, à multiplication près par une unité de $\mathrm{E}\otimes_{\mathbf{Z}_p}\Lambda$, comme le produit des diviseurs élémentaires de M.

Si W est une E-représentation de $\mathscr{G}_{\mathbf{Q}}$, soient $\mathrm{H}^i_{\mathrm{Iw}}(\mathrm{W}) = \mathrm{H}^i(\mathscr{G}_{\mathbf{Q}}, \mathscr{D}_0(\mathbf{Z}_p^*, \mathrm{W}))$, $i \in \mathbf{N}$, les modules d'Iwasawa associés à W ; ce sont des $\mathrm{E}\otimes_{\mathbf{Z}_p}\Lambda$-modules de type fini, nuls si $i = 0$ ou si $i \geq 3$. Si η est un caractère de Dirichlet de conducteur M premier à p, on note $\mathbf{z}_{\mathrm{Kato}}(f, \eta)$ l'élément de $\mathrm{H}^1_{\mathrm{Iw}}(\mathrm{V}_{f\otimes\eta})$ défini[75] par

$$\int_{\mathbf{Z}_p^*} \phi\ \mathbf{z}_{\mathrm{Kato}}(f,\eta) = \int_{\widehat{\mathbf{Z}}^{(p)}} \eta(x)\phi(x_p)\ \mathbf{z}_{\mathrm{Kato}}(f).$$

Théorème 3.2. — (i) $\mathrm{H}^1_{\mathrm{Iw}}(\mathrm{V}_{f\otimes\eta})$ *est un* $\mathbf{Q}_p(f,\eta)\otimes\Lambda$*-module libre de rang* 1.

(ii) $\mathrm{H}^2_{\mathrm{Iw}}(\mathrm{V}_{f\otimes\eta})$ *et* $\mathrm{H}^1_{\mathrm{Iw}}(\mathrm{V}_{f\otimes\eta})/\mathbf{z}_{\mathrm{Kato}}(f,\eta)$ *sont des* $\mathbf{Q}_p(f,\eta)\otimes_{\mathbf{Z}_p}\Lambda$*-modules de torsion, et* $\big|\mathrm{H}^2_{\mathrm{Iw}}(\mathrm{V}_{f\otimes\eta})\big|_\Lambda$ *divise* $\big|\mathrm{H}^1_{\mathrm{Iw}}(\mathrm{V}_{f\otimes\eta})/\mathbf{z}_{\mathrm{Kato}}(f,\eta)\big|_\Lambda \cdot |\mathrm{H}^2(\mathscr{G}_{\mathbf{Q}_p}, \Lambda\otimes\mathrm{V}_{f\otimes\eta})|_\Lambda$.

Remarque 3.3. — (i) On conjecture que l'on a en fait

$$\big|\mathrm{H}^2_{\mathrm{Iw}}(\mathrm{V}_{f\otimes\eta})\big|_\Lambda = \big|\mathrm{H}^1_{\mathrm{Iw}}(\mathrm{V}_{f\otimes\eta})/\mathbf{z}_{\mathrm{Kato}}(f,\eta)\big|_\Lambda \cdot |\mathrm{H}^2(\mathscr{G}_{\mathbf{Q}_p}, \Lambda\otimes\mathrm{V}_{f\otimes\eta})|_\Lambda,$$

ce qui est une des formulations de la « conjecture principale ». Dans cette formulation en termes « d'éléments zêta », spécialisation aux formes modulaires d'une conjecture générale de Kato [99], les fonctions L p-adiques n'apparaissent pas. Le lien avec la formulation de Perrin-Riou [142] s'établit en montrant que la fonction L p-adique est l'image de $\mathbf{z}_{\mathrm{Kato}}(f)$ par l'exponentielle de Perrin-Riou (c'est le sujet du chapitre 4 ; voir en particulier les th. 4.4, 4.11 et 4.15). Remarquons quand même que la formulation de la conjecture principale en termes d'éléments zêta n'impose aucune propriété de « bonne réduction » à la forme modulaire f, alors qu'il reste du travail pour définir une fonction L p-adique en toute généralité.

[73]Dans cet énoncé, t“=”$2i\pi$ désigne le générateur habituel de $\mathbf{Z}_p(1)$, $x_p \in \mathbf{Z}_p^*$ désigne la composante de x sur $\mathbf{Z}_p$, ce qui fait que, $\int_{\widehat{\mathbf{Z}}^{(p)}} \phi(x)\ (t\cdot x_p)^j\ \mathbf{z}_{\mathrm{Kato}}(f) \in \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}(\zeta_{\mathrm{N}})}, \mathrm{V}_f(j))$, si ϕ est constante modulo $\mathrm{N}\widehat{\mathbf{Z}}$. Son image par $\exp^*$ appartient donc à $\mathbf{D}^0_{\mathrm{dR}}(\mathrm{V}_f(j))\otimes_{\mathbf{Q}_p(f)}\mathbf{Q}_p(f,\zeta_{\mathrm{N}}) = \mathbf{Q}_p(f,\zeta_{\mathrm{N}})\cdot f$, ce qui donne un sens à l'égalité du théorème, l'identification de $\mathbf{D}^0_{\mathrm{dR}}(\mathrm{V}_f)$ à $\mathbf{Q}_p(f)\cdot f$ se faisant via les deux applications $\exp^*$ comme expliqué dans l'introduction (cf. n° 0.6.5).

[74]Sur les caractères du sous-groupe de torsion de $\mathbf{Z}_p^*$.

[75]Dans cette formule, on voit η comme une fonction sur $\widehat{\mathbf{Z}}$ localement constante modulo M.

(ii) Si W est une E-représentation de $\mathscr{G}_{\mathbf{Q}_p}$, le module $\mathrm{H}^2(\mathscr{G}_{\mathbf{Q}_p}, \Lambda \otimes \mathrm{W})$ est isomorphe à[76] $\mathrm{H}^0(\mathscr{G}_{\mathbf{Q}_p(\zeta_{p^\infty})}, \mathrm{W}^*(1))^*$; il est donc nul en général.

(iii) Si le conducteur de $f \otimes \eta$ n'est pas divisible par N, la divisibilité ci-dessus n'est pas optimale : il peut s'être introduit des facteurs d'Euler en les places divisant N.

(iv) Sous des hypothèses supplémentaires concernant la représentation (satisfaites pour presque tout nombre premier si f n'est pas de type CM), on peut prouver des résultats du même genre sans avoir à inverser p.

(v) La démonstration des théorèmes 3.1 et 3.2 est un peu tortueuse. On projette les systèmes d'Euler $\mathbf{z}_{\mathrm{Kato}}(k, j)$, pour $1 \leq j \leq k-1$, sur la composante correspondant à f, ce qui permet de construire toute une famille (cf. § 3.3) de systèmes d'Euler pour V_f et ses tordues. On calcule l'image par l'application $\exp^*$ des éléments ainsi construits en utilisant la loi de réciprocité explicite de Kato et en projetant sur la composante correspondant à f, ce qui nous conduit à calculer le produit scalaire de Petersson de f avec un produit de séries d'Eisenstein ; on utilise la méthode de Rankin (cf. § 3.2) pour ce faire, et le résultat fait intervenir les valeurs de fonctions L du théorème 3.1. Ces systèmes d'Euler ne sont pas optimaux[77], mais ils permettent, en utilisant la technique des dérivées de Kolyvagin [107, 100, 143, 159, 116] de démontrer que $\mathrm{H}^1_{\mathrm{Iw}}(\mathrm{V}_{f\otimes\eta})$ est un $\mathbf{Q}_p(f,\eta)\otimes\Lambda$-module libre de rang 1 pour tout caractère η. On construit[78] alors $\mathbf{z}_{\mathrm{Kato}}(f, \eta)$ comme combinaison linéaire, à coefficients dans l'anneau des fractions de $\mathbf{Q}(f,\eta) \otimes_{\mathbf{Z}_p} \Lambda$, des systèmes d'Euler précédents[79] ; le problème étant de montrer que l'élément ainsi construit est encore dans $\mathrm{H}^1_{\mathrm{Iw}}(\mathrm{V}_{f\otimes\eta})$, ce qui se fait en utilisant les calculs précédents pour l'application $\exp^*$ ainsi que le fait que l'on a une infinité de choix à notre disposition, ce qui permet de montrer que l'on n'a pas introduit de pôle parasite. Une fois que l'on a rendu le système d'Euler optimal, on peut réutiliser la technique de Kolyvagin pour démontrer le (ii) du théorème 3.2.

3.2. **La méthode de Rankin-Selberg**

3.2.1. *Le cas général.* Soit $\Gamma = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbf{Z}) \ b \equiv c \equiv 0 \ [\mathrm{N}]\right\}$. Soit ε_1 et ε_2 des caractères de Dirichlet modulo N (pas nécessairement primitifs). Soient $k \geq 2$, $1 \leq j \leq k-1$, et

$$f = \sum_{n \in \frac{1}{\mathrm{N}}\mathbf{Z},\ n>0} a_n q^n \in \mathrm{S}_k(\Gamma, \varepsilon_1) \quad \text{et} \quad g = \sum_{n \in \frac{1}{\mathrm{N}}\mathbf{Z},\ n\geq 0} b_n q^n \in \mathrm{M}_{k-j}(\Gamma, \varepsilon_2),$$

[76] et pas à $\mathrm{H}^0(\mathscr{G}_{\mathbf{Q}_p(\zeta_{p^\infty})}, \mathrm{W}(-1))$ comme il est affirmé dans [54]...

[77] Il y a des tas de facteurs parasites qui interviennent, par exemple à cause de l'introduction de c et d pour définir $\mathbf{z}_{\mathrm{Kato},c,d}(k, j)$, ou de la disparition des facteurs d'Euler en les places divisant N.

[78] Pour cette partie de l'argument, le lecteur est invité à consulter le §13 de [102].

[79] tordus à la Soulé pour passer de $\mathrm{V}_f(j)$ à V_f.

des forme propres pour tous les opérateurs $\mathrm{T}(\ell)$, ℓ premier ne divisant pas N. On a donc

$$\sum_{n>0}\frac{a_n}{n^s}=\Big(\sum_{n\in\mathbf{Z}[\frac{1}{\mathrm{N}}]^*}\frac{a_n}{n^s}\Big)\cdot\prod_{\ell\nmid\mathrm{N}}\frac{1}{((1-\alpha_{\ell,1}\ell^{-s})(1-\alpha_{\ell,2}\ell^{-s})},\quad\text{avec } \alpha_{\ell,1}\alpha_{\ell,2}=\varepsilon_1(\ell)\ell^{k-1},$$

$$\sum_{n>0}\frac{b_n}{n^s}=\Big(\sum_{n\in\mathbf{Z}[\frac{1}{\mathrm{N}}]^*}\frac{b_n}{n^s}\Big)\cdot\prod_{\ell\nmid\mathrm{N}}\frac{1}{((1-\beta_{\ell,1}\ell^{-s})(1-\beta_{\ell,2}\ell^{-s})},\quad\text{avec } \beta_{\ell,1}\beta_{\ell,2}=\varepsilon_2(\ell)\ell^{k-j-1}.$$

Soient $\mathrm{D}(f,g,s)$ la série de Dirichlet définie par

$$\mathrm{D}(f,g,s)=\mathrm{L}(\overline{\varepsilon}_1\varepsilon_2,j+2(s-k+1))\cdot\sum_{n>0}\frac{\overline{a_n}b_n}{n^s}$$

et $\mathrm{E}_s(\tau)$ la série d'Eisenstein (de poids j) définie par

$$\mathrm{E}_s(\tau)=\sum_{c\equiv d-1\equiv 0\ [\mathrm{N}]}\frac{1}{(c\tau+d)^j}\Big(\frac{\operatorname{Im}\tau}{|c\tau+d|^2}\Big)^{s+1-k}.$$

Proposition 3.4. — *Sous les hypothèses ci-dessus, on a*

$$\mathrm{D}(f,g,s)=\Big(\sum_{n\in\mathbf{Z}[\frac{1}{\mathrm{N}}]^*}\frac{\overline{a_n}b_n}{n^s}\Big)\cdot\prod_{\ell\nmid\mathrm{N}}\frac{1}{(1-\frac{\overline{\alpha_{\ell,1}}\beta_{\ell,1}}{\ell^s})(1-\frac{\overline{\alpha_{\ell,1}}\beta_{\ell,2}}{\ell^s})(1-\frac{\overline{\alpha_{\ell,2}}\beta_{\ell,1}}{\ell^s})(1-\frac{\overline{\alpha_{\ell,2}}\beta_{\ell,2}}{\ell^s})}.$$

$$\frac{\Gamma(s)}{(4\pi)^s}\mathrm{D}(f,g,s)=\frac{[\mathbf{SL}_2(\mathbf{Z}):\Gamma(\mathrm{N})]}{\mathrm{N}}\langle f,g\mathrm{E}_s\rangle.$$

Démonstration. — La première formule se démontre facteur d'Euler par facteur d'Euler et est un petit exercice de sommation de séries géométriques. Pour démontrer le (ii), on utilise le fait que f et g sont des formes modulaires pour Γ pour écrire $\langle f,g\mathrm{E}_s\rangle$ sous la forme $\frac{1}{[\Gamma:\Gamma(\mathrm{N})]}\langle f,g\mathrm{E}'_s\rangle$, avec (avec $\Gamma_\infty=\big\{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma,\ c=0\big\}$) :

$$\begin{aligned}\mathrm{E}'_s(\tau)&=\Big(\sum_{(e,\mathrm{N})=1}\frac{\overline{\varepsilon}_1\varepsilon_2(e)}{e^{j+2(s-k+1)}}\Big)\cdot\Big(\sum_{\substack{\mathrm{N}|c\\(c,d)=1}}\frac{\overline{\varepsilon}_1\varepsilon_2(d)}{(c\tau+d)^j}\Big(\frac{\operatorname{Im}\tau}{|c\tau+d|^2}\Big)^{s+1-k}\Big)\\&=\mathrm{L}(\overline{\varepsilon}_1\varepsilon_2,j+2(s-k+1))\cdot\sum_{\gamma=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma_\infty\backslash\Gamma}\frac{\overline{\varepsilon}_1\varepsilon_2(d)}{(c\tau+d)^j}\Big(\frac{\operatorname{Im}\tau}{|c\tau+d|^2}\Big)^{s+1-k}.\end{aligned}$$

Par ailleurs, on a

$$\begin{aligned}\frac{\Gamma(s)}{(4\pi)^s}\mathrm{D}(f,g,s)&=\mathrm{L}(\overline{\varepsilon}_1\varepsilon_2,j+2(s-k+1))\cdot\frac{1}{\mathrm{N}}\cdot\int_0^{+\infty}\Big(\int_0^{\mathrm{N}}\overline{f}g\,dx\Big)y^s\frac{dy}{y}\\&=\mathrm{L}(\overline{\varepsilon}_1\varepsilon_2,j+2(s-k+1))\cdot\frac{1}{\mathrm{N}}\cdot\int_{\Gamma_\infty\backslash\mathscr{H}}\overline{f}g\,y^{s+1}\frac{dx\,dy}{y^2}\\&=\mathrm{L}(\overline{\varepsilon}_1\varepsilon_2,j+2(s-k+1))\cdot\frac{1}{\mathrm{N}}\cdot\int_{\Gamma\backslash\mathscr{H}}\sum_{\gamma\in\Gamma\infty\backslash\Gamma}\overline{f}(\gamma\tau)g(\gamma\tau)(\operatorname{Im}\gamma\tau)^{s+1}\frac{dx\,dy}{y^2}\\&=\frac{1}{\mathrm{N}}\cdot\int_{\Gamma\backslash\mathscr{H}}\overline{f}g\,\mathrm{E}'_s\,y^k\frac{dx\,dy}{y^2},\end{aligned}$$

le passage de la seconde à la troisième ligne utilisant l'invariance de la forme volume hyperbolique $\frac{dx\,dy}{y^2}$, et le passage de la troisième à la quatrième utilisant les formules de transformations

$$f\Big(\frac{a\tau+b}{c\tau+d}\Big)=\varepsilon_1(d)(c\tau+d)^k f(\tau),\quad g\Big(\frac{a\tau+b}{c\tau+d}\Big)=\varepsilon_2(d)(c\tau+d)^{k-j}g(\tau)$$
$$\text{et}\quad \mathrm{Im}\Big(\frac{a\tau+b}{c\tau+d}\Big)=\frac{\mathrm{Im}\,\tau}{|c\tau+d|^2},\quad \text{si } \left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma.$$

