Classes des corps surcirculaires et des corps de fonctions*

Jean-François Jaulent & Alexis Michel

Résumé. Nous nous intéressons aux formules de translation du genre à la Riemann-Hurwitz obtenues par plusieurs auteurs pour les corps de fonctions ou les $\mathbb{Z}_\ell$-extensions cyclotomiques de corps de nombres. Nous prouvons en particulier que toutes ces formules, y compris celles énoncées à la Chevalley-Weil en termes de représentations, résultent identiquement pour des raisons purement algébriques du calcul arithmétique d'un quotient de Herbrand convenable qu'il suffit de mener dans le cas cyclique de degré premier. En appendice, nous montrons qu'elles valent encore pour certaines extensions non galoisiennes.

Abstract. We are interested in Riemann-Hurwitz formulas about the genus or the Hasse-Witt invariant of function fields and the minus part of the Iwasawa lambda invariant of cyclotomic $\mathbb{Z}_\ell$-fields. We prove that all these formulas (including the Chevalley-Weil ones in terms of Galois representations) do follow by purely algebraic arguments from the arithmetic computation of a convenient Herbrand quotient in the cyclic case of prime degree ℓ. In the appendix, we show how our proof is still valid in certain non-Galois cases.

Introduction

On sait, depuis les travaux essentiels d'Iwasawa sur les corps cyclotomiques, qu'il existe des anaogies remarquables entre ℓ-groupes de classes des corps surcirculaires[1] relatifs à un premier donné ℓ et les ℓ-groupes de classes de diviseurs d'un corps de fonctions, l'exemple le plus éclairant étant probablement le parallèle formel rigoureux entre la formule de translation de Kuz'min-Kida sur l'invariant λ^- des corps surcirculaires et le célèbre théorème de Deuring-Šafarevič, qui généralise la classique identité de Riemann-Hurwitz sur le genre des corps de fonctions.

Sous leur forme la plus élémentaire, ces deux résultats peuvent, en effet, s'énoncer respectivement comme suit :

Formule 1 (Kuz'min [Ku], Kida [Ki$_1$]). *Soit N/K une ℓ-extension cyclique élémentaire de corps surcirculaires à conjugaison complexe (en ce sens que K est une extension quadratique totalement imaginaire d'un sous-corps totalement réel K_+ et que N provient, par composition avec K, d'une ℓ-extension cyclique élémentaire totalement réelle N_+ de K_+) satisfaisant la conjecture d'Iwasawa ($\mu_K = \mu_N = 0$). Dans ce cas, les invariants λ^- attachés aux ℓ-groupes de classes imaginaires sont liés par l'identité :*

$$\lambda_N^- - \delta \;=\; [N:K](\lambda_K^- - \delta) + \sum_{\mathfrak{p}^-} (d_{\mathfrak{p}}(N/K) - 1).$$

*Sém. Théor. Nombres Paris 1989–1990, Prog. in Math. **102** (1992), 141–162.

[1] Un corps surcirculaire est la $\mathbb{Z}_\ell$-extension cyclotomique d'un corps de nombres.

Dans celle-ci $d_{\mathfrak{p}}(N/K) = [N_{\mathfrak{p}} : K_{\mathfrak{p}}]$ *désigne le degré local ; la sommation porte sur les places de* K_+ *décomposées dans* K/K_+ *; et* δ *vaut 1 ou 0, suivant que* K *contient ou non les racines* 2ℓ*-ièmes de l'unité.*

Formule 2 (Deuring [Deu], Šafarevič [Ša]). *Soit* N/K *une* ℓ*-extension cyclique élémentaire de corps de fonctions d'une variable sur un corps des constantes algébiquement clos de caractéristique arbitraire* p*. Dans ce cas, les codimensions* λ_N^0 *et* λ_K^0 *des* ℓ*-groupes de classes de diviseurs de degré nul attachés à* N *et à* K *sont liés par l'identité :*

$$\lambda_N^0 - \delta \;=\; [N:K](\lambda_K^0 - \delta) + \sum_{\mathfrak{p}} (d_{\mathfrak{p}}(N/K) - 1),$$

Dans celle-ci $d_{\mathfrak{p}}(N/K) = [N_{\mathfrak{p}} : K_{\mathfrak{p}}]$ *désigne encore le degré local ; la sommation porte sur toutes les places de* K *; et* δ *vaut 1 ou 0, suivant que* K *contient ou non les racines* 2ℓ*-ièmes de l'unité.*