Corollaire 3.5. — *Sous les hypothèses ci-dessus, il existe une constante* $\mathrm{C}(\mathrm{N})\in\mathbf{Q}^*$ *telle que l'on ait*

$$\frac{\Gamma(k-1)}{(4\pi)^{k-1}}\cdot\frac{\Gamma(j)}{(-2i\pi)^j}\cdot\mathrm{D}(f,g,k-1)=\mathrm{C}(\mathrm{N})\langle f\,,\,g\mathrm{E}^{(j)}_{0,\frac{1}{\mathrm{N}}}\rangle.$$

3.2.2. *Projection d'un produit de deux séries d'Eisenstein.* Si $\chi_1:(\mathbf{Z}/\mathrm{M}_1\mathbf{Z})^*$ est un caractère de Dirichlet modulo M_1 (pas nécessairement primitif), et $\chi_2:(\mathbf{Z}/\mathrm{M}_2\mathbf{Z})^*$ est un caractère de Dirichlet de conducteur M_2, et si $\chi_1\chi_2(-1)=(-1)^{k-j}$, on pose

$$\mathrm{F}^{(k-j)}_{\chi_1,\chi_2}=\frac{1}{2\mathrm{G}(\chi_2)}\sum_{a=1}^{\mathrm{M}_1}\sum_{b=1}^{\mathrm{M}_2}\chi_1(a)\chi_2(b)\,\mathrm{F}^{(k-j)}_{\frac{a}{\mathrm{M}_1},\frac{b}{\mathrm{M}_2}},$$

où $\mathrm{G}(\chi_2)=\sum_{b=1}^{\mathrm{M}_2}\chi_2(b)e^{2i\pi b/\mathrm{M}_2}$ est la somme de Gauss associée à χ_2. Un petit calcul montre que l'on a

$$(\mathrm{F}^{(k-j)}_{\chi_1,\chi_2})_{|_{k-j}}\gamma=\chi_1\chi_2^{-1}(d)\mathrm{F}^{(k-j)}_{\chi_1,\chi_2},\quad \text{si } \gamma=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathbf{SL}_2(\mathbf{Z}),\text{ et } b\equiv 0\ [\mathrm{M}_1],\ c\equiv 0\ [\mathrm{M}_2].$$

D'autre part, en utilisant la proposition 1.3, on peut calculer le q-développement $\sum_{n\in\mathbf{Q}_+}c_nq^n$ de $\mathrm{F}^{(k-j)}_{\chi_1,\chi_2}$, et obtenir la formule

$$\sum_{n\in\mathbf{Q}_+^*}\frac{c_n}{n^s}=\mathrm{M}_1^{s-(k-j)+1}\mathrm{L}(\chi_1,s-(k-j)+1)\cdot\mathrm{L}(\chi_2^{-1},s).$$

Corollaire 3.6. — *Si f est une forme primitive de* $\mathrm{S}_k(\Gamma_0(\mathrm{N}),\varepsilon)$*, et si* M *est un multiple de* N*,* M_1 *et* M_2*, alors*

$$\langle f,\mathrm{F}^{(k-j)}_{\chi_1,\chi_2}\mathrm{E}^{(j)}_{0,\frac{1}{\mathrm{M}}}\rangle=\mathrm{C}(\mathrm{M})^{-1}\cdot\frac{\Gamma(j)}{(-2i\pi)^j}\mathrm{L}(f^*,\chi_1,j)\cdot\chi_2^{-1}(\mathrm{M}_1)\frac{\Gamma(k-1)}{(4\pi)^{k-1}}\mathrm{L}(f^*,\chi_2^{-1},k-1).$$

Démonstration. — Si $f=\sum_{n\in\mathbf{Q}_+}a_nq^n$, on a $a_n=0$ si $n\notin\mathbf{N}$. En prenant en compte cette remarque, la première formule de la prop. 3.4, et le calcul du q-développement de $\mathrm{F}^{(k-j)}_{\chi_1,\chi_2}$ effectué ci-dessus, on obtient

$$\mathrm{D}(f,\mathrm{F}^{(k-j)}_{\chi_1,\chi_2},s)=\chi_2^{-1}(\mathrm{M}_1)\mathrm{L}(f^*,\chi_1,s-(k-j)+1)\cdot\mathrm{L}(f^*,\chi_2^{-1},s),$$

et on conclut en utilisant le corollaire 3.5.

3.3. Projection du système d'Euler de Kato

Soit $\widehat{\Gamma} \subset \mathbf{SL}_2(\widehat{\mathbf{Z}})$ un sous-groupe de congruence ; soit $\widetilde{\Gamma}$ son image inverse dans $\Pi_{\mathbf{Q}}$ et soit $\overline{\Gamma}$ l'intersection de $\widetilde{\Gamma}$ avec $\Pi_{\overline{\mathbf{Q}}}$. On suppose que $\det : \widehat{\Gamma} \to \widehat{\mathbf{Z}}^*$ est surjectif et donc que $\overline{\mathbf{Q}}^{\widetilde{\Gamma}} = \mathbf{Q}$. Si $\phi \in \mathrm{H}^0(\widetilde{\Gamma}, \mathrm{LC}(\mathbf{M}_2(\widehat{\mathbf{Z}}^{(p)}), \mathbf{Z}))$, on définit un élément $\mathbf{z}_\phi(f,j) \in \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}}, \mathscr{D}_0(\widehat{\mathbf{Z}}^{(p)}, \mathrm{V}_f(k-j)))$ de la manière suivante. Soit $\mathbf{z}_{\phi,0}(k,j) \in \mathrm{H}^2(\widetilde{\Gamma}, \mathscr{D}_0(\widehat{\mathbf{Z}}^{(p)}, \mathrm{V}_{k,j}))$ la mesure définie par

$$\int_{\widehat{\mathbf{Z}}^{(p)}} \psi\ \mathbf{z}_{\phi,0}(k,j) = \int_{\mathbf{M}_2(\widehat{\mathbf{Z}})^{(p)}} \psi(\det x)\phi(x)\ \mathbf{z}_{\mathrm{Kato}}(k,j).$$

Soit $\mathbf{z}_{\phi,1}(k,j)$ l'image de $\mathbf{z}_{\phi,0}(k,j)$ dans[80]

$$\mathrm{H}^1(\mathscr{G}_{\mathbf{Q}}, \mathrm{H}^1(\overline{\Gamma}, \mathscr{D}_0(\widehat{\mathbf{Z}}^{(p)}, \mathrm{V}_{k,j}))) \cong \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}}, \mathscr{D}_0(\widehat{\mathbf{Z}}^{(p)}, \mathrm{H}^1(\overline{\Gamma}, \mathrm{V}_{k,j}))),$$

et soit $\mathbf{z}_\phi(f,j)$ la projection de $\mathbf{z}_{\phi,1}(k,j)$ sur une des composantes de $\mathrm{H}^1(\overline{\Gamma}, \mathrm{V}_{k,j})_{\pi_f} \cong \mathrm{V}_f(k-j)^r$, où r est un entier dépendant de $\widehat{\Gamma}$.

On déduit alors de la proposition 1.10 le fait que la famille $c_{\mathrm{M}} = \int_{(1+\mathrm{M}\widehat{\mathbf{Z}})\cap\widehat{\mathbf{Z}}^{(p)}} \mathbf{z}_\phi(f,j)$, $\mathrm{M} \geq 1$ forme un système d'Euler pour $\mathrm{V}_f(k-j)$. D'autre part, en utilisant la loi de réciprocité explicite de Kato (th. 1.9) et le cor. 3.6, on montre que l'on peut choisir ϕ de manière à ce que ce système d'Euler soit non identiquement nul (et même, si $\mathrm{L}(f^*,j) \neq 0$, de telle sorte que c_1 ne soit pas de torsion), ce qui permet de faire marcher la machine des dérivées de Kolyvagin.

4. FONCTIONS L p-ADIQUES DES FORMES MODULAIRES

Dans ce chapitre, on explique comment utiliser la machine de Perrin-Riou (i.e. son application exponentielle [141, 145] construite par interpolation des exponentielles de Bloch-Kato) pour construire la fonction L p-adique attachée à une forme modulaire à partir du système d'Euler de Kato.

La construction de la fonction L p-adique via les symboles modulaires est rappelée au § 4.2. La normalisation adoptée est un peu différente de celle de [121], ce qui permet d'obtenir une distribution sur $\widehat{\mathbf{Z}}$ au lieu d'une famille de distributions sur $(\mathbf{Z}/\mathrm{M}\mathbf{Z}) \times \mathbf{Z}_p$, $\mathrm{M} \geq 1$ premier à p. La description de la machine de Perrin-Riou fait l'objet du § 4.3. Le point de vue adopté est différent de l'approche originale de Perrin-Riou : il utilise la théorie des (φ, Γ)-modules de Fontaine [75, 37]. L'intérêt de cette théorie est de fournir une description explicite (et quasiment gratuite : th. 4.8 et 4.9) du module d'Iwasawa $\mathrm{H}^1(\mathscr{G}_{\mathbf{Q}_p}, \mathscr{D}_0(\mathbf{Z}_p^*, \mathrm{V}))$ associé à une représentation *arbitraire* V de $\mathscr{G}_{\mathbf{Q}_p}$ grâce à une application Exp^*. Si V est cristalline ou semi-stable, on déduit de lois de réciprocités explicites

[80] L'isomorphisme $\mathrm{H}^1(\overline{\Gamma}, \mathscr{D}_0(\widehat{\mathbf{Z}}^{(p)}, \mathrm{V}_{k,j})) \cong \mathscr{D}_0(\widehat{\mathbf{Z}}^{(p)}, \mathrm{H}^1(\overline{\Gamma}, \mathrm{V}_{k,j}))$ provient de ce que $\overline{\Gamma}$ agit trivialement sur $\widehat{\mathbf{Z}}^{(p)}$ et de ce que l'on peut échanger cohomologie et limite projective car on est sous les conditions de Mittag-Leffler, la cohomologie de $\overline{\Gamma}$ dans un module fini étant un groupe fini.

le fait que l'application Exp^* est (à normalisation près) l'inverse de l'application exponentielle de Perrin-Riou. L'inconvénient d'utiliser les (φ, Γ)-modules est que l'on atterrit dans un module $\mathbf{D}^\dagger(\mathrm{V})^{\psi=1}$ qui est un petit peu mystérieux en général, et le gros du travail consiste à analyser la structure de ce module suivant le type de la représentation V. Cette analyse fait l'objet des §§ 4.4-4.6. Dans le cas semi-stable, on en déduit (cf. nº 4.5.1) une formule purement locale pour la dérivée, en un « zéro supplémentaire », d'une fonction L p-adique, ce qui fournit une démonstration[81] (cf. th. 4.16) de la conjecture de Mazur-Tate-Teitelbaum pour la dérivée première de la fonction L p-adique d'une forme modulaire dans le cas d'un zéro supplémentaire.

4.1. **Mesures, distributions et fonctions analytiques**

4.1.1. *Anneaux de séries de Laurent.* Si L est un sous-corps de $\mathbf{C}_p$, on note $\mathscr{R}_{\mathrm{L}}^+$ (resp. $\mathscr{E}_{\mathrm{L}}^+$) l'anneau des fonctions analytiques (resp. analytiques bornées) sur le disque $v_p(\mathrm{T}) > 0$ et $\mathscr{R}_{\mathrm{L}}$ (resp. $\mathscr{E}_{\mathrm{L}}^\dagger$) l'anneau des fonctions analytiques (resp. analytiques bornées) sur la couronne d'épaisseur nulle[82] et de valuation 0. Un élément d'un des anneaux ci-dessus est défini par une série de Laurent $\sum_{k\in\mathbf{Z}} a_k\mathrm{T}^k$, où $a_k \in \mathrm{L}$ quel que soit $k \in \mathbf{Z}$, et on a les équivalences suivantes :

(i) $\sum_{k\in\mathbf{Z}} a_k\mathrm{T}^k \in \mathscr{E}_{\mathrm{L}}^+$ si et seulement si $a_k = 0$ si $k \leq -1$ et si la suite de terme général $v_p(a_k)$ est minorée ;

(ii) $\sum_{k\in\mathbf{Z}} a_k\mathrm{T}^k \in \mathscr{R}_{\mathrm{L}}^+$ si et seulement si $a_k = 0$ si $k \leq -1$ et si $\liminf\limits_{k\to+\infty} \frac{1}{k}v_k(a_k) \geq 0$;

(iii) $\sum_{k\in\mathbf{Z}} a_k\mathrm{T}^k \in \mathscr{E}_{\mathrm{L}}^\dagger$ si et seulement si $\liminf\limits_{k\to-\infty} \frac{1}{|k|}v_p(a_k) > 0$ et si la suite de terme général $v_p(a_k)$ est minorée ;

(iv) $\sum_{k\in\mathbf{Z}} a_k\mathrm{T}^k \in \mathscr{R}_{\mathrm{L}}$ si et seulement si $\liminf\limits_{k\to-\infty} \frac{1}{|k|}v_p(a_k) > 0$ et $\liminf\limits_{k\to+\infty} \frac{1}{k}v_k(a_k) \geq 0$.

On a bien évidemment $\mathscr{E}_{\mathrm{L}}^\dagger \cap \mathscr{R}_{\mathrm{L}}^+ = \mathscr{E}_{\mathrm{L}}^+$.

Si r est un nombre réel, un élément $\sum_{k\in\mathbf{Z}} a_k\mathrm{T}^k$ de $\mathscr{R}_{\mathrm{L}}$ est *d'ordre* r si la suite de terme général $v_p(a_k) + r\log k$, $k \geq 1$, est minorée. On remarquera qu'un élément de $\mathscr{R}_{\mathrm{L}}$ est d'ordre 0 si et seulement s'il appartient à $\mathscr{E}_{\mathrm{L}}^\dagger$, ce qui fournit un moyen de récupérer $\mathscr{E}_{\mathrm{L}}^\dagger$ à l'intérieur de $\mathscr{R}_{\mathrm{L}}$.

Proposition 4.1. — *Si h est un entier supérieur ou égal à la partie entière de r, alors quel que soit $n_0 \in \mathbf{N}$, un élément x de $\mathscr{R}_{\mathrm{L}}$ d'ordre r est entièrement déterminé par son développement de Taylor à l'ordre h en les $\zeta_{p^n} - 1$, pour $n \geq n_0$.*

[81]Cette démonstration est une traduction dans le langage des (φ, Γ)-modules de celle qu'en a donnée, modulo l'existence d'un système d'Euler relié à la fonction L p-adique, Perrin-Riou [146] ; c'est une variante de celle de Kato-Kurihara et Tsuji [104]. (Cf. note 96 pour des compléments.)

[82]Sur une couronne $0 < v_p(\mathrm{T}) \leq r$, où $r > 0$ dépend de l'élément considéré.

4.1.2. *Mesures et distributions sur* $\mathbf{Z}_p$. Si X est un ouvert compact de $\mathbf{Z}_p$, soit $\mathscr{C}^0(\mathrm{X},\mathrm{L})$ l'espace des fonctions continues sur X à valeurs dans L ; on munit cet espace de la norme du sup. qui est bien définie puisque X est compact.