De plus, d'après D'Mello et Madan (cf. [DM]), le même résultat vaut identiquement lorsque le corps des constantes k *n'est plus un corps algébriquement clos mais la* $\mathbb{Z}_\ell$*-extension d'un corps fini* $\mathbb{F}_q$*.*

Dans l'un ou l'autre cas les hypothèses faites excluent toute possibilité d'inertie (à l'exception notable des places au-dessus de ℓ dans le cas surcirculaire) et les degrés locaux $d_{\mathfrak{p}}(N/K)$ se réduisent aux seuls indices d'inertie $e_{\mathfrak{p}}(N/K)$ (ce qui redonne les formulations plus traditionnelles de ces résultats), sauf dans le cas surcirculaire où la formule de Kuz'min diffère sensiblement de celle de Kida pour les raisons exposées dans [Ja$_6$] sur lesquelles nous reviendrons plus loin.

Sous cette forme élémentaire, les résultats énoncés contiennent en fait le cas le plus général, puisque toute ℓ-extension (galoisienne) s'obtient évidemment par empilement d'extensions élémentaires. Plus précisément, ils peuvent alors s'énoncer en termes de représentations à la Chevalley-Weil, comme suit :

Formule 1$^{\text{bis}}$ (Iwasawa [Iw$_2$], Jaulent [Ja$_6$]). *Soit* N/K *une* ℓ*-extension (galoisienne) de corps surcirculaires à conjugaison complexe (en ce sens que* K *est une extension quadratique totalement imaginaire d'un sous-corps totalement réel* K_+ *et que* N *provient, par composition avec* K*, d'une* ℓ*-extension (galoisienne) totalement réelle* N_+ *de* K_+*) satisfaisant la conjecture d'Iwasawa (*$\mu_K = \mu_N = 0$*). Dans ce cas, le caractère* χ_N^- *de la représentation galoisienne associée au* $\mathbb{Q}_\ell$*-espace vectoriel* $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} X_N^-$ *construit sur le* $\mathbb{Z}_\ell$*-module des formes entières* $X_N^- := \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{C}\ell_N^{-\,*}, \mathbb{Z}_\ell)$ *sur le dual de Pontrjagin* $\mathcal{C}\ell_N^{-\,*} := \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{C}\ell_N^-, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$ *du* ℓ*-groupe des* ℓ*-classes imaginaires du corps* N *est donné par la formule :*

$$\chi_N^- - \delta\, 1_G \;=\; (\lambda_K^- - \delta)\ \mathrm{Rég}_G + \sum_{\mathfrak{p}^-} \mathrm{Ind}_{D_{\mathfrak{p}}}^G(\mathrm{Aug}_{D_{\mathfrak{p}}}).$$

Dans celle-ci $\mathrm{Rég}_G$ *désigne le caractère régulier du groupe* $G = \mathrm{Gal}(N/K)$ *;* 1_G *est le caractère unité ;* $\mathrm{Ind}_{D_{\mathfrak{p}}}^G(\mathrm{Aug}_{D_{\mathfrak{p}}})$ *est l'induit à* G *du caractère d'augmentation du sous-groupe de décomposition*[2] $D_{\mathfrak{p}}$ *; la sommation porte sur les places de* K_+ *décomposées dans* K/K_+ *; et les indices* λ_K^- *et* δ *sont définis comme plus haut.*

Formule 2$^{\text{bis}}$ (Gold & Madan [GM$_3$]). *Soit* N/K *une* ℓ*-extension (galoisienne) de corps de fonctions d'une variable sur un corps des constantes algébiquement clos de caractéristique arbitraire* p*. Dans ce cas, le caractère* χ_N *de la représentation associée au* $\mathbb{Q}_\ell$*-espace vectoriel* $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} X_N$ *construit sur le module des* $\mathbb{Z}_\ell$*-formes* $X_N := \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{C}\ell_N^{0\,*}, \mathbb{Z}_\ell)$ *sur le dual de Pontrjagin* $\mathcal{C}\ell_N^{0\,*} := \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{C}\ell_N^0, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$