Soit aussi $\mathrm{LA}(\mathrm{X},\mathrm{L})$ l'espace des fonctions localement analytiques sur X à valeurs dans L ; si $f \in \mathrm{LA}(\mathrm{X},\mathrm{L})$ et si $a \in \mathrm{X}$, alors il existe un voisinage de a tel que l'on puisse écrire $f(x)$ sous la forme $f(x) = \sum_{k=0}^{+\infty} c_k(x-a)^k$ dans ce voisinage. L'espace $\mathrm{LA}(\mathrm{X},\mathrm{L})$ est naturellement une limite inductive d'espaces de Banach.

Si V est un L-espace vectoriel topologique, on note $\mathscr{D}_0(\mathrm{X},\mathrm{V})$ l'espace des mesures sur X à valeurs dans V (i.e. l'espace des applications linéaires continues de $\mathscr{C}^0(\mathrm{X},\mathrm{L})$ dans V) ; si $f \in \mathscr{C}^0(\mathrm{X},\mathrm{L})$ et $\mu \in \mathscr{D}_0(\mathrm{X},\mathrm{V})$, on note en général $\int_{\mathrm{X}} f\,\mu$ la valeur de μ sur f. On note aussi $\mathscr{D}(\mathrm{X},\mathrm{V})$ l'espace des distributions sur X à valeurs dans V (i.e. l'espace des applications linéaires continues de $\mathrm{LA}(\mathrm{X},\mathrm{L})$ dans V) ; comme précédemment, si $f \in \mathrm{LA}(\mathrm{X},\mathrm{L})$ et $\mu \in \mathscr{D}(\mathrm{X},\mathrm{V})$, on note en général $\int_{\mathrm{X}} f\,\mu$ la valeur de μ sur f. Une fonction localement analytique étant continue, on a une application naturelle de $\mathscr{D}_0(\mathrm{X},\mathrm{V})$ dans $\mathscr{D}(\mathrm{X},\mathrm{V})$ qui est injective, ce qui permet de considérer une mesure comme une distribution d'un type particulier.

A une distribution μ, on associe sa *transformée d'Amice* $\mathscr{A}_\mu(\mathrm{T})$ qui est une série formelle définie par

$$\mathscr{A}_\mu(\mathrm{T}) = \sum_{n=0}^{+\infty} \Big(\int_{\mathrm{X}} \binom{x}{n}\,\mu \Big) \cdot \mathrm{T}^n = \int_{\mathrm{X}} (1+\mathrm{T})^x\,\mu.$$

La transformée d'Amice fournit une caractérisation particulièrement agréable [2, 3, 56] des distributions sur $\mathbf{Z}_p$ et, en particulier, permet de construire des distributions à partir de séries entières[83].

THÉORÈME 4.2. — *L'application* $\mu \mapsto \mathscr{A}_\mu(\mathrm{T})$ *induit un isomorphisme de* $\mathscr{D}(\mathbf{Z}_p,\mathrm{L})$ *sur* $\mathscr{R}_{\mathrm{L}}^+$ *et de* $\mathscr{D}_0(\mathbf{Z}_p,\mathrm{L})$ *sur* $\mathscr{E}_{\mathrm{L}}^+$.

Une distribution sur X ouvert compact de $\mathbf{Z}_p$ est *d'ordre* r si sa transformée d'Amice est d'ordre r. On note $\mathscr{D}_r(\mathrm{X},\mathrm{V})$ l'espace des distributions d'ordre r sur X à valeurs dans V. En utilisant l'isomorphisme du théorème 4.2, on peut traduire les résultats sur les fonctions analytiques par :

(i) une distribution est d'ordre 0 si et seulement si c'est une mesure (il n'y a donc pas de conflit de notation...) ;

(ii) Si h est un entier supérieur ou égal à la partie entière de r, alors quel que soit $n_0 \in \mathbf{N}$, une distribution d'ordre r est entièrement déterminée par les intégrales $\int_{\mathbf{Z}_p} x^i \zeta_{p^n}^x$, pour $n \geq n_0$ et $0 \leq i \leq h$.

Finalement, on a le résultat suivant [3, 56, 192, 56] qui permet de construire une distribution d'ordre r en connaissant les valeurs des intégrales $\int_{\mathbf{Z}_p} x^i \zeta_{p^n}^x$, pour $n \geq n_0$ et $0 \leq i \leq h$.

[83]Voir [166] pour les distributions sur l'anneau des entiers d'une extension finie de $\mathbf{Q}_p$.

Proposition 4.3. — *Soit $r \in \mathbf{R}$. Si h est un entier supérieur ou égal à la partie entière de r, et si μ est une forme linéaire à valeurs dans* L *sur les fonctions localement polynomiales de degré $\leq h$ telle qu'il existe une constante* C *telle que l'on ait*

$$\Big|\int_{a+p^n\mathbf{Z}_p}(x-a)^h\Big| \leq \mathrm{C}\cdot p^{n(r-h)} \quad \textit{quels que soient } a \in \mathbf{Z}_p \textit{ et } n \in \mathbf{N},$$

alors μ s'étend de manière unique en une distribution d'ordre r sur $\mathbf{Z}_p$.

4.1.3. *Distributions sur $\widehat{\mathbf{Z}}$.* Si X est un ouvert compact de $\widehat{\mathbf{Z}}$, une fonction $f : \mathrm{X} \to \mathrm{L}$ est dite localement analytique si tout point $a = (a_p, a^{]p[}) \in \mathrm{X}$ possède un voisinage sur lequel on peut écrire $f(x)$ sous la forme $f(x) = \sum_{k=0}^{+\infty} c_k(x_p - a_p)^k$. Une fonction localement analytique sur X est donc localement constante par rapport à $x^{]p[}$ et localement analytique par rapport à x_p. On note $\mathrm{LA}(\mathrm{X},\mathrm{L})$ l'espace des fonctions localement analytiques sur X à valeurs dans L et $\mathscr{D}(\mathrm{X},\mathrm{V})$ l'espace des distributions sur X à valeurs dans V. Si $\mathrm{X} = \mathrm{X}_p \times \mathrm{X}^{]p[}$, où X_p (resp. $\mathrm{X}^{]p[}$) est un ouvert compact de $\mathbf{Z}_p$ (resp. de $\widehat{\mathbf{Z}}^{]p[}$), alors écrivant $\mathrm{X}^{]p[}$ comme limite projective d'ensembles finis, on obtient un isomorphisme

$$\mathscr{D}(\mathrm{X},\mathrm{V}) \cong \mathscr{D}_{\mathrm{alg}}(\mathrm{X}^{]p[}, \mathscr{D}(\mathrm{X}_p,\mathrm{V})).$$

Soit $\mathscr{D}_r(\mathrm{X},\mathrm{V}) = \mathscr{D}_{\mathrm{alg}}(\mathrm{X}^{]p[}, \mathscr{D}_r(\mathrm{X}_p,\mathrm{V})) \subset \mathscr{D}(\mathrm{X},\mathrm{V})$ l'ensemble des distributions d'ordre r. De manière équivalente, une distribution μ sur $\widehat{\mathbf{Z}}$ est d'ordre r si et seulement si la distribution $\phi_p \mapsto \int_{\widehat{\mathbf{Z}}} \phi_p(x_p)\phi^{]p[}(x^{]p[})\,\mu$ est une distribution d'ordre r sur $\mathbf{Z}_p$, quelle que soit la fonction localement constante $\phi^{]p[}$ sur $\mathrm{X}^{]p[}$.

4.2. **Formes modulaires et fonctions L p-adiques**

Soit f une forme primitive de poids $k \geq 2$, de caractère ε et de niveau N. Le facteur d'Euler en p de $\mathrm{L}(f,s)$ peut se mettre sous la forme $(1-\alpha p^{-s})(1-\beta p^{-s})$, où α et β sont des entiers algébriques (éventuellement nuls). On suppose dans toute la suite $v_p(\alpha) < k-1$; en particulier $\alpha \neq 0$.

Soit f_α la forme modulaire définie par $f_\alpha(z) = f(z) - \beta f(pz)$. Si $\beta = 0$, on a bien évidemment $f_\alpha = f$, et si $\beta \neq 0$, alors f_α est de niveau Np, propre pour tous les opérateurs de Hecke, de valeur propre α pour l'opérateur T_p de niveau Np (i.e. l'opérateur U_p). Soit $f_\alpha = \sum_{n=1}^{+\infty} a_n q^n$ le q-développement de f_α. On a $a_{np} = \alpha a_n$, si $n \in \mathbf{Z}$, ce qui permet de prolonger l'application $n \mapsto a_n$ à $\mathbf{Z}[\frac{1}{p}]$ en forçant l'équation fonctionnelle $a_{np} = \alpha a_n$ si $n \in \mathbf{Z}[\frac{1}{p}]$.

Si $\phi \in \mathrm{LC}_c(\mathbf{Q}_p \times \widehat{\mathbf{Z}}^{]p[}, \overline{\mathbf{Q}})$, soit $\mathrm{L}(f_\alpha,\phi,s) = \sum_{n\in\mathbf{Z}[\frac{1}{p}]} \phi(n) a_n n^{-s}$. Si $1 \leq j \leq k-1$, on définit $\widetilde{\mathrm{L}}(f_\alpha,\phi,j) \in \overline{\mathbf{Q}}$ comme précédemment.

Si $\phi \in \mathrm{LC}_c(\mathbf{Q}_p, \overline{\mathbf{Q}})$ est constante modulo p^n, on définit sa transformée de Fourier $\hat{\phi} \in \mathrm{LC}_c(\mathbf{Q}_p, \overline{\mathbf{Q}})$ par la formule

$$\hat{\phi}(x) = p^{-m} \sum_{y \bmod p^m} \phi(y) e^{-2i\pi xy},$$

où m est un entier arbitraire $\geq \sup(n, -v_p(x))$, $e^{-2i\pi xy}$ est la racine de l'unité d'ordre une puissance de p obtenue en utilisant l'isomorphisme $\mathbf{Q}_p/\mathbf{Z}_p \cong \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$.

Si $\chi : \mathbf{Z}_p^* \to \overline{\mathbf{Q}}$ est un caractère de Dirichlet de conducteur p^n, on a

$$\hat{\chi}(x) = \begin{cases} \frac{1}{\mathrm{G}(\chi^{-1})}\chi^{-1}(p^n x) & \text{si } n \geq 1, \\ \mathbf{1}_{\mathbf{Z}_p}(x) - \frac{1}{p}\mathbf{1}_{p^{-1}\mathbf{Z}_p}(x) & \text{si } n = 0. \end{cases}$$

Si $\phi_p \in \mathrm{LC}_c(\mathbf{Q}_p, \overline{\mathbf{Q}})$, si $\phi^{]p[} \in \mathrm{LC}(\widehat{\mathbf{Z}}^{]p[}, \overline{\mathbf{Q}})$ et si $\phi \in \mathrm{LC}_c(\mathbf{Q}_p \times \widehat{\mathbf{Z}}^{]p[}, \overline{\mathbf{Q}})$ est donnée par la formule $\phi(x) = \phi_p(x_p) \cdot \phi^{]p[}(x^{]p[})$, on définit sa p-transformée de Fourier $\mathscr{F}_p\phi$ comme l'élément de $\mathrm{LC}_c(\mathbf{Q}_p \times \widehat{\mathbf{Z}}^{]p[}, \overline{\mathbf{Q}})$ donné par la formule

$$\mathscr{F}_p\phi(x) = \hat{\phi}_p(x_p) \cdot \phi^{]p[}(x^{]p[}).$$

On étend $\mathscr{F}_p$ en une application $\overline{\mathbf{Q}}$-linéaire de $\mathrm{LC}_c(\mathbf{Q}_p \times \widehat{\mathbf{Z}}^{]p[}, \overline{\mathbf{Q}})$ dans lui-même.

Théorème 4.4. — *Si $v_p(\alpha) < k-1$, il existe une unique*[84] *distribution $\mu_{f,\alpha}$ d'ordre $v_p(\alpha)$ sur $\widehat{\mathbf{Z}}$, telle que, quel que soit $\phi \in \mathrm{LC}(\widehat{\mathbf{Z}}, \overline{\mathbf{Q}})$ et $1 \leq j \leq k-1$, on ait*

$$\int_{\widehat{\mathbf{Z}}} \phi(x) x_p^{j-1}\ \mu_{f,\alpha} = \widetilde{\mathrm{L}}(f_\alpha, \mathscr{F}_p\phi, j).$$

De plus, quel que soit $\phi \in \mathrm{LA}(\widehat{\mathbf{Z}}, \mathbf{C}_p)$, on a

$$\int_{p\widehat{\mathbf{Z}}} \phi(p^{-1}x_p, px^{]p[})\ \mu_{f,\alpha} = \frac{1}{\alpha}\int_{\widehat{\mathbf{Z}}} \phi(x)\mu_{f,\alpha}.$$

Démonstration. — L'ingrédient principal pour démontrer ce théorème [4, 112, 192, 121] est la théorie des symboles modulaires qui permet de montrer qu'il existe un $\mathscr{O}_{\mathbf{Q}(f)}$-réseau Λ de $\mathbf{Q}(f)\Omega_f^+ + \mathbf{Q}(f)\Omega_f^- \subset \mathbf{C}$ tel que $\int_r^{i\infty} \mathrm{P}(z)f(z)\,dz \in \Lambda$ quels que soient $r \in \mathbf{Q}$ et $\mathrm{P} \in \mathscr{O}_{\mathbf{Q}(f)}[\mathrm{X}]$ de degré $\leq k-2$, ce qui permet d'utiliser la prop. 4.3.

On note $\lambda_{f,\alpha}$ la distribution sur $\widehat{\mathbf{Z}}^{(p)}$ obtenue en multipliant la restriction de $\mu_{f,\alpha}$ à $\widehat{\mathbf{Z}}^{(p)}$ par la fonction x_p^{-1}. On définit la fonction L p-adique de f (associée à α) comme la fonction qui à un caractère[85] χ de $\widehat{\mathbf{Z}}^{(p)}$, localement analytique, associe la valeur

$$\mathrm{L}_{p,\alpha}(f, \chi) = \int_{\widehat{\mathbf{Z}}^{(p)}} \chi(x)\ \lambda_{f,\alpha}.$$

Si χ est un tel caractère, on définit une fonction $\mathrm{L}_{p,\alpha}(f, \chi, s)$ de la variable $s \in \mathbf{Z}_p$, en posant

$$\mathrm{L}_{p,\alpha}(f, \chi, s) = \mathrm{L}_{p,\alpha}(f, \chi \cdot \langle x_p \rangle^s) = \int_{\widehat{\mathbf{Z}}^{(p)}} \chi(x) \cdot \langle x_p \rangle^s\ \lambda_{f,\alpha}.$$

On peut voir un caractère de Dirichlet modulo M comme un caractère de $\widehat{\mathbf{Z}}^{(p)}$ constant modulo $p\mathrm{M}\widehat{\mathbf{Z}}$, et la proposition suivante montre que la fonction L p-adique est obtenue par interpolation des valeurs aux entiers des fonctions L complexes :

[84] Cf. rem 4.12 pour le cas $v_p(\alpha) = k-1$.

[85] $\chi(xy) = \chi(x)\chi(y)$ si $x, y \in \widehat{\mathbf{Z}}^{(p)}$.

Proposition 4.5. — *Si $v_p(\alpha) < k-1$, si χ est un caractère de Dirichlet de conducteur* M *premier à p, si η est un caractère de Dirichlet de conducteur p^m, et si $1 \leq j \leq k-1$, alors*

$$\mathrm{L}_{p,\alpha}(f, \chi\cdot\eta\cdot x_p^j) = \begin{cases} \left(1 - \frac{\chi^{-1}(p)p^{j-1}}{\alpha}\right)\cdot\left(1 - \frac{\beta\chi(p)}{p^j}\right)\cdot \widetilde{\mathrm{L}}(f,\chi,j) & \text{si } m = 0,\\ \frac{\chi^{-1}(p^m)}{\alpha^m}\cdot p^{mj}\cdot \frac{\widetilde{\mathrm{L}}(f,\chi\cdot\eta^{-1},j)}{\mathrm{G}(\eta^{-1})} & \text{si } m \geq 1.\end{cases}$$

4.3. **L'application** Exp*

4.3.1. (φ,Γ)*-modules.* On munit $\mathscr{E}^\dagger_{\mathbf{Q}_p}$ et $\mathscr{R}_{\mathbf{Q}_p}$ d'un frobenius φ et d'une action de $\Gamma = \mathrm{Gal}(\mathbf{Q}_p(\zeta_{p^\infty})/\mathbf{Q}_p)$ via les formules

$$\varphi\Big(\sum_{k\in\mathbf{Z}} a_k\mathrm{T}^k\Big) = \sum_{k\in\mathbf{Z}} a_k((1+\mathrm{T})^p-1)^k \quad \text{et} \quad \gamma\Big(\sum_{k\in\mathbf{Z}} a_k\mathrm{T}^k\Big) = \sum_{k\in\mathbf{Z}} a_k((1+\mathrm{T})^{\chi_{\mathrm{cycl}}(\gamma)}-1)^k.$$

Ces actions commutent entre elles. Si L est une extension finie de $\mathbf{Q}_p$, on étend ces actions à $\mathscr{E}^\dagger_{\mathrm{L}}$ et $\mathscr{R}_{\mathrm{L}}$ par L-linéarité.

Un (φ,Γ)-*module étale* sur $\mathscr{E}^\dagger_{\mathrm{L}}$ est un $\mathscr{E}^\dagger_{\mathrm{L}}$-espace vectoriel D de dimension finie d muni d'actions semi-linéaires de φ et Γ commutant entre elles, l'action de φ étant *étale* (= *de pente* 0), ce qui signifie qu'il existe une base de D sur $\mathscr{E}^\dagger_{\mathrm{L}}$ telle que les matrices de φ et φ^{-1} dans cette base soient à coefficients dans l'anneau des entiers de $\mathscr{E}^\dagger_{\mathrm{L}}$ (pour la valuation $v_p(\sum a_k\mathrm{T}^k) = \inf v_p(a_k)$).

Théorème 4.6 ([75, 37, 55]). — *On dispose d'un foncteur naturel*[86] $\mathrm{V} \mapsto \mathbf{D}^\dagger(\mathrm{V})$ *qui induit une équivalence de catégories de la catégorie des* L*-représentations de dimension finie de $\mathscr{G}_{\mathbf{Q}_p}$ sur celle des (φ,Γ)-modules étales sur $\mathscr{E}^\dagger_{\mathrm{L}}$.*

La théorie des (φ,Γ)-modules ayant déjà fait l'objet d'un demi-exposé à ce séminaire [55], nous ne nous étendrons pas sur la démonstration de ce théorème. On pourra consulter

[86]Notons $\widetilde{\mathbf{E}}$ le corps des fractions de $\widetilde{\mathbf{E}}^+ = \mathbb{R}(\overline{\mathbf{Q}}_p)$ (cf. n° 2.1.1) et $\widetilde{\mathbf{A}} = \mathrm{W}(\widetilde{\mathbf{E}})$ l'anneau des vecteurs de Witt à coefficients dans $\widetilde{\mathbf{E}}$. Il est naturellement muni d'actions de $\mathscr{G}_{\mathbf{Q}_p}$ et φ commutant entre elles et on dispose d'un plongement de l'anneau des entiers de $\mathscr{E}^\dagger_{\mathbf{Q}_p}$ dans $\widetilde{\mathbf{A}}$ commutant aux actions de $\mathscr{G}_{\mathbf{Q}_p}$ et φ, à savoir celui envoyant T sur $\pi = \tilde{\zeta} - 1$. L'adhérence $\mathbf{A}_{\mathbf{Q}_p}$ de son image dans $\widetilde{\mathbf{A}}$ est l'ensemble des séries de Laurent $\sum_{k\in\mathbf{Z}} a_k\pi^k$ avec $a_k \in \mathbf{Z}_p$ et $\lim_{k\to-\infty} v_p(a_k) = +\infty$. On note $\mathbf{A}$ l'adhérence pour la topologie p-adique de l'anneau des entiers de l'extension maximale non ramifiée de $\mathbf{B}_{\mathbf{Q}_p} = \mathbf{A}_{\mathbf{Q}_p}[\frac{1}{p}]$ dans $\widetilde{\mathbf{B}} = \widetilde{\mathbf{A}}[\frac{1}{p}]$, et on pose $\mathbf{B} = \mathbf{A}[\frac{1}{p}]$. On définit le sous-corps $\widetilde{\mathbf{B}}^\dagger$ des éléments surconvergents de $\widetilde{\mathbf{B}}$ comme l'ensemble des éléments $x = \sum_{k\gg-\infty} p^k[x_k]$, où $(x_k)_{k\gg-\infty}$ est une suite d'éléments de $\widetilde{\mathbf{E}}$ vérifiant $\liminf_{k\to+\infty} \frac{1}{p}v_{\mathbf{E}}(x_k) > -\infty$, et on pose $\mathbf{B}^\dagger = \mathbf{B}\cap\widetilde{\mathbf{B}}^\dagger$; c'est un sous-corps de $\widetilde{\mathbf{B}}$ stable par φ et $\mathscr{G}_{\mathbf{Q}_p}$ et on a $\mathscr{E}^\dagger_{\mathbf{Q}_p} = (\mathbf{B}^\dagger)^{\mathscr{H}}$, si $\mathscr{H} = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p(\zeta_{p^\infty}))$, et $(\mathbf{B}^\dagger)^{\varphi=1} = \mathbf{Q}_p$. Ceci nous permet de définir un foncteur $\mathbf{D}^\dagger$ qui à une $\mathbf{Q}_p$-représentation V de $\mathscr{G}_{\mathbf{Q}_p}$ associe le (φ,Γ)-module étale $\mathbf{D}^\dagger(\mathrm{V}) = (\mathbf{B}^\dagger\otimes_{\mathbf{Q}_p}\mathrm{V})^{\mathscr{H}}$ et le foncteur $\mathbf{V}^\dagger$ qui à un (φ,Γ)-module D étale sur $\mathscr{E}^\dagger_{\mathbf{Q}_p}$ associe le $\mathbf{Q}_p$-espace vectoriel $\mathbf{V}^\dagger(\mathrm{D}) = (\mathbf{B}^\dagger\otimes_{\mathbf{B}^\dagger_{\mathbf{Q}_p}}\mathrm{D})^{\varphi=1}$. Ces deux foncteurs sont inverses l'un de l'autre et fournissent une description de l'équivalence de catégories du théorème. (On n'a traité dans cette note que le cas des $\mathbf{Q}_p$-représentations, mais si on est parti d'une L-représentation, tous les objets considérés sont des L-espaces vectoriels.)

la note 86 pour une description du foncteur $\mathbf{D}^\dagger$; celui-ci fait intervenir l'anneau $\mathbf{B}^\dagger$ de Fontaine qui n'est pas franchement facile à appréhender...

Remarque 4.7. — On étend l'action de φ et Γ sur $\mathscr{R}_{\mathrm{L}}$ à $\mathscr{R}_{\mathrm{L}}[\log \mathrm{T}]$ par les formules

$$\varphi(\log \mathrm{T}) = \log \varphi(\mathrm{T}) = p \log \mathrm{T} + \log \frac{\varphi(\mathrm{T})}{\mathrm{T}^p} \quad \text{et} \quad \gamma(\log \mathrm{T}) = \log \gamma(\mathrm{T}) = \log \mathrm{T} + \log \frac{\gamma(\mathrm{T})}{\mathrm{T}},$$

ces formules ayant un sens car la série définissant $\log \frac{\varphi(\mathrm{T})}{\mathrm{T}^p}$ converge dans $\mathscr{E}_{\mathrm{L}}^\dagger$ et celle définissant $\log \frac{\gamma(\mathrm{T})}{\mathrm{T}}$ dans $\mathscr{R}_{\mathrm{L}}^+$ vers un élément d'ordre 1. On munit aussi $\mathscr{R}_{\mathrm{L}}[\log \mathrm{T}]$ de l'unique $\mathscr{R}_{\mathrm{L}}$-dérivation N telle que $\mathrm{N}(\log \mathrm{T}) = -\frac{p}{p-1}$.

Grâce aux travaux de Berger [12, 55], on sait décrire $\mathbf{D}_{\mathrm{cris}}(\mathrm{V})$ et $\mathbf{D}_{\mathrm{st}}(\mathrm{V})$ en termes de $\mathbf{D}^\dagger(\mathrm{V})$, tous ces modules vivant à l'intérieur de $\mathscr{R}_{\mathrm{L}}[\log \mathrm{T}, \frac{1}{t}] \otimes_{\mathscr{E}_{\mathrm{L}}^\dagger} \mathbf{D}^\dagger(\mathrm{V})$, avec $t = \log(1+\mathrm{T})$, et on peut en tirer une « description » (pas très explicite, mais suffisante pour ce que l'on veut en faire dans ce texte (prop. 4.10 et 4.14)) de $\mathbf{D}^\dagger(\mathrm{V})$ en termes de $\mathbf{D}_{\mathrm{cris}}(\mathrm{V})$, si V est cristalline, et de $\mathbf{D}_{\mathrm{st}}(\mathrm{V})$, si V est semi-stable.

4.3.2. *(φ, Γ)-modules et théorie d'Iwasawa.* Si D est un (φ, Γ)-module étale sur $\mathscr{E}_{\mathrm{L}}^\dagger$, tout élément x de D peut s'écrire de manière unique sous la forme $\sum_{i=0}^{p-1}(1+\mathrm{T})^i \varphi(x_i)$, ce qui permet de définir un inverse à gauche ψ de φ par la formule $\psi(x) = x_0$; ce morphisme commute à l'action de Γ et joue un rôle très important [88, 36, 53] pour le calcul de la cohomologie galoisienne ou la théorie d'Iwasawa des L-représentations de $\mathscr{G}_{\mathbf{Q}_p}$.

Théorème 4.8. — *Si* V *est une* L*-représentation de* $\mathscr{G}_{\mathbf{Q}_p}$*, on dispose d'un isomorphisme naturel*[87]

$$\mathrm{Exp}^* : \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}_p}, \mathscr{D}_0(\mathbf{Z}_p^*, \mathrm{V})) \longrightarrow \mathbf{D}^\dagger(\mathrm{V})^{\psi=1}.$$

L'application Exp^* doit son nom au résultat suivant qui se déduit assez facilement [36] de la formule explicite donnée dans la note 87.

Théorème 4.9. — *Si* V *est une* L*-représentation de de Rham de* $\mathscr{G}_{\mathbf{Q}_p}$*, si* $n \in \mathbf{N}$ *est assez grand, et si* $\mu \in \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}_p}, \mathscr{D}_0(\mathbf{Z}_p^*, \mathrm{V}))$*, alors* $\varphi^{-n}(\mathrm{Exp}^*(\mu))$ *converge*[88] *dans* $\mathbf{B}_{\mathrm{dR}}^+ \otimes \mathrm{V}$*, et*

---

[87] Cet isomorphisme est dû à Fontaine (non publié) et repose sur les travaux de Herr [88]. Il est parfaitement explicite et utilise l'application $x \mapsto (1-\varphi)x$ qui donne naissance à la suite exacte $0 \to \mathbf{Q}_p \to \mathbf{B}^\dagger \to \mathbf{B}^\dagger \to 0$. L'autre ingrédient de la construction est le fait que, si γ_n est un générateur de $\mathrm{Gal}(\mathbf{Q}_p(\zeta_{p^\infty})/\mathbf{Q}_p(\zeta_{p^n}))$, alors $1-\gamma_n$ agissant sur $\mathbf{D}^\dagger(\mathrm{V})^{\psi=0}$ est un isomorphisme (c'est le point délicat de la théorie). Muni de ces deux ingrédients, on peut décrire l'inverse de Exp^* comme suit : si $x \in \mathbf{D}^\dagger(\mathrm{V})^{\psi=1}$, alors $(1-\varphi)x \in \mathbf{D}^\dagger(\mathrm{V})^{\psi=0}$ et il existe $x_n \in \mathbf{D}^\dagger(\mathrm{V})^{\psi=0}$ vérifiant $(1-\gamma_n)x_n = (1-\varphi)x$. Si $b_n \in \mathbf{B}^\dagger \otimes_{\mathbf{Q}_p} \mathrm{V}$ est une solution de l'équation $(1-\varphi)b_n = x_n$, alors le cocycle $\sigma \mapsto \log \chi_{\mathrm{cycl}}(\gamma_n)(\frac{\sigma-1}{\gamma_n-1}x + (\sigma-1)b_n)$ (sur $\mathscr{G}_{\mathbf{Q}_p(\zeta_{p^n})}$) est à valeurs dans V (car tué par $1-\varphi$) et sa classe dans $\mathrm{H}^1(\mathscr{G}_{\mathbf{Q}_p(\zeta_{p^n})}, \mathrm{V})$ est l'image de $(\mathrm{Exp}^*)^{-1}x \in \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}_p}, \mathscr{D}_0(\mathbf{Z}_p^*, \mathrm{V}))$ par l'application $\mu \mapsto \int_{1+p^n\mathbf{Z}_p} \mu$.

[88] $\mathbf{B}_{\mathrm{dR}}^+$ et $\mathbf{B}$ sont construits à partir de $\mathrm{W}(\widetilde{\mathbf{E}}^+)$ en localisant et en complétant, mais pour des topologies trop différentes pour que l'on puisse plonger $\mathbf{B}^\dagger$ dans $\mathbf{B}_{\mathrm{dR}}^+$; par contre, $\mathbf{B}^\dagger$ est exactement le sous-ensemble de $\mathbf{B}$ des éléments $x = \sum_{k \geq k(x)} p^k [x_k]$ tels que la série $\sum_{k \geq k(x)} p^k [x_k^{p^{-n}}] = \varphi^{-n}(x)$ converge dans $\mathbf{B}_{\mathrm{dR}}^+$ si n est assez grand. Par ailleurs, on a $\int_{1+p^n\mathbf{Z}_p} x^{-k}\mu \in \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}_p(\zeta_{p^n})}, \mathrm{V}(-k))$ et $\exp^*(\int_{1+p^n\mathbf{Z}_p} x^{-k}\mu) \in t^k \mathrm{L}(\zeta_{p^n}) \mathbf{D}_{\mathrm{dR}}^{-k}(\mathrm{V})$ est nul si $k \ll 0$.

on a

$$p^{-n}\varphi^{-n}(\mathrm{Exp}^*(\mu)) = \sum_{k\in\mathbf{Z}} \exp^*\Big(\int_{1+p^n\mathbf{Z}_p} x^{-k}\mu\Big) \in \mathrm{L}(\zeta_{p^n})[[t]] \otimes_{\mathrm{L}} \mathbf{D}_{\mathrm{dR}}(\mathrm{V}).$$

Pour pouvoir utiliser l'application Exp^* pour construire les fonctions L p-adiques attachées aux formes modulaires, nous allons avoir besoin d'analyser plus en détail la structure de $\mathbf{D}^\dagger(\mathrm{V}_f)^{\psi=1}$, si f est une forme primitive de poids $k \geq 2$. On est amené à distinguer les cas où la représentation V_f est cristalline, semi-stable ou seulement potentiellement semi-stable.