[2] Contrairement à $D_{\mathfrak{p}}$, le caractère $\mathrm{Ind}_{D_{\mathfrak{p}}}^G(\mathrm{Aug}_{D_{\mathfrak{p}}})$ est indépendant de la place au-dessus de $\mathfrak{p}$.

du ℓ-groupe des ℓ-classes de diviseurs de degré nul attaché à N est donné par la formule :

$$\chi_N - \delta\, 1_G \;=\; (\lambda_K - \delta)\ \mathrm{Rég}_G + \sum_{\mathfrak{p}} \mathrm{Ind}_{D_\mathfrak{p}}^G(\mathrm{Aug}_{D_\mathfrak{p}}).$$

Dans celle-ci $\mathrm{Rég}_G$ désigne le caractère régulier du groupe $G = \mathrm{Gal}(N/K)$; 1_G est le caractère unité ; $\mathrm{Ind}_{D_\mathfrak{p}}^G(\mathrm{Aug}_{D_\mathfrak{p}})$ est l'induit à G du caractère d'augmentation du sous-groupe de décomposition $D_\mathfrak{p}$; la sommation porte sur les places de K_+ décomposées dans K/K_+ ; et les indices λ_K et δ sont définis comme plus haut.

Ici encore, le même résultat vaut identiquement lorsque le corps des constantes k n'est plus un corps algébriquement clos mais la $\mathbb{Z}_\ell$-extension d'un corps fini $\mathbb{F}_q$.

Nous nous proposons d'expliquer ici pourquoi ces diverses formulations, les unes en termes de codimension, les autres en termes de caractères, se déduisent les unes des autres de façon élémentaire en dépit de leur apparente hiérarchie, et d'en donner une démonstration algébrique succinte qui vaille dans chacun des cas considérés et indépendamment de la parité de ℓ.

1. Un peu d'histoire

La situation originelle est évidemment celle des corps de fonctions ou, pour parler le langage de la géométrie, celle des surfaces de Riemann complexes : sous sa forme primitive, le théorème de Riemann-Hurwitz (cf. [Hur]) affirme, en effet, que si X est un revêtement à ℓ feuillets d'une surface de Riemann compacte connexe Y, ramifié en d points $P_1, \ldots, P_d$, d'indices de ramification respectifs $e_{P_1}, \ldots, e_{P_d}$, le genre g_X de X est donné en fonction de celui g_Y de Y par la formule :

$$2g_X - 2 \;=\; \ell(2g_Y - 2) + \sum_{P_i} (e_{P_i} - 1).$$

Plus généralement maintenant, si N/K est une extension séparable de degré fini ℓ de corps de fonctions d'une variable sur un corps algébriquement clos k, la formule précédente pour les courbes algébriques complètes non singulières, disons X et Y, respectivement associées à N et à K, s'écrit encore :

$$2g_X - 2 \;=\; \ell(2g_Y - 2) + \deg R_{X/Y}.$$

où $R_{X/Y} := \sum_{P \in X} \mathrm{long}(\Omega_{X/Y})_P P$ est le diviseur construit sur le faisceau des différentielles relatives $\Omega_{X/Y}$; et la quantité $\mathrm{long}(\Omega_{X/Y})_P$ est égale à $e_P - 1$ en tout point où la ramification est modérée, mais strictement plus grande sinon.

Lorsque maintenant ℓ est un nombre premier différent de la caractéristique p, le double du genre $2g$ n'est autre que la codimension sur $\mathbb{Z}_\ell$, disons λ, du ℓ-groupe $\mathcal{C}\ell^0$ des classes de diviseurs de degré nul du corps considéré ; et, la ramification étant alors automatiquement modérée, la formule de Riemann-Hurwitz prend bien la forme (2) de l'introduction. Pour $\ell = p$, en revanche, la situation se complique du fait des possibilités de ramification sauvage d'abord, et parce que la codimension λ du ℓ-groupe $\mathcal{C}\ell^0$ n'est plus le double du genre mais l'invariant de Hasse-Witt de la courbe associée. Dans ce cas, la formule (2) a été établie d'abord par Deuring en 1936 (cf. [Deu]) sans condition sur ℓ, mais dans le cas particulier où l'extension N/K est (totalement) ramifiée, puis par Šafarevič en 1952 pour $\ell = p$ dans le cas non ramifié. Quelque vingt ans après, Subrao (cf. [Su]) a produit une preuve valable pour $\ell = p$ indépendamment de la ramification et, deux ans plus tard, Madan (cf. [Ma]), reprenant les idées de Deuring, a montré que les erreurs manifestes contenues dans son article pouvaient être aisément corrigées pour aboutir à une démonstration unifiée des différents cas.

D'un autre côté, l'étude des $\mathbb{Z}_\ell$-extensions de corps de nombres a été inaugurée par Iwasawa dans une longue série de travaux publiés entre 1958 et 1973, dont l'article [Iw_1] constitue une première synthèse. Le point essentiel qui nous intéresse ici est que sous la conjecture d'Iwasawa (qui postule que les ℓ-rangs des groupes de classes attachés aux étages finis d'une $\mathbb{Z}_\ell$-extension restent bornés lorsqu'on monte la tour), le ℓ-groupe des classes d'idéaux (au sens ordinaire) d'une telle $\mathbb{Z}_\ell$-extension est un $\mathbb{Z}_\ell$-module divisible de codimension finie dont l'arithmétique présente des analogies troublante avec celle des ℓ-groupes de classes des corps de fonctions. Malheureusement, la conjecture d'Iwasawa n'est établie à ce jour que pour les $\mathbb{Z}_\ell$-extensions cyclotomiques des corps abéliens (c'est-à-dire, en fait, pour les $\mathbb{Z}_\ell$-corps absolument abéliens ; c'est le théorème de Ferrero et Washington) et l'on sait qu'elle peut être en défaut lorsqu'on considère des $\mathbb{Z}_\ell$-extensions non cyclotomiques ; ce qui justifie amplement que l'on se restreigne ici au cas des corps surcirculaires (i.e. des $\mathbb{Z}_\ell$-extensions des corps de nombres).

C'est dans ce contexte que Kida, en 1981, publia une formule reliant les invariants λ des ℓ-groupes de classes imaginaires (et cette restriction est essentielle, commme nous le verrons plus loin) dans une ℓ-extension (galoisienne) de corps surcirculaires à conjugaison complexe, identique à celle (1) donnée plus haut, si ce n'est qu'elle ne fait pas intervenir les places au-dessus de ℓ (cf. [Ki_1, Ki_2]). Deux ans auparavant cependant, mais dans un article passé inaperçu (cf. [Ku]), Kuz'min avait produit une formule analogue pour les ℓ-groupes de ℓ-classes (i.e. pour les quotients de ℓ-groupes de classes au sens ordinaire par leurs sous-groupes respectifs construits sur les places au-dessus de ℓ). Ultérieurement, Wingberg (cf. [W_2]) montra qu'un résultat semblable valait encore pour les ℓ-groupes de classes infinitésimales (au sens de [Ja_4]) des corps surcirculaires totalement réels. De fait, comme expliqué dans [Ja_6], les résultats de Jaulent (cf. [Ja_5]) montrent que les paramètres d'Iwasawa attachés à ces différents groupe se déduisent aisément les uns des autres par des formules standard ne faisant intervenir que des invariants galoisiens simples des corps considérés. Nous avons choisi ici la formule donnée par Kuz'min, d'une part parce que c'est celle qui préserve le mieux le parallèle avec les corps de fonctions, d'autre part parce que d'autres considérations (notamment l'existence discutée dans [Ja_7] d'un accouplement de Weil) suggèrent que ce sont bien les ℓ-groupes de ℓ-classes des corps surcirculaires qui correspondent le mieux aux ℓ-groupes de classes de diviseurs de degré nul des corps de fonctions.

Bien antérieurement à ces travaux sur les corps surcirculaires, la formule de Deuring et Šafarevič avait été réinterprétée en termes galoisiens : dès 1934, en effet, Chevalley et Weil avaient déterminé le caractère de l'action du groupe de Galois d'un revêtement sur l'espace des différentielles de première espèce et généralisé par là-même la formule de Riemann-Hurwitz en un théorème de représentation (cf. [CW]). Peu après le résultat de Kida, Iwasawa montra donc dans le même esprit que la formule obtenue par celui-ci pouvait également s'écrire en termes de caractères, ce qui en constituait d'ailleurs une nouvelle démonstration (cf. [Iw_2]). Transposée dans le cadre légèrement différent des groupes de ℓ-classes, c'est la formule (1^{bis}) telle qu'énoncée par Jaulent[3] en 1986 (cf. [Ja_6]). La même année, Gold et Madan montraient qu'il en allait de même dans le cas des corps de fonctions et généralisaient le théorème de Deuring et Šafarevič en déterminant explicitement le caractère de la représentation modulaire donnée par le ℓ-groupe des classes de diviseurs de degré 0, ce qui, traduit en termes de représentations ℓ-adiques, conduit à la formule (2^{bis}) (cf. [GM_3]). Simultanément, ils produisaient une preuve unifiée de l'ensemble de ces formules (cf. [GM_2]), très voisine de l'une des démonstrations données indépendamment dans [Ja_6]. Enfin, tout récemment Wingberg (cf. [W_2]) a prouvé qu'une