4.4. Le cas cristallin

Soit f une forme primitive de poids $k \geq 2$ et niveau N premier à p. La représentation V_f est alors cristalline et, si on factorise le facteur d'Euler en p de la fonction $\mathrm{L}(f,s)$ sous la forme $(1-\alpha p^{-s})(1-\beta p^{-s})$, alors α et β sont les valeurs propres de φ sur $\mathbf{D}_{\mathrm{cris}}(\mathrm{V}_f)$. Pour nous simplifier la vie, nous allons supposer[89] $\alpha \neq \beta$ et utiliser le fait que ni α ni β ne peuvent être égaux[90] à 1 ou p^{k-1}. Soit $\mathrm{L} = \mathbf{Q}_p(f,\alpha)$, et considérons V_f comme une L-représentation de dimension 2 de $\mathscr{G}_{\mathbf{Q}_p}$. Comme les poids de Hodge-Tate de V_f sont $1-k$ et 0, le φ-module filtré $\mathrm{D} = \mathbf{D}_{\mathrm{cris}}(\mathrm{V}_f)$ est un L-espace vectoriel de dimension 2 muni d'une action L-linéaire de φ et d'une filtration $(\mathrm{D}^i)_{i\in\mathbf{Z}}$ vérifiant $\mathrm{D}^i = \mathrm{D}$ si $i \leq 0$, $\mathrm{D}^i = \mathrm{D}^{k-1}$ si $0 < i \leq k-1$, et $\mathrm{D}^i = 0$ si $i > k-1$ (en particulier, cette filtration est complètement déterminée par la donnée de la L-droite D^{k-1} dont f est naturellement une base) ; il est isomorphe à l'un des modules $\mathrm{D}_{\alpha,\beta}$ ou $\mathrm{D}_\alpha \oplus \mathrm{D}_\beta$ ci-dessous[91].

- si $\alpha,\beta \in \mathrm{L}$ vérifient $v_p(\alpha) \geq v_p(\beta) \geq 0$ et $v_p(\alpha)+v_p(\beta) = k-1$, on note $\mathrm{D}_{\alpha,\beta}$ le φ-module filtré défini par $\mathrm{D}_{\alpha,\beta} = \mathrm{L}\cdot e_\alpha \oplus \mathrm{L}\cdot e_\beta$, avec $\varphi(e_\alpha) = \alpha e_\alpha$, $\varphi(e_\beta) = \beta e_\beta$, et $\mathrm{D}^{k-1}_{\alpha,\beta} = \mathrm{L}\cdot(e_\alpha + e_\beta)$;
- si $\alpha,\beta \in \mathrm{L}$ vérifient $v_p(\alpha) = k-1$ et $v_p(\beta) = 0$, on note $\mathrm{D}_\alpha \oplus \mathrm{D}_\beta$ le φ-module filtré défini par $\mathrm{D}_\alpha \oplus \mathrm{D}_\beta = \mathrm{L}\cdot e_\alpha \oplus \mathrm{L}\cdot e_\beta$, avec $\varphi(e_\alpha) = \alpha e_\alpha$, $\varphi(e_\beta) = \beta e_\beta$, et $(\mathrm{D}_\alpha \oplus \mathrm{D}_\beta)^{k-1} = \mathrm{L}\cdot e_\alpha$.

Les modules $\mathrm{D}_{\alpha,\beta}$ et $\mathrm{D}_\alpha \oplus \mathrm{D}_\beta$ sont faiblement admissibles et donc [59], les représentations $\mathbf{V}_{\mathrm{cris}}(\mathrm{D}_\alpha \oplus \mathrm{D}_\beta)$ et $\mathbf{V}_{\mathrm{cris}}(\mathrm{D}_{\alpha,\beta})$ sont des L-représentations cristallines de $\mathscr{G}_{\mathbf{Q}_p}$ de dimension 2 dont les poids de Hodge-Tate sont $1-k$ et 0. On pose

$$\mathrm{D}^\dagger_{\alpha,\beta} = \mathbf{D}^\dagger(\mathbf{V}_{\mathrm{cris}}(\mathrm{D}_{\alpha,\beta})) \quad \text{et} \quad \mathrm{D}^\dagger_\alpha \oplus \mathrm{D}^\dagger_\beta = \mathbf{D}^\dagger(\mathbf{V}_{\mathrm{cris}}(\mathrm{D}_\alpha \oplus \mathrm{D}_\beta)).$$

Proposition 4.10. — (i) *Si $\alpha,\beta \in \mathrm{L}$ vérifient $v_p(\alpha) \geq v_p(\beta) \geq 0$ et $v_p(\alpha)+v_p(\beta) = k-1$, alors $w = w_\alpha \cdot t^{1-k} e_\alpha + w_\beta \cdot t^{1-k} e_\beta \in \mathscr{R}_{\mathrm{L}}[\frac{1}{t}] \otimes_{\mathrm{L}} \mathrm{D}_{\alpha,\beta}$ appartient à $(\mathrm{D}^\dagger_{\alpha,\beta})^{\psi=1}$ si et seulement si il existe des distributions μ_α et μ_β sur $\mathbf{Z}_p$, à valeurs dans* L, *vérifiant*

[89] On conjecture que c'est toujours le cas : semi-simplicité du frobenius cristallin plus admissibilité de $\mathbf{D}_{\mathrm{cris}}(\mathrm{V}_f)$.

[90] On a $|\alpha| = |\beta| = p^{(k-1)/2}$ d'après Deligne.

[91] Le cas $\mathrm{D}_\alpha \oplus \mathrm{D}_\beta$ correspond au cas où la représentation V_f est scindée ; il semble raisonnable de penser que cela ne peut se produire que si f est de type CM ; Ghate et Vatsal [81] ont démontré que, si on fixe le niveau et qu'on laise le poids varier, il ne peut y avoir qu'un nombre fini de contre-exemples.

(a) μ_α *est d'ordre* $k-1-v_p(\alpha)$ *et* μ_β *est d'ordre* $k-1-v_p(\beta)$,

(b)[92] $\psi(\mu_\alpha)=p^{1-k}\alpha\cdot\mu_\alpha$ *et* $\psi(\mu_\beta)=p^{1-k}\beta\cdot\mu_\beta$,

(c) $\alpha^{-n}\int_{\mathbf{Z}_p}x^i\zeta_{p^n}^x\mu_\alpha=\beta^{-n}\int_{\mathbf{Z}_p}x^i\zeta_{p^n}^x\mu_\beta$ *quels que soient* $n\geq 1$ *et* $0\leq i\leq k-2$,

telles que l'on ait $w_\alpha=\int_{\mathbf{Z}_p}(1+\mathrm{T})^x\,\mu_\alpha$ *et* $w_\beta=\int_{\mathbf{Z}_p}(1+\mathrm{T})^x\,\mu_\beta$.

(ii) *Si* $\alpha,\beta\in\mathrm{L}$ *vérifient* $v_p(\alpha)=k-1$, $\alpha\neq p^{k-1}$ *et* $v_p(\beta)=0$, $\beta\neq 1$, *alors* $w\in(\mathrm{D}_\alpha^\dagger\oplus\mathrm{D}_\beta^\dagger)^{\psi=1}$ *si et seulement si il existe des mesures* μ_α *et* μ_β *sur* $\mathbf{Z}_p$, *à valeurs dans* L, *vérifiant* $\psi(\mu_\alpha)=p^{1-k}\alpha\cdot\mu_\alpha$ *et* $\psi(\mu_\beta)=\beta\cdot\mu_\beta$ *telles que l'on ait*

$$w=\int_{\mathbf{Z}_p}(1+\mathrm{T})^x\,\mu_\alpha\cdot t^{1-k}e_\alpha+\int_{\mathbf{Z}_p}(1+\mathrm{T})^x\,\mu_\beta\cdot e_\beta.$$

Démonstration. — Le (ii) se démontre comme le (i), mais est plus simple donc nous n'allons considérer que le (i). La condition (b) est une traduction de l'égalité $\psi(w)=w$; la condition (c) se traduit en terme du développement limité de $\varphi^{-n}(w)$ à l'ordre $k-2$ et permet de montrer que $w\in\mathscr{R}_\mathrm{L}\otimes_{\mathscr{E}_\mathrm{L}^\dagger}\mathrm{D}^\dagger$, et la condition (a) implique que w est « d'ordre 0 », ce qui permet de montrer que $w\in\mathrm{D}^\dagger$. Dans l'autre sens, l'existence de distributions vient de ce qu'une solution dans $\mathscr{R}_\mathrm{L}$ d'une équation du type $\psi(x)-\alpha x\in\mathscr{R}_\mathrm{L}^+$, où $\alpha\in\mathrm{L}$ vérifie $v_p(\alpha)\leq 0$, appartient à $\mathscr{R}_\mathrm{L}^+$ (resp. $\mathscr{R}_\mathrm{L}^+\oplus\mathrm{L}\cdot\frac{1}{\mathrm{T}}$) si $\alpha\neq 1$ (resp. si $\alpha=1$), et donc est la transformée d'Amice d'une distribution.

Soit π_α (resp. π_β) la projection sur $\mathrm{L}\cdot e_\alpha$ (resp. $\mathrm{L}\cdot e_\beta$) parallèlement à $\mathrm{L}\cdot e_\beta$ (resp. $\mathrm{L}\cdot e_\alpha$). Il ressort de ce qui précède que, si $z\in\mathrm{H}^1(\mathscr{G}_{\mathbf{Q}_p},\mathscr{D}_0(\mathbf{Z}_p^*,\mathrm{V}_f))$, alors $\pi_\alpha(\mathrm{Exp}^*(z))=w_\alpha\cdot t^{1-k}e_\alpha$, où w_α est la transformée d'Amice d'un élément de $\mathscr{D}_{k-1-v_p(\alpha)}(\mathbf{Z}_p,\mathrm{L})$. Les mêmes arguments montrent que, si $z\in\mathrm{H}^1(\mathscr{G}_{\mathbf{Q}_p},\mathscr{D}_0(\widehat{\mathbf{Z}}^{(p)},\mathrm{V}_f))$, alors $\pi_\alpha(\mathrm{Exp}^*(z))=w_\alpha\cdot t^{1-k}e_\alpha$, où w_α est la transformée d'Amice d'un élément de $\mathscr{D}_{k-1-v_p(\alpha)}(\widehat{\mathbf{Z}},\mathrm{L})$.

Théorème 4.11. — *Si* $v_p(\alpha)>0$, *alors* $\pi_\alpha(f)\neq 0$ *et, si* $\partial=(1+\mathrm{T})\frac{d}{d\mathrm{T}}$,

$$\partial\big(\pi_\alpha(\mathrm{Exp}^*(\mathbf{z}_{\mathrm{Kato}}(f)))\big)=\Big(\int_{\mathbf{Z}_p}(1+\mathrm{T})^x\ \mu_{f^*,p^{k-1}\alpha^{-1}}\Big)\cdot t^{1-k}\pi_\alpha(f).$$

Démonstration. — C'est une conséquence de la caractérisation (th. 3.1) de $\mathbf{z}_{\mathrm{Kato}}(f)$, de la définition (th. 4.4) de la mesure $\mu_{f^*,p^{k-1}\alpha^{-1}}$ et de la loi de réciprocité explicite du th. 4.9.

Remarque 4.12. — On peut aussi projeter $\mathrm{Exp}^*(\mathbf{z}_{\mathrm{Kato}}(f))$ sur la droite propre pour la valeur propre β. Si $v_p(\beta)>0$, le résulat précédent reste valable. Si $v_p(\beta)=0$ et la représentation V_f de $\mathscr{G}_{\mathbf{Q}_p}$ n'est pas une somme directe de deux sous-représentations, alors $\pi_\beta(f)\neq 0$, et on récupère une distribution d'ordre $k-1$ qui permet de définir une fonction L p-adique. Les valeurs de cette fonction L p-adique aux caractères critiques (i.e. les $\mathrm{L}_{p,\beta}(f,\eta\cdot x_p^j)$, pour η d'ordre fini et $j\in\{1,\dots,k-1\}$) sont reliées aux valeurs de la fonction L complexe comme pour α, mais ces valeurs ne suffisent pas à déterminer complètement la

[92] On définit $\psi(\mu)$, si μ est une distribution à valeurs dans L, en passant par les transformées d'Amice, par la formule $\mathscr{A}_{\psi(\mu)}=\psi(\mathscr{A}_\mu)$. On a alors $\int_{\mathbf{Z}_p}\phi(x)\,\psi(\mu)=\int_{p\mathbf{Z}_p}\phi(\frac{x}{p})\,\mu$ quelle que soit la fonction localement analytique ϕ.

fonction L p-adique ; il manque les valeurs pour un entier j quelconque n'appartenant pas à $\{1,\dots,k-1\}$. Une voie d'approche pour restaurer une unicité est d'utiliser le fait que la machine de Perrin-Riou fournit des renseignements en tous les caractères algébriques pour une fonction L p-adique fabriquée à partir d'un système d'Euler[93] ; on obtient en particulier, si $j=0$, une expression pour $\mathrm{L}_{p,\beta}(f,\eta\cdot x_p^j)$ en termes du régulateur [22, 23] des éléments de Beilinson [8] ou de Scholl [162] (cf. [80] et [146]). Une autre approche est fournie par les symboles modulaires « en famille » (cf. [150]). Le cas d'une forme modulaire de type CM est un peu étrange : comme $\pi_\beta(f)=0$, la fonction L que l'on construit[94] s'annule en tous les caractères critiques et il n'y a aucune raison pour qu'elle soit identiquement nulle !

4.5. **Le cas semi-stable**

Supposons maintenant que le niveau de f est divisible par p, mais que $a_p\neq 0$. La représentation V_f est alors semi-stable, et le (φ,N)-module filtré $\mathrm{D}=\mathbf{D}_{\mathrm{st}}(\mathrm{V}_f)$ est un L-espace vectoriel de dimension 2 muni d'actions L-linéaires de φ et N vérifiant la relation $\mathrm{N}\varphi=p\varphi\mathrm{N}$ et d'une filtration $(\mathrm{D}^i)_{i\in\mathbf{Z}}$ entièrement déterminée par la donnée de la L-droite D^{k-1} ; il est isomorphe à un des modules $\mathrm{D}_{\alpha,\mathscr{L}}$ ci-dessous (avec $\alpha=pa_p$ et $\mathscr{L}=\mathscr{L}_f$ invariant de Fontaine).

Si $\alpha\in\mathrm{L}$ vérifie $2v_p(\alpha)-1=k-1$ et $\mathscr{L}\in\mathrm{L}$, on note $\mathrm{D}_{\alpha,\mathscr{L}}$ le (φ,N)-module filtré défini par $\mathrm{D}_{\alpha,\mathscr{L}}=\mathrm{L}\cdot e_\alpha\oplus\mathrm{L}\cdot\mathrm{N}e_\alpha$, avec $\varphi(e_\alpha)=\alpha e_\alpha$ et $\mathrm{D}^{k-1}_{\alpha,\mathscr{L}}=\mathrm{L}\cdot(e_\alpha+\mathscr{L}\cdot\mathrm{N}e_\alpha)$. (La relation $\mathrm{N}\varphi=p\varphi\mathrm{N}$ entraîne que l'on a de plus $\varphi(\mathrm{N}e_\alpha)=p^{-1}\alpha\cdot\mathrm{N}e_\alpha$ et $\mathrm{N}(\mathrm{N}e_\alpha)=0$.)

Le (φ,N)-module filtré $\mathrm{D}_{\alpha,\mathscr{L}}$ est admissible et $\mathbf{V}_{\mathrm{st}}(\mathrm{D}_{\alpha,\mathscr{L}})$ est une L-représentation semi-stable de $\mathscr{G}_{\mathbf{Q}_p}$ de dimension 2 dont les poids de Hodge-Tate sont $1-k$ et 0. Posons $\mathrm{D}^\dagger_{\alpha,\mathscr{L}}=\mathbf{D}^\dagger(\mathbf{V}_{\mathrm{st}}(\mathrm{D}_{\alpha,\mathscr{L}}))$. Pour décrire $(\mathrm{D}^\dagger_{\alpha,\mathscr{L}})^{\psi=1}$ à l'intérieur de $\mathscr{R}_\mathrm{L}[\log\mathrm{T},\frac{1}{t}]\otimes_\mathrm{L}\mathrm{D}_{\alpha,\mathscr{L}}$, nous aurons besoin du lemme suivant.