[3] Page 146, après correction de l'erreur de signe manifeste contenue dans l'énoncé de [Ja_6].

identité de représentations analogue s'applique également aux groupes de Selmer de certaines courbes elliptiques à multiplication complexe.

Pour compléter ce tour d'horizon, sans doute faut-il dire un mot des méthodes analytiques dont nous avons peu parlé jusqu'ici. Les preuves analytiques de la formule de Kuz'min-Kida reposent évidemment sur la correspondance établie par Iwasawa entre fonctions L et invariants λ. La plus ancienne est celle obtenue par Gras (cf. [Gr_2]) pour les corps absolument abéliens, qui utilise les fonctions L ℓ-adiques de Kubota-Leopoldt. L'étude du cas général est l'œuvre de Sinnot (cf. [Sin]) et repose sur la notion de pseudo-mesure ℓ-adique introduite par Serre. Tout récemment, Gold et Madan (cf. [GM_4]) ont appliqué les méthodes de Sinnot dans un cadre non abélien pour généraliser les résultats de Rück (cf. [Rü]) sur les corps de fonctions ; nous y reviendrons en appendice.

2. Réduction algébrique au cas cyclique élémentaire

Dans chacun des deux cas fondamentaux considérés, des considérations arithmétiques permettent d'associer à un corps K un $\mathbb{Z}_\ell$-module divisible de codimension finie, que nous noterons $\mathcal{C}\ell_K^0$ ou $\mathcal{C}\ell_K^-$ suivant le contexte, à savoir :

- le ℓ-groupe des classes de diviseurs de degré nul $\mathcal{C}\ell_K^0$, si K est un corps de fonctions d'une variable sur un corps algébriquement clos ou sur la $\mathbb{Z}_\ell$-extension d'un corps fini ;
- le ℓ-groupe des classes de ℓ-diviseurs, i.e. le le quotient du ℓ-groupe des classes de diviseurs au sens ordinaire par le sous-groupe construit sur les places au-dessus de ℓ, si K est un corps surcirculaire (i.e. la $\mathbb{Z}_\ell$-extension cyclotomique d'un corps de nombres).

En fait, dans ce dernier cas, on est amené à se restreindre à la composante imaginaire du ℓ-groupe des ℓ-classes et cela pour deux excellentes raisons : d'abord, parce que la composante réelle étant conjecturalement nulle, l'intérêt d'une formule de translation pour les classes réelles n'est pas évident ; ensuite et plus concrètement, parce qu'on est de fait dans l'incapacité d'établir une telle formule, faute de maîtriser convenablement la cohomologie des unités.

Le cas $\ell = 2$ étant particulier, disons un mot rapide sur la définition des groupes $\mathcal{C}\ell_K^-$: lorsque le corps considéré admet une conjugaison complexe τ (i.e. lorsque K est une extension quadratique totalement imaginaire d'un corps surcirculaire totalement réel K_+), celle-ci permet de définir deux idempotents orthogonaux

$$e_+ \;:=\; \tfrac{1}{2}\,(1+\tau) \qquad \text{et} \qquad e_- \;:=\; \tfrac{1}{2}\,(1-\tau)$$

de l'algèbre $\mathbb{Z}_\ell[\mathrm{Gal}(K/K_+)]$. Si ℓ est impair, ceux-ci ont leurs coefficients dans l'anneau $\mathbb{Z}_\ell$ et tout $\mathbb{Z}_\ell$-module galoisien M s'écrit canoniquement comme somme directe

$$M \;=\; M^+ \oplus M^-$$

de ses composantes réelle $M^+ := M^{e_+}$ et imaginaire $M^- := M^{e_-} \simeq M/M^+$. Si ℓ vaut 2, on pose simplement $M^- := M/M^+$, ce qui, appliqué avec $M = \mathcal{C}\ell_K$, définit dans tous les cas un $\mathbb{Z}_\ell$-module divisible de codimension finie.

Cela fait, à chacun des modules $\mathcal{C}\ell_K^0$ (resp. $\mathcal{C}\ell_K^-$) on sait associer canoniquement un $\mathbb{Q}_\ell$-espace vectoriel V_K^0 (resp. V_K^-) de dimension finie λ_K^0 (resp. λ_K^-) et un $\mathbb{Z}_\ell$-réseau X_K^0 (resp. X_K^-) de V_K^0 (resp. de V_K^-) tels qu'on ait :

$$\mathcal{C}\ell_K^0 \;\simeq\; V_K^0/X_K^0 \qquad \text{resp.} \qquad \mathcal{C}\ell_K^- \;\simeq\; V_K^-/X_K^-.$$

Il suffit, en effet, de prendre par exemple pour X_K^0 le module des formes linéaires entières $\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{C}\ell_K^{0\,*}, \mathbb{Z}_\ell)$ sur le dual de Pontrjagin $\mathcal{C}\ell_K^{0\,*} := \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{C}\ell_K^0, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$ de

$\mathcal{C}\ell_K^0$ et pour V_K^0 le $\mathbb{Q}_\ell$-espace vectoriel $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} X_K^0$ construit sur X_K^0 ; auquel cas les isomorphismes de dualité donnent, comme attendu :

$$V_K^0/X_K^0 \;\simeq\; \mathbb{Q}_\ell/\mathbb{Z}_\ell \otimes_{\mathbb{Z}_\ell} \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{C}\ell_K^{0\,*}, \mathbb{Z}_\ell) \;\simeq\; \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{C}\ell_K^{0\,*}, \mathbb{Q}_\ell/\mathbb{Z}_\ell) \;\simeq\; \mathcal{C}\ell_K^0.$$

Si maintenant N/K est une ℓ-extension (galoisienne) de groupe G, le module divisible $\mathcal{C}\ell_N$ (et donc l'espace associé V_N) est canoniquement un module galoisien. Plus précisément dans ce cas, l'extension des diviseurs de K à N induit par passage au quotient un morphisme naturel à noyau et conoyau finis du ℓ-groupe des classes $\mathcal{C}\ell_K$ dans le sous-groupe des points fixes $\mathcal{C}\ell_N^G$ de $\mathcal{C}\ell_N$; puis, par la construction précédente, un isomorphisme canonique du $\mathbb{Q}_\ell$-espace V_K sur le sous-espace fixe V_N^G de V_N, ce qui permet d'identifier $V_{N^G} = V_K$ à V_N^G. Autrement dit, les espaces V satisfont la théorie de Galois.

Ce point acquis, il est facile de voir que, pour calculer le caractère de G associé à V_N, il suffit de déterminer les dimensions respectives des sous-groupes des points fixes $V_N^H = V_{N^H}$ pour tous les sous-groupes H de G, c'est-à-dire finalement les codimensions respectives des $\mathbb{Z}_\ell$-modules divisibles $\mathcal{C}\ell_L$ pour chaque sous-extension L/K de N/K : en effet, l'égalité de deux caractères se lisant sur les éléments du groupe G, et la valeur d'un caractère en un élément donné de G se calculant dans le sous-groupe cyclique engendré par cet élément, ce n'est pas restreindre la généralité que raisonner dans le cas très particulier où G est cyclique, disons d'ordre ℓ^m. Or, dans ce cas, la décomposition

$$\mathbb{Q}_\ell[G] \;\simeq\; \mathbb{Q}_\ell[X]/(X^{\ell^m} - 1) \;\simeq\; \bigoplus_{i=0}^{m} \mathbb{Q}_\ell[X]/(\phi_{\ell^i}(X)) \;\simeq\; \bigoplus_{i=0}^{m} \mathbb{Q}_\ell[\zeta_{\ell^i}]$$

de l'algèbre $\mathbb{Q}_\ell[G]$ comme produit de corps cyclotomiques montre que le caractère régulier