Lemme 4.13. — Si $\alpha\in\mathrm{L}$, il existe $\ell_\alpha\in\mathscr{R}_\mathrm{L}[\log\mathrm{T}]$ (non unique) vérifiant les conditions suivantes :

$$(1-\alpha\varphi)\cdot\mathrm{N}(\ell_\alpha)=-\begin{cases}1+\mathrm{T} & \text{si } \alpha\notin p^{-\mathbf{N}},\\ 1+\mathrm{T}-p^i\frac{t^i}{i!} & \text{si } \alpha=p^{-i},\end{cases}$$

$$\text{et}\quad(\psi-p^{-1}\alpha)\cdot\ell_\alpha=\begin{cases}0 & \text{si } \alpha\notin p^{-\mathbf{N}},\\ -\frac{(p-1)\log\mathrm{T}}{p^2}\cdot\frac{t^i}{i!} & \text{si } \alpha=p^{-i}.\end{cases}$$

Démonstration. — On commence par construire $\ell_\alpha^{(0)}=-\mathrm{N}(\ell_\alpha)$. Si $v_p(\alpha)>-1$, on prend $\ell_\alpha^{(0)}$ de la forme $c_\alpha+\sum_{n=0}^{+\infty}\alpha^n\varphi^n(\mathrm{T})$, et on ajuste la constante c_α pour que ça marche. On

[93] Par construction pour les entiers $\gg 0$, et grâce à la loi de réciprocité explicite [51, 103, 11] pour les autres.

[94] On a quand même le problème, pour normaliser cette fonction, de choisir une base de l'espace propre pour β, le choix évident $\pi_\beta(f)$ ne marchant pas.

passe de α à $p^{-1}\alpha$ par la formule $\partial\ell_{\alpha/p}^{(0)} = \ell_\alpha^{(0)}$, en ajustant la constante d'intégration. On définit alors ℓ_α par la formule

$$\ell_\alpha = \frac{p-1}{p}\Big(\ell_\alpha^{(0)}\frac{\log\varphi(\mathrm{T})}{p} - \sum_{n=0}^{+\infty}(p\alpha^{-1})^n\psi^n\Big(p^{-1}\ell_\alpha^{(0)}\log\frac{\varphi(\mathrm{T})}{\mathrm{T}^p}\Big)\Big).$$

Proposition 4.14. — *$w = t^{1-k}\big(w_\alpha\cdot e_\alpha + w_{\alpha/p}\cdot \mathrm{N}e_\alpha\big) \in \mathscr{R}_{\mathrm{L}}[\log\mathrm{T},\frac{1}{t}]\otimes_{\mathrm{L}}\mathrm{D}_{\alpha,\mathscr{L}}$ appartient à $(\mathrm{D}^\dagger_{\alpha,\mathscr{L}})^{\psi=1}$ si et seulement si*

(i) *$w_{\alpha/p}(\zeta_{p^n}e^{t/p^n}-1) \equiv p^{-n}\mathscr{L}w_\alpha(\zeta_{p^n}e^{t/p^n}-1) \bmod t^{k-1}\mathrm{L}(\zeta_{p^n})[[t]]$, pour n assez grand;*

(ii) *il existe[95] des distributions μ_α et $\mu_{\alpha/p}$ sur $\mathbf{Z}_p$, à valeurs dans* L, *vérifiant*

  (a) *μ_α est d'ordre $k-1-v_p(\alpha)$ et $\mu_{\alpha/p}$ est d'ordre $k-v_p(\alpha)$,*

  (b) *$\psi(\mu_\alpha) = p^{1-k}\alpha\cdot\mu_\alpha$ et $\psi(\mu_{\alpha/p}) = p^{-k}\alpha\cdot\mu_{\alpha/p}$,*

telles que l'on ait $w_\alpha = \int_{\mathbf{Z}_p}(1+\mathrm{T})^x\mu_\alpha$ et

$$w_{\alpha/p} = \int_{\mathbf{Z}_p}(1+\mathrm{T})^x\mu_{\alpha/p} + \int_{\mathbf{Z}_p^*}\ell_{p^{1-k}\alpha}((1+\mathrm{T})^x-1)\mu_\alpha$$
$$+\begin{cases}0 & si\ \alpha\notin p^{k-1-\mathbf{N}},\\ \big(\int_{\mathbf{Z}_p}x^i\mu_\alpha\big)\frac{(p-1)\log\mathrm{T}}{p^2}\cdot\frac{t^i}{i!} & si\ \alpha = p^{k-1-i}.\end{cases}$$

Soit π_α la projection sur $\mathrm{L}\cdot e_\alpha$ parallèlement à $\mathrm{L}\cdot e_{\alpha/p}$. Comme dans le cas cristallin, on déduit de la proposition 4.14 le résultat suivant qui montre que la fonction L p-adique est l'image du système d'Euler de Kato.

Théorème 4.15. — *On a $\pi_\alpha(f)\neq 0$ et*

$$\partial\big(\pi_\alpha(\mathrm{Exp}^*(\mathbf{z}_{\mathrm{Kato}}(f)))\big) = \Big(\int_{\mathbf{Z}_p}(1+\mathrm{T})^x\ \mu_{f^*,p^{k-1}\alpha^{-1}}\Big)\cdot t^{1-k}\pi_\alpha(f).$$

4.5.1. *Zéros supplémentaires des fonctions* L *p-adiques.* Ce qui précède va nous permettre de donner une démonstration d'un théorème de Kato-Kurihara-Tsuji[96]

[95] La distribution μ_α est déterminée par w, mais $\mu_{\alpha/p}$ dépend du choix de $\ell_{p^{1-k}\alpha}$.

[96] Ce théorème [104] fait intervenir l'invariant $\mathscr{L}_{f^*}$ de Fontaine [115] ; un autre candidat pour l'invariant $\mathscr{L}_{f^*}$ a été proposé par Coleman [45] via sa théorie de l'intégration p-adique. Dans le cas d'une forme modulaire correspondant à une courbe elliptique E définie sur $\mathbf{Q}$, l'égalité de ces deux invariants et la formule $\mathscr{L}_{f^*} = \mathscr{L}_{\mathrm{E}}$ sont des conséquences faciles du théorème d'uniformisation de Tate [186]. La formule du th. 4.16 a été démontrée par Stevens [183] (la démonstration est une généralisation de celle de [85] en poids 2 ; les deux ingrédients principaux en sont, d'une part, une formule [182] pour l'invariant de Coleman en termes de dérivées de valeur propres de l'opérateur de Hecke T_p et, d'autre part, la construction d'une fonction L p-adique pour une famille analytique de formes modulaires [183, 134]) avec l'invariant de Coleman, ce qui permet, en regroupant les théorèmes de Stevens et Kato-Kurihara-Tsuji, de montrer (de manière très détournée) que les invariants de Fontaine et Coleman coïncident ; ce dernier fait a été vérifié directement par Coleman et Iovita [48]. (Cf. [94] pour un résultat du même type, et aussi [58] pour une démonstration basée sur une formule exprimant l'invariant $\mathscr{L}_{f^*}$ de Fontaine en termes de dérivées de valeurs propres de frobenius, le résultat de Stevens [182] mentionné ci-dessus et un résultat de Kisin [105] permettant de passer d'une formule à l'autre.)

THÉORÈME 4.16. — *Si f est une forme primitive de poids $k = 2i+2 \geq 2$, de niveau* N *divisible par p, et si la valeur propre de* T_p *est $p^i = \beta$, alors* $\mathrm{L}_{p,\beta}(f, x_p^{i+1}, 0) = 0$ *et*

$$\mathrm{L}'_{p,\beta}(f, x_p^{i+1}, 0) = \mathscr{L}_{f^*} \cdot \widetilde{\mathrm{L}}(f, i+1).$$

Démonstration. — Utilisant le th. 4.15, on se ramène à un calcul purement local dans $(\mathrm{D}^\dagger_{\alpha,\mathscr{L}})^{\psi=1}$, avec $\alpha = p^{i+1}$ et $\mathscr{L} = \mathscr{L}_{f^*}$, et on reprend les notations de la proposition 4.14. Comme $\psi(\mu_\alpha) = p^{1-k}\alpha\mu_\alpha$, on a

$$\int_{\mathbf{Z}_p^*} x^i \mu_\alpha = \int_{\mathbf{Z}_p} x^i\,(1 - p^{1-k}\alpha\varphi) \cdot \mu_\alpha = (1 - \alpha p^{i-k+1}) \int_{\mathbf{Z}_p} x^i \mu_\alpha.$$

En particulier, si $\alpha \neq p^{k-1-i}$, l'intégrale $\int_{\mathbf{Z}_p^*} x^i \mu_\alpha$ ne s'annule que si $\int_{\mathbf{Z}_p} x^i \mu_\alpha = 0$. Par contre, si $\alpha = p^{k-1-i}$ ce qui est le cas sous les hypothèses du théorème, la fonction $s \mapsto \int_{\mathbf{Z}_p^*} x^i \langle x\rangle^s\, \mu_\alpha$ a un zéro trivial en $s = 0$ et sa dérivée est donnée par la proposition suivante qui permet de conclure.

PROPOSITION 4.17. — *Si $\alpha = p^{k-1-i}$, alors*

$$\int_{\mathbf{Z}_p^*} x^i \log x\, \mu_\alpha = \mathscr{L} \cdot \int_{\mathbf{Z}_p} x^i \mu_\alpha.$$

Démonstration. — L'idée est d'évaluer $\partial^i((1-p\varphi)\cdot w) = (1-p^{i+1}\varphi)\cdot \partial^i w$ en $\mathrm{T} = 0$; on note $ae_\alpha + b\mathrm{N}e_\alpha$ le résultat. La fonction w n'est pas définie en $\mathrm{T} = 0$, mais on peut utiliser l'équation fonctionnelle $\psi(w) = w$ pour prolonger $(1-p\varphi)\cdot w$ en 0. Cette équation fonctionnelle se traduit, en utilisant la relation $1 + \mathrm{T} = e^t$, par les identités

$$\begin{aligned}
(1-p\varphi)\cdot w = w - p\varphi(\psi(w)) &= \sum_{j\in(\mathbf{Z}/p\mathbf{Z})^*} \Big(w_\alpha(\zeta_p^j e^t - 1)\frac{e_\alpha}{t^{k-1}} + w_{\alpha/p}(\zeta_p^j e^t - 1)\frac{\mathrm{N}e_\alpha}{t^{k-1}}\Big) \\
&= \frac{1}{p^{n-1}} \sum_{j\in(\mathbf{Z}/p^n\mathbf{Z})^*} \Big(w_\alpha(\zeta_{p^n}^j e^{t/p^{n-1}} - 1)\varphi^{1-n}\Big(\frac{e_\alpha}{t^{k-1}}\Big) \\
&\qquad\qquad + w_{\alpha/p}(\zeta_{p^n}^j e^{t/p^{n-1}} - 1)\varphi^{1-n}\Big(\frac{\mathrm{N}e_\alpha}{t^{k-1}}\Big)\Big)
\end{aligned}$$

Cette dernière expression converge pour n assez grand. Notons $a_{n,i}^{(j)}$ (resp. $b_{n,i}^{(j)}$) le coefficient de t^i dans le développement de $w_\alpha(\zeta_{p^n}^j e^t - 1)$ (resp. de $w_{\alpha/p}(\zeta_{p^n}^j e^t - 1)$). On a alors

$$a = \frac{1}{p^{n-1}} \sum_{j\in(\mathbf{Z}/p^n\mathbf{Z})^*} \Big(\frac{p^i\alpha}{p^{k-1}}\Big)^{-(n-1)} a_{n,i}^{(j)} \quad \text{et} \quad b = \frac{1}{p^{n-1}} \sum_{j\in(\mathbf{Z}/p^n\mathbf{Z})^*} \Big(\frac{p^i\alpha}{p^{k}}\Big)^{-(n-1)} b_{n,i}^{(j)}.$$

D'après le (i) de la prop. 4.14, on a $b_{n,i}^{(1)} = p^{-n}\mathscr{L} a_{n,i}^{(1)}$, ce qui implique en vertu de l'action de $\mathrm{Gal}(\mathbf{Q}_p(\zeta_{p^\infty})/\mathbf{Q}_p)$, la relation $b_{n,i}^{(j)} = p^{-n}\mathscr{L} a_{n,i}^{(j)}$ pour tout $j \in (\mathbf{Z}/p^n\mathbf{Z})^*$, et finalement, la relation

$$b = p^{-1}\mathscr{L} a.$$

Il reste à calculer explicitement a et b pour pouvoir exploiter cette relation. Soit $f_i = \partial^i \ell_{p^{-i}}$ et $g_i = \partial^i(\log \mathrm{T}\cdot\frac{t^i}{i!}) - \log \mathrm{T} \in \mathscr{R}_{\mathrm{L}}^+$. On peut alors écrire $t^{k-1}\cdot\partial^i w$ sous la forme $w_1 e_\alpha + w_2 \mathrm{N} e_\alpha$, avec $w_1 = \int_{\mathbf{Z}_p} x^i (1+\mathrm{T})^x \mu_\alpha$ et

$$w_2 = \int_{\mathbf{Z}_p} x^i(1+\mathrm{T})^x\mu_{\alpha/p} + \int_{\mathbf{Z}_p^*} x^i f_i((1+\mathrm{T})^x - 1)\mu_\alpha + \frac{p-1}{p}\cdot\int_{\mathbf{Z}_p} x^i\mu_\alpha\cdot(\log \mathrm{T} + g_i).$$

On a $t^{k-1}\cdot(1-p^{i+1}\varphi)\cdot\partial^i w = (1-p\varphi)w_1 e_\alpha + (1-\varphi)w_2 \mathrm{N} e_\alpha$. On obtient donc en évaluant en $\mathrm{T}=0$,

$$a = (1-p)\int_{\mathbf{Z}_p} x^i \mu_\alpha.$$

Pour évaluer $(1-\varphi)w_2$ en $\mathrm{T}=0$, il faut faire un petit peu attention car les fonctions ne sont définies en $\mathrm{T}=0$ que par un procédé de régularisation (si tout était défini en 0, on obtiendrait 0) ; le premier et le troisième terme donnent une contribution nulle (la contribution du troisième est nulle car $\log p = 0$), et on obtient

$$b = \Big((1-\varphi)\Big(\int_{\mathbf{Z}_p^*} x^i f_i((1+\mathrm{T})^x - 1)\mu_\alpha\Big)\Big)_{\mathrm{T}=0} = \Big(\int_{\mathbf{Z}_p^*} x^i\big((1-\varphi)\cdot f_i\big)((1+\mathrm{T})^x-1)\mu_\alpha\Big)_{\mathrm{T}=0}.$$

Pour continuer le calcul, nous aurons besoin du lemme suivant.

Lemme 4.18. — (i) f_i se prolonge de manière unique en une fonction localement analytique sur le disque épointé $0 < v_p(z) < +\infty$ vérifiant l'équation fonctionnelle

$$f_i(z) = \frac{p-1}{p}\log z + \sum_{(y+1)^p = z+1} f_i(y).$$

(ii) $(1-\varphi)\cdot f_i + \frac{p-1}{p}\log\varphi(\mathrm{T})$ se prolonge en une fonction continue sur le disque $0 < v_p(z)$.

(iii) Si $x \in \mathbf{Z}_p^*$, alors $h_x = ((1-\varphi)\cdot f_i)((1+\mathrm{T})^x - 1) - (1-\varphi)\cdot f_i(\mathrm{T})$ se prolonge en une fonction continue sur le disque $0 < v_p(z)$, et on a $h_x(0) = -\frac{p-1}{p}\log x$.

Démonstration. — Le (i) suit de ce que f_i est définie sur une couronne non vide $0 < v_p(z) \le r$, $r > 0$ et de l'équation fonctionnelle $f_i = p\psi(f_i) + \frac{p-1}{p}(\log \mathrm{T} + g_i)$. Le (iii) est une conséquence immédiate du (ii) qui suit du (i) et de l'équation fonctionnelle déjà mentionnée que l'on peut réécrire (en appliquant φ aux deux membres) sous la forme

$$\varphi(f_i) - f_i = \frac{p-1}{p}(\log\varphi(\mathrm{T}) + \varphi(g_i)) + \sum_{\zeta^p=1,\zeta\ne 1} f_i((1+\mathrm{T})\zeta - 1).$$

Pour terminer le calcul de b, on peut retrancher $\int_{\mathbf{Z}_p^*} x^i\big((1-\varphi)\cdot f_i\big)\mu_\alpha$, qui est nul car $\int_{\mathbf{Z}_p^*} x^i\mu_\alpha = 0$, à l'intégrale ci-dessus, et la réécrire sous la forme

$$b = \Big(\int_{\mathbf{Z}_p^*} x^i h_x(\mathrm{T})\mu_\alpha\Big)_{\mathrm{T}=0} = \int_{\mathbf{Z}_p^*} x^i h_x(0)\,\mu_\alpha = -\frac{p-1}{p}\cdot\int_{\mathbf{Z}_p^*} x^i\log x\,\mu_\alpha.$$

4.6. **Les cas potentiellement cristallin et potentiellement semi-stable**

On peut, en principe, faire la liste, à isomorphisme près, des $\mathbf{D}_{\mathrm{pst}}$ des L-représentations potentiellement semi-stables de $\mathscr{G}_{\mathbf{Q}_p}$ de dimension 2, dont les poids de Hodge-Tate sont 0 et $1-k$, mais on ne sait pas décrire les $\mathrm{D}^{\psi=1}$ en termes de distributions (sauf si l'extension sur laquelle la représentation devient semi-stable est abélienne), ce qui rend problématique la construction de fonctions L p-adiques dans ce cas. Mais il est clair que l'on veut que la fonction L p-adique soit, comme dans les th. 4.11 et 4.15, l'image de $\mathbf{z}_{\mathrm{Kato}}(f^*)$ dans $\mathbf{D}^\dagger(\mathrm{V}_{f^*})^{\psi=1}$; notre problème est donc juste d'interpréter le résultat.

Remerciements. Ce texte aurait probablement été beaucoup plus superficiel sans le séjour que j'ai effectué au Japon au printemps 2003 à l'invitation de K. Fujiwara ; je voudrais profiter de l'occasion pour remercier K. Fujiwara, K. Kato et T. Saito ainsi que les universités de Tokyo, Nagoya et Kyoto, de leur hospitalité. Il aurait aussi contenu beaucoup plus d'inexactitudes sans les explications, remarques et corrections de L. Berger, D. Blasius, C. Breuil, G. Chenevier, A. Iovita, G. Kings, K. Kato, J. Nekovář, K. Rubin, J. Tilouine et M-F. Vigneras que je voudrais remercier pour leur aide.

RÉFÉRENCES

[1] A. Agboola et B. Howard, Anticyclotomic Iwasawa theory of CM elliptic curves, preprint 2003.

[2] Y. Amice, Interpolation p-adique, Bull. Soc. France **92** (1964) 117-180.

[3] Y. Amice, Duals. Proc. of a conf. on p-adic analysis (Nijmegen 1978), 1-15, Nijmegen, Math. Institut Katholische Univ., 1978.

[4] Y. Amice et J. Vélu, Distributions p-adiques associées aux séries de Hecke, Astérisque **24-25** (1975) 119–131.

[5] K. Barré-Sirieix, G. Diaz, F. Gramain, G. Philibert, Une preuve de la conjecture de Mahler-Manin, Invent. Math. **124** (1996) 1–9.

[6] D. Barsky, Fonctions zêta p-adiques d'une classe de rayon des corps totalement réels, Groupe d'études d'analyse ultramétrique, 1977-1978 ; errata 1978-1979

[7] A. Beilinson, Higher regulators and values of L-functions, J. Soviet Math. **30** (1985) 2036–2070.

[8] A. Beilinson, Higher regulators of modular curves, Cont. Math. **55** (1986) 1–34.

[9] J. Bellaïche, Congruences endoscopiques et représentations galoisiennes, Thèse de l'université Paris 11, 2002.

[10] J. Bellaïche et G. Chenevier, Formes non tempérées pour U(3) et conjectures de Bloch-Kato, Annales E.N.S. (à paraître).

[11] D. Benois, On Iwasawa theory of crystalline representations, Duke Math. J. **104** (2000) 211–267.

[12] L. Berger, Représentations p-adiques et équations différentielles, Invent. Math. **148** (2002), 219–284.

[13] L. Berger, Représentations de de Rham et normes universelles, Bull. S.M.F. (à paraître).

[14] M. Bertolini et H. Darmon, Heegner points on Mumford-Tate curves, Invent. Math. **126** (1996) 413–456.

[15] M. Bertolini et H. Darmon, A rigid-analytic Gross-Zagier formula and arithmetic applications, Ann. of Math. **146** (1997) 111–147.

[16] M. Bertolini et H. Darmon, Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformisation, Invent. Math. **131** (1998) 453–491.

[17] M. Bertolini et H. Darmon, p-adic periods, p-adic L-functions and the p-adic uniformisation of Shimura curves, Duke Math. J. **98** (1999) 305–334.

[18] M. Bertolini et H. Darmon, The p-adic L-functions of modular elliptic curves, *in 2001 and Beyond*, Springer-Verlag 2001.

[19] M. Bertolini, H. Darmon, A. Iovita et M. Spiess, Teitelbaum's conjecture in the anticyclotomic setting, Amer. J. Math. **124** (2002) 411–449.

[20] M. Bertolini et H. Darmon, Iwasawa's main conjecture for elliptic curves in the anticyclotomic setting, preprint.

[21] D. Bertrand, Relations d'orthogonalité sur les groupes de Mordell-Weil, Séminaire de théorie des nombres, Paris 1984–85, 33–39, Progr. Math. **63**, Birkhäuser 1986.

[22] A. Besser, Syntomic regulators and p-adic integration I : rigid syntomic regulators, Isr. J. Math. **120** (2000) 291-334.

[23] A. Besser, Syntomic regulators and p-adic integration II : K_2 of curves, Isr. J. Math. **120** (2000) 335-359.

[24] A. Besser, The p-adic height pairings of Coleman-Gross et Nekovář, proceedings of CNTA7, Montréal (à paraître).

[25] B. Birch et H. Swinnerton-Dyer, Notes on elliptic curves. I, J. Reine Angew. Math. **212** (1963) 7–25.

[26] B. Birch et H. Swinnerton-Dyer, Notes on elliptic curves. II, J. Reine Angew. Math. **218** (1965) 79–108.

[27] S. Bloch et K. Kato, L functions and Tamagawa numbers of motives, dans The Grothendieck Festschrift, vol. 1, Prog. in Math. **86**, 333–400, Birkhäuser 1990.

[28] J-B. Bost, Algebraic leaves of algebraic foliations over number fields, Publ. Math. I.H.E.S **93** (2001) 161–221.

[29] C. Breuil, B. Conrad, F. Diamond et R. Taylor, On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises, J. Amer. Math. Soc. **14** (2001), 843–939.

[30] A. Brumer, On the units of algebraic number fields, Mathematika **14** (1967) 121–124.

[31] H. Carayol, Sur les représentations l-adiques associées aux formes modulaires de Hilbert, Ann. Sci. cole Norm. Sup. (4) **19** (1986) 409–468.

[32] J. Cassels, Arithmetic on an elliptic curve, 1963 Proc. Internat. Congr. Mathematicians (Stockholm, 1962) 234–246 Inst. Mittag-Leffler, Djursholm.

[33] J. Cassels, Diophantine equations with special reference to elliptic curves, J. London Math. Soc. **41** (1966) 193–291.

[34] P. Cassou-Noguès, Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques. Invent. Math. **51** (1979) 29-59.

[35] A. Chambert-Loir, Théorèmes d'algébricité en géométrie diophantienne (d'après J.-B. Bost, Y. André, D. et G. Chudnovsky), *Sém. Bourbaki 2000/01*, exp. 886, Astérisque **282** (2002) 175–209.

[36] F. Cherbonnier, P. Colmez, Théorie d'Iwasawa des représentations p-adiques d'un corps local, J. Amer. Math. Soc **12**, 241-268, 1999

[37] F. Cherbonnier et P. Colmez, Représentations p-adiques surconvergentes, Invent. Math. **133** (1998), 581–611.

[38] D.V. Chudnovsky et G.V. Chudnovsky, Padé approximations and Diophantine geometry. Proc. Natl. Acad. Sci. USA **82** (1985) 2212–2216.

[39] J. Coates, The work of Mazur and Wiles on cyclotomic fields, *Sém. Bourbaki 1980/81*, exp. 575, 220–242, Lecture Notes in Math. **901**.

[40] J. COATES, The work of Gross and Zagier on Heegner points and the derivatives of L-series, *Sem. Bourbaki 1984/85*, exp. 635, Astérisque **133-134** (1986) 57–72.

[41] J. COATES et A. WILES, On the conjecture of Birch and Swinnerton-Dyer, Invent. Math. **39** (1977) 223–251.

[42] J. COATES et A. WILES, On p-adic L-functions and elliptic units, J. Australian Math. Soc., **A 26** (1978) 1–25.

[43] R. COLEMAN, Division values in local fields, Invent. Math. **53** (1979) 91-116.

[44] R. COLEMAN, The dilogarithm and the norm residue symbol, Bull. S.M.F. **109** (1981) 373–402.

[45] R. COLEMAN, A p-adic Shimura isomorphism and p-adic periods of modular forms, Contemp. Math. **165** (1994) 21–51.

[46] R. COLEMAN et B. GROSS, p-adic heights on curves, Adv. Math. **17** (1989) 73-81.

[47] R. COLEMAN et E. DE SHALIT, p-adic regulators on curves and special values of p-adic L-functions, Invent. Math. **93** (1988), 239–266.

[48] R. COLEMAN et A. IOVITA, Hidden structures on semi-stable curves, preprint 2003.

[49] C. CORNUT, Mazur's conjecture on higher Heegner points, Invent. Math. **148** (2002) 495–523.

[50] P. COLMEZ, Résidu en $s = 1$ des fonctions zêta p-adiques, Invent. Math. **91** (1988) 371-389.

[51] P. COLMEZ, Théorie d'Iwasawa des représentations de de Rham d'un corps local, Ann. of Math. **148** (1998) 485-571.

[52] P. COLMEZ, Intégration sur les variétés p-adiques, Astérisque **248** (1998).

[53] P. COLMEZ, Représentations p-adiques d'un corps local, *Proceedings of the International Congress of Mathematicians II (Berlin 1998)*, Doc. Mat. Extra vol. II (1998), 153–162.

[54] P. COLMEZ, Fonctions L p-adiques, *Sém. Bourbaki 1998/99*, exp. 851, Astérisque **266** (2000) 21–58.

[55] P. COLMEZ, Les conjectures de monodromie p-adiques, *Sém. Bourbaki 2001/02*, exp. 897, Astérisque **290** (2003), 53-101.

[56] P. COLMEZ, Arithmétique de la fonction zêta, dans *La fonction zêta*, 37-164, journées X-UPS 2002.

[57] P. COLMEZ, Espaces de Banach de dimension finie, J. Inst. Math. Jussieu **1** (2002), 331–439.

[58] P. COLMEZ, Invariants $\mathscr{L}$ et dérivées de valeurs propres de frobenius, preprint 2003.

[59] P. COLMEZ et J-M. FONTAINE, Construction des représentations p-adiques semi-stables, Invent. Math. **140** (2000), 1–43.

[60] H. DARMON, Integration on $\mathscr{H}_p \times \mathscr{H}$ and arithmetic applications, Ann. of Math. **154** (2001) 589–639.

[61] H. DARMON et A. IOVITA, The anticyclotomic main conjecture for supersingular elliptic curves, preprint 2003.

[62] D. DELBOURGO, On the p-adic Birch, Swinnerton-Dyer conjecture for non-semistable reduction, J. Number Theory **95** (2002) 38–71.

[63] P. DELIGNE, Formes modulaires et représentations ℓ-adiques, *Sém. Bourbaki 1968/69*, exp. 343, SLN **179** (1971) 139-172.

[64] P. DELIGNE, Valeurs de fonctions L et périodes d'intégrales, dans Automorphic forms, representations and L-functions, Proc. Symp. Pure Math. **33** (1979) 313–346.

[65] P. DELIGNE, Preuve des conjectures de Tate et de Shafarevitch (d'après G. Faltings), *Sém. Bourbaki 1983/84*, exp. 616, Astérisque **121-122** (1985) 25–41.

[66] P. DELIGNE et K. RIBET, Values of Abelian L-functions at Negative Integers Over Totally Real Fields, Invent. Math. **59** (1980) 227–286.

[67] C. DENINGER et A. SCHOLL, The Beilinson conjectures, L-*functions and arithmetic (Durham, 1989)*, 173–209, London Math. Soc. Lecture Note Ser. **153**, Cambridge Univ. Press 1991.

[68] M. DEURING, Die Zetafunktion einer algebraischen Kurve vom Geschlecte Eins, I,…,IV, Gött. Nac., 1953-1957.

[69] B. Edixhoven, Rational elliptic curves are modular (after Breuil, Conrad, Diamond and Taylor), *Sém. Bourbaki 1999/2000*, exp. 871 Astérisque No. **276** (2002) 161–188.

[70] M. Eichler, Quaternäre quadratische Formen und die Riemannsche Vermutung für die Konguenzzetafunktion, Archiv der Mat. **5** (1954) 355–366.

[71] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **73** (1983), 349–366.

[72] G. Faltings, Almost étale extensions, Astérisque **279** (2002), 185–270.

[73] J.-M. Fontaine, Sur certains types de représentations p-adiques du groupe de Galois d'un corps local ; construction d'un anneau de Barsotti-Tate, Ann. Math. **115** (1982) 529–577.

[74] J.-M. Fontaine, Le corps des périodes p-adiques. dans "*Périodes p-adiques*" exposé II, Astérisque **223** (1994) 59–102.

[75] J.-M. Fontaine, Représentations p-adiques des corps locaux, dans "*The Grothendieck Festschrift*", vol 2, Prog. in Math. **87**, 249–309, Birkhäuser 1991.

[76] J.-M. Fontaine, Valeurs spéciales de fonctions L des motifs, *Sém. Bourbaki 1991/92*, exp. 751, Astérisque **206**, 205-249, 1992.

[77] J.-M. Fontaine et B. Perrin-Riou, Autour des conjectures de Bloch et Kato : cohomologie galoisienne et valeurs de fonctions L, dans *Motives (Seattle)*, Proceedings of Symposia in Pure Mathematics, vol. **55**, part 1, 599-706, 1994.

[78] T. Fukaya, The theory of Coleman power series for K_2, J. Alg. Geom. **12** (2003) 1–80.

[79] T. Fukaya, Coleman power series for K-groups and explicit reciprocity laws, preprint 2003.

[80] M. Gealy, Special values of p-adic L-functions associated to modular forms, preprint 2003.

[81] E. Ghate et V. Vatsal, On the local behaviour of Λ-adic representations, preprint 2003.

[82] D. Goldfeld, The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer, Ann. Scuola Norm. Sup. Pisa (4) **3** (1976) 624–663.

[83] R. Greenberg, Iwasawa theory for p-adic representations, Adv. Stud. Pure Math. **17** (1989) 97–137.