$$\mathrm{Rég}_G = \sum_{i=0}^{m} \chi_i$$

est la somme de $m+1$ caractères irréductibles de degrés respectifs $\deg \chi_i = \varphi(\ell^i)$ pour $i = 0, \ldots, m$. Par suite, si $M = M_m$ est un $\mathbb{Q}_\ell[G]$-module de caractère

$$\chi_M = \sum_{i=0}^{m} n_i \chi_i,$$

et G_k l'unique sous-groupe d'indice ℓ^k de G (pour $k = 0, \ldots, m$), la décomposition

$$\chi_{M_k} = \sum_{i=0}^{k} n_i \chi_i,$$

du caractère du sous-module $M_k := M^{G_k}$ des points de M fixes par G_k, les équations aux dimensions qui en résultent

$$\deg \chi_{M_k} = \sum_{i=0}^{k} n_i \, \varphi(\ell^i),$$

montrent que les $m+1$ entiers n_i (pour $k = 0, \ldots, m$) sont entièrement déterminés par les dimensions respectives $\dim_{\mathbb{Q}_\ell} M_k = \deg \chi_{M_k}$ des $m+1$ sous-espaces M_k.

Appliqué au problème qui nous intéresse, ce résultat nous dit alors que la validité des formules (1^{bis}) et (2^{bis}) se vérifie en constatant qu'elles conduisent aux bons degrés pour toutes les sous-extensions L/K de N/K, ce qui résulte clairement des formules (1) et (2) par empilement de ℓ-extensions cycliques élémentaires.

Reste donc à établir les formules (1) et (2) dans le cas cyclique élémentaire.

Or, si G est un groupe d'ordre ℓ, on sait par un résultat de Rosen (cf. [Ro, Ja$_2$, Ja$_3$]) que tout $\mathbb{Z}[G]$-module noethérien $\mathbb{Z}_\ell$-projectif s'écrit de façon essentiellement unique comme somme directe de $\mathbb{Z}[G]$-modules indécomposables sous la forme :

$$M^* \ \simeq \ {\mathbb{Z}_\ell}^\alpha \oplus \mathbb{Z}_\ell[\zeta]^\beta \oplus Zl[G]^\gamma \ .$$

Une autre fmanière d'énoncer ce résultat consiste à dire par dualité que tout $\mathbb{Z}[G]$-module de cotype fini $\mathbb{Z}_\ell$-divisible s'écrit de façon essentiellement unique comme somme directe de $\mathbb{Z}[G]$-modules indécomposables sous la forme :

$$M \ \simeq \ (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^\alpha \oplus (\mathbb{Q}_\ell[\zeta]/\mathbb{Z}_\ell[\zeta])^\beta \oplus (\mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell[G]^\gamma \ .$$

Un calcul immédiat montre alors que l'on a :

$$M^G \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\alpha+\gamma} \ ; \qquad H^1(G,M) \simeq {\mathbb{F}_\ell}^\alpha \ ; \qquad H^2(G,M) \simeq {\mathbb{F}_\ell}^\beta$$

En particulier :

(i) $\alpha+\gamma = \mathrm{codim}_{\mathbb{Z}_\ell} M^G$ est la codimension du module des points fixes M^G et

(ii) $\beta-\alpha = \dim_{\mathbb{F}_\ell} H^1(G,M) - \dim_{\mathbb{F}_\ell} H^2(G,M) = q(G,M)$ est le *quotient de Herbrand dimensionnel* du module M.

Maintenant, le caractère du $\mathbb{Q}_\ell[G]$-module V associé à M est donné par l'identité :

$$\chi_M \ = \ \alpha\, 1_G + \beta\ \mathrm{Aug}_G + \gamma\ \mathrm{Rég}_G \ = \ (\alpha+\gamma)\ \mathrm{Rég}_G + (\beta-\alpha)\ \mathrm{Aug}_G \ ;$$

c'est-à-dire finalement :

$$\chi_M \ = \ \mathrm{codim}_{\mathbb{Z}_\ell} M^G\ \mathrm{Rég}_G + q(G,M)\ \mathrm{Aug}_G \ ;$$

d'où, en termes de degrés :

$$\mathrm{codim}_{\mathbb{Z}_\ell} M \ = \ \ell\, \mathrm{codim}_{\mathbb{Z}_\ell} M^G + (\ell-1)\, q(G,M).$$

Revenant alors aux formules de Deuring-Šafarevič et de Kuz'min-Kida citées dans l'introduction et prenant pour M le groupe $\mathcal{C}\ell_N^0$ (respectivement le groupe $\mathcal{C}\ell_N^-$), nous voyons que tout le problème consiste en fin de compte à évaluer le quotient de Herbrand dimensionnel correspondant $q(G,\mathcal{C}\ell_N^0)$ (resp. $q(G,\mathcal{C}\ell_N^-)$) dans une ℓ-extension cyclique élémentaire, ce qui relève de l'arithmétique des corps de fonctions (resp. des corps surcirculaires).

3. Étude arithmétique du cas cyclique élémentaire

De façon générale, le calcul du quotient de Herbrand d'un $\mathbb{Z}_\ell[G]$-module repose sur deux lemmes de Herbrand (cf. [Her]) que l'on peut énoncer dimensionnellement comme suit :

Lemme de Herbrand. *Soit G un ℓ-groupe cyclique élémentaire. Alors :*

(i) Pour toute suite exacte courte $1 \to D \to N \to Q \to 1$ de $\mathbb{Z}_\ell[G]$-modules, les quotients de Herbrand des trois termes sont définis dès que deux d'entre eux le sont, auquel cas on a l'identité :

$$q(G,D) - Q(G,N) + q(G,Q) = 0.$$

(ii) le quotient de Herbrand dimlensionnel d'un $\mathbb{Z}_\ell[G]$-module fini est nul.

Du point de vue théorique, ces deux résultats montrent clairement que le quotient de Herbrand d'un $\mathbb{Z}_\ell[G]$-module M ne dépend que de la classe de ce module dans un groupe de Grothendieck convenable, que l'on laisse le soin au lecteur de préciser. Du point de vue pratique, l'assertion (i) interprète le quotient de Herbrand d'un quotient $Q = N/D$ comme différence des quotients de Herbrand respectifs de son numérateur N et de son dénominateur D ; et l'assertion (ii) permet de remplacer, chaque fois qu'on le souhaite, un module donné par un autre qui lui est pseudo-isomorphe (ce qui réduit à néant les difficultés particulières survenant pour $\ell = 2$ dans le cas surcirculaire).

Or, dans chacun des deux cas fondamentaux qui nous intéressent , le ℓ-groupe des classes étudié se présente de façon naturelle comme un quotient :

(i) Si N est un corps de fonctions d'une variable sur un corps des constantes k qui est algébriquement clos ou $\mathbb{Z}_\ell$-extension d'un corps fini), le ℓ-groupe $\mathcal{C}\ell_N^0$ est, par définition, le quotient du tensorisé $\mathcal{D}\ell_N^0 := \mathbb{Z}_\ell \otimes_{\mathbb{Z}} D_N^0$ du groupe des diviseurs de degré nul par son sous-groupe principal $\mathcal{P}\ell_N^0 := \mathbb{Z}_\ell \otimes_{\mathbb{Z}} P_N^0$.

(ii) Si N est un corps surcirculaire à conjugaison complexe τ (extension quadratique totalement imaginaire d'un sous-corps surcirculaire totalement réel N_+), le ℓ-groupe des ℓ-classes de diviseurs $\mathcal{C}\ell_N$ est le quotient du tensorisé $\mathcal{D}\ell_N := \mathbb{Z}_\ell \otimes_{\mathbb{Z}} Dl_N$ du groupe des ℓ-diviseurs[4] de N par son sous-groupe principal $\mathcal{P}\ell_N := \mathbb{Z}_\ell \otimes_{\mathbb{Z}} Pl_N$; et le le ℓ-groupe des ℓ-classes imaginaires est, par définition, le quotient $\mathcal{C}\ell_N^- := \mathcal{C}\ell_N/\mathcal{C}\ell_N^{1+\tau} \simeq \mathcal{D}\ell_N/\mathcal{D}\ell_N^{1+\tau}\mathcal{P}\ell_N$.

Une observation s'impose ici :

– si ℓ est impair, 2 est inversible dans $\mathbb{Z}_\ell$ et, comme τ est l'identité sur $\mathcal{D}\ell_{N_+}$, l'opérateur norme $N_{N/N_+} = 1 + \tau$ envoie surjectivement $\mathcal{D}\ell_N$ sur $\mathcal{D}\ell_{N_+}$;

– si ℓ vaut 2, la