[84] R. Greenberg, On the Birch and Swinnerton-Dyer conjecture, Invent. Math. **72** (1983) 241–265.

[85] R. Greenberg et G. Stevens, p-adic L-functions and p-adic periods of modular forms, Invent. Math. **111** (1993) 407–447.

[86] B. Gross et D. Zagier, Heegner points and derivatives of L-series, Invent. Math. **84** (1986) 225–320.

[87] L. Guo, General Selmer groups and critical values of Hecke L-functions, Math. Ann. **297** (1993) 221–233.

[88] L. Herr, Sur la cohomologie galoisienne des corps p-adiques, Bull. S.M.F. **126** (1998), 563–600.

[89] H. Hida, Anticyclotomic Main Conjectures, preprint 2003.

[90] H. Hida et J. Tilouine, On the anticyclotomic main conjecture for CM fields, Invent. Math. **117** (1994) 89–147.

[91] H. Hida et J. Tilouine, Anti-cyclotomic Katz p-adic L-functions and congruence modules. Ann. Sci. E.N.S. **26** (1993) 189–259.

[92] O. Hyodo, On the Hodge-Tate decomposition in the imperfect residue field case, J. Reine Angew. Math. **365** (1986) 97–113.

[93] A. Iovita et R. Pollack, Iwasawa theory of Elliptic Curves at Supersingular Primes over $\mathbf{Z}_p$-extensions of number fields, MSRI Proceedings of a Conference on "Rankin's method in arithmetic" (à paraître).

[94] A. Iovita et M. Spiess, Derivatives of p-adic L-functions, Heegner cycles and monodromy modules attached to modular forms, Invent. Math. **154** (2003) 333-384.

[95] A. Iovita et A. Werner, p-adic height pairings on abelian varieties with semistable ordinary reduction, J. Crelle **564** (2003), 181-203.

[96] K. Iwasawa, On explicit formulas for the norm residue symbol, J. Math. Soc. Japan **20** (1968) 151–164.

[97] H. Jacquet et J. Shalika, A non vanishing theorem for zeta functions of $\mathbf{GL}_n$, Invent. Math. **38** (1976) 1–16.

[98] K. Kato, The explicit reciprocity law and the cohomology of Fontaine-Messing, Bull. S.M.F. **119** (1991) 397–441.

[99] K. Kato, Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via $\mathbf{B}_{\mathrm{dR}}$, in *Arithmetic Algebraic Geometry*, Lect. Notes in Math. **1553**, Springer 1993.

[100] K. Kato, Euler systems, Iwasawa theory and Selmer groups, Kodai Math. J. **22** (1999) 313–372.

[101] K. Kato, Generalized explicit reciprocity laws, *Algebraic number theory (Hapcheon/Saga, 1996)*, Adv. Stud. Contemp. Math. (Pusan) **1** (1999), 57–126.

[102] K. Kato, Hodge theory and values of zeta functions of modular forms, Astérisque (à paraître).

[103] K. Kato, M. Kurihara et T. Tsuji, Local Iwasawa theory of Perrin-Riou and syntomic complexes, preprint 1996

[104] K. Kato, M. Kurihara et T. Tsuji, cours au centre Émile Borel, premier semestre 1997.

[105] M. Kisin, Overconvergent modular forms and the Fontaine-Mazur conjecture, Invent. Math. **153** (2003) 373–454.

[106] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, Invent. Math. **152** (2003) 1–36.

[107] V. Kolyvagin, Euler systems, The Grothendieck Festschrift, vol. **2**, Prog. in Math. **87**, 436–483, Birkhäuser 1990.

[108] D. Kubert et S. Lang, Units in the modular function fields II, Math. Ann. **218** (1975) 175–189.

[109] M. Kurihara, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I, Invent. Math. **149** (2002) 195–224.

[110] S. Lang, Les formes bilinéaires de Néron et Tate, *Sém. Bourbaki 1963/64*, exp. 274, rééd. Sém Bourbaki 1948-1968, vol. **8**, Soc. Math. France 1995.

[111] S. Lang, Sur la conjecture de Birch-Swinnerton-Dyer (d'après J. Coates et A. Wiles), *Sém. Bourbaki 1976/77*, exp. 503, pp. 189–200, Lecture Notes in Math. **677** (1978) 189–200.

[112] Y. Manin, Periods of cusp forms, and p-adic Hecke series, Math USSR-Sb. **92** (1973) 371–393.

[113] B. Mazur, Rational points of abelian varieties in towers of number fields, Invent. Math. **18** (1972) 183–266.

[114] B. Mazur, Modular curves and arithmetic, *Proceedings of the International Congress of Mathematicians (Warsaw, 1983)*, 185–211, PWN, Warsaw, 1984.

[115] B. Mazur, On monodromy invariants occuring in global arithmetic, and Fontaine's theory, Contemp. Math. **165** (1994) 1–20.

[116] B. Mazur et K. Rubin, Kolyvagin systems, Memoirs of the A.M.S. **168** (2004).

[117] B. Mazur et K. Rubin, Elliptic curves and class field theory, Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002), 185–195, Higher Ed. Press, Beijing, 2002.

[118] B. Mazur et P. Swinnerton-Dyer, Arithmetic of Weil curves, Invent. Math. **25** (1974), 1–61.

[119] B. Mazur et J. Tate, Canonical height pairings via biextensions, Prog. in Math. **35**, 195–238, Birkhäuser, 1983.

[120] B. Mazur et J. Tate, The p-adic sigma function, Duke Math. J. **62** (1991) 663-688.

[121] B. Mazur, J. Tate et J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Invent. Math. **84** (1986) 1-48.

[122] B. Mazur et J. Tilouine, Représentations galoisiennes, différentielles de Kähler et « conjectures principales », Publ. Math I.H.E.S. **71** (1990) 65–103.

[123] B. Mazur et A. Wiles, Class fields of abelian extensions of $\mathbf{Q}$, Invent. Math. **76** (1984) 179-330.

[124] J-F. Mestre, Formules explicites et minorations de conducteurs de variétés algébriques, Comp. Math. **58** (1986) 209–232.

[125] J. Nekovář, Kolyvagin's method for Chow groups of Kuga-Sato varieties, Invent. Math. **107** (1992) 99-125.

[126] J. Nekovář, On p-adic height pairings, dans Séminaire de théorie des nombres 1990-1991, Prog. in Math. **108**, 127-202, Birkhäuser 1993.

[127] J. Nekovář, On the p-adic heights of Heegner cycles, Math. Ann. **302** (1995) 609–686.

[128] J. Nekovář, On the parity of ranks of Selmer groups II, C.R.A.S. **332** (2001) 99–104.

[129] A. Néron, Quasi-fonctions et hauteurs sur les variétés abéliennes, Ann. of Math. **82** (1965) 249-331.

[130] A. Néron, Fonctions thêta p-adiques et hauteurs p-adiques, Séminaire de Théorie des Nombres, Paris 1980-1981, Prog. in Math. **22**, Birkhäuser, 1982.

[131] J. Oesterlé, Nombres de classes des corps quadratiques imaginaires, *Sém. Bourbaki 1983/84*, exp. 631, Astérisque **121-122** (1985), 309–323.

[132] J. Oesterlé, Travaux de Wiles (et Taylor, ...). II, *Sém. Bourbaki 1994/95*, exp. 804, Astérisque **237** (1996) 333–355.

[133] A. Panchishkin, A new method of constructing p-adic L-functions associated with modular forms, Mosc. Math. J. **2** (2002) 313–328.

[134] A. Panchishkin, Two variable p-adic L functions attached to eigenfamilies of positive slope, Invent. Math. **154** (2003), 551-615.

[135] B. Perrin-Riou, Hauteurs p-adiques, Séminaire de Théorie des Nombres, Paris 1982-1983, Prog. in Math. **51**, Birkhäuser, 1984.

[136] B. Perrin-Riou, Points de Heegner et dérivées de fonctions L p-adiques, Invent. Math. **89** (1987) 455–510.

[137] B. Perrin-Riou, Théorie d'Iwasawa p-adique locale et globale, Invent. Math. **99** (1990) 247-292.

[138] B. Perrin-Riou, Travaux de Kolyvagin et Rubin, *Sém. Bourbaki 1989/90*, exp. 717, Astérisque **189-190** (1990) 69–106.

[139] B. Perrin-Riou, Théorie d'Iwasawa et hauteurs p-adiques, Invent. Math. **109** (1992) 137-185.

[140] B. Perrin-Riou, Fonctions L p-adiques d'une courbe elliptique et points rationnels, Ann. Inst. Fourier **43** (1993) 945–995.

[141] B. Perrin-Riou, Théorie d'Iwasawa des représentations p-adiques sur un corps local, Invent. Math. **115** (1994) 81-149.

[142] B. Perrin-Riou, *Fonctions L p-adiques des représentations p-adiques*, Astérisque **229** (1995).

[143] B. Perrin-Riou, Systèmes d'Euler et représentations p-adiques, Ann. Inst. Fourier **48** (1998) 1231-1307.

[144] B. Perrin-Riou, Représentations p-adiques et normes universelles I, le cas cristallin, J. Amer. Math. Soc. **13** (2000) 533–551.

[145] B. Perrin-Riou, Théorie d'Iwasawa des représentations p-adiques semi-stables, Mém. Soc. Math. Fr. **84** (2001).

[146] B. Perrin-Riou, Quelques remarques sur la théorie d'Iwasawa des courbes elliptiques, *Number theory for the millennium, III* (Urbana, IL, 2000) 119–147.

[147] B. Perrin-Riou, Arithmétique des courbes elliptiques à réduction supersingulière en p, preprint 2001.

[148] R. Pollack, On the p-adic L-function of a modular form at a supersingular prime, Duke Math. J. **118** (2003) 523–558.

[149] R. Pollack et K. Rubin, The main conjecture for CM elliptic curves at supersingular primes, Ann. of Maths **159** (2004), 447-464.

[150] R. Pollack et G. Stevens, The "missing" p-adic L-function, preprint 2003.

[151] K. Ribet, Galois representations attached to modular forms, Invent. Math. **28** (1975) 245–275.

[152] K. Ribet, A modular construction of unramified extensions of $\mathbf{Q}(\zeta_p)$, Invent. Math. **34** (1976) 151–162.

[153] K. Ribet, Galois representations attached to modular forms II, Glasgow Math. J. **27** (1985) 185–194.

[154] D. Rohrlich, On L-functions of elliptic curves and cyclotomic towers, Invent. Math. **75** (1984) 409–423.

[155] K. Rubin, Elliptic curves and $\mathbf{Z}_p$-extensions, Comp. Math. **56** (1985) 237-250.

[156] K. Rubin, Local units, elliptic units, Heegner points, and elliptic curves, Invent. Math. **88** (1987) 405–422.

[157] K. Rubin, Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication, Invent. Math. **89** (1987) 527–560.

[158] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Invent. Math. **103** (1991) 25–68.

[159] K. Rubin, *Euler systems*, Ann. of Math. Studies **147**, Princeton Univ. Press (2000).

[160] A. Scholl, Motives for modular forms, Invent. Math. **100** (1990) 419–430.

[161] A. Scholl, Remarks on special values of L-functions, dans L-*functions and Arithmetic*, Proc. of the Durham Symp., London Math. Soc. L.N.S. **153**, Cambridge University Press, 1991, 373–392.

[162] A. Scholl, An introduction to Kato's Euler systems, dans *Galois representations in arithmetic algebraic geometry*, 379-460, Cambridge University Press, 1998

[163] A. Scholl, Higher regulators and special values of L-functions of modular forms, en préparation.

[164] A. Scholl, Zeta elements for higher weight modular forms, en préparation.

[165] P. Schneider, p-adic height pairings, II, Invent. Math. **79**, 329-374, 1985

[166] P. Schneider et J. Teitelbaum, p-adic Fourier theory, Doc. Math. **6** (2001) 447–481.

[167] J-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, W. A. Benjamin 1968.

[168] J-P. Serre, Formes modulaires et fonctions zêta p-adiques, *Modular functions of one variable III*, Lect. Notes Math. **350** (1972) 191–268.

[169] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972) 259-331.

[170] J-P. Serre, Travaux de Wiles (et Taylor, ...). I, *Sém. Bourbaki 1994/95*, exp. 803, Astérisque **237** (1996) 319–332.

[171] J-P. Serre, lettre du 13/11/59, in *Correspondance Grothendieck-Serre*, Documents Mathématiques **2**, Soc. Math. de France 2001.

[172] G. Shimura, Correspondances modulaires et les fonctions ζ de courbes algébriques, J. Math. Soc. Japan **10** (1958) 1–28.

[173] G. Shimura, Sur les intégrales attachées aux formes automorphes, J. Math. Soc. Japan **11** (1959) 291–311.

[174] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kan Memorial Lectures 1, Pub. of the Math. Soc. of Japan **11**, 1971.

[175] G. Shimura, On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields, Nagoya Math. J. **43** (1971) 199–208.

[176] G. Shimura, On the factors of the jacobian variety of a modular function field. J. Math. Soc. Japan **25** (1973) 523–544.

[177] G. Shimura, The special values of the zeta functions associated with cusp forms, Comm. Pure Appl. Math. **29** (1976) 783–804.

[178] C. Skinner et E. Urban, Sur les déformations p-adiques des formes de Saito-Kurokawa, C.R.A.S. **335** (2002) 581–586.

[179] C. Skinner et E. Urban, En préparation.

[180] C. Soulé, Régulateurs, *Sém. Bourbaki 1984/85*, exp. 644, Astérisque **133-134** (1986) 237–253.

[181] C. Soulé, Eléments cyclotomiques en K-théorie, Astérisque **147-148** (1987) 225-257.

[182] G. Stevens, Coleman's $\mathscr{L}$-invariant and families of modular forms, preprint 1996.

[183] G. Stevens, Cours au centre Émile Borel, premier semestre 2000.

[184] J. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, *Sém. Bourbaki 1965/66*, exp. 306, rééd. Sém Bourbaki 1948-1968, vol. **9**, Soc. Math. France 1995.

[185] J. Tate, p-divisible groups, Proc. of a conference on local fields, Nuffic Summer School at Driebergen, Springer, Berlin, 158-183, 1967

[186] J. Tate, A review of non-Archimedean elliptic functions, *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, 162–184, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995.

[187] F. Thaine, On the ideal class group of real abelian number fields, Ann. of Math. **128** (1988) 1–18.

[188] J. Tilouine, Sur la conjecture principale anticyclotomique Duke Math. J. **59** (1989) 629-673.

[189] T. Tsuji, p-adic étale cohomology and crystalline cohomology in the semi-stable reduction case. Invent. Math. **137** (1999), 233–411.

[190] T. Tsuji, Semi-stable conjecture of Fontaine-Jannsen : a survey, Astérisque **279** (2002), 323–370.

[191] V. Vatsal, Uniform distribution of Heegner points, Invent. Math. **148** (2002) 1–46.

[192] M. Vishik, Non-archimedian measures connected with Dirichlet series, Math. USSR Sbornik **28** (1976) 216–228.

[193] M. Waldschmidt, Sur la nature arithmétique des valeurs de fonctions modulaires, *Sém. Bourbaki 1996/97*, exp. 824, Astérisque **245** (1997) 105–140.

[194] A. Weil, *Elliptic functions according to Eisenstein and Kronecker*, Erg. der Math. **88** (1976), Springer-Verlag.

[195] A. Wiles, Higher explicit reciprocity laws, Ann. of Math. **107** (1978) 235–254.

[196] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. **141** (1995) 443–551.

[197] Y. Zarhin, p-adic heights on abelian varieties, Séminaire de Théorie des Nombres, Paris 1987-1988, Prog. in Math. **81**, Birkhäuser, 1989.

Pierre COLMEZ

Institut de mathématiques de Jussieu
4 place Jussieu
75005 PARIS
E-mail : `colmez@math.jussieu.fr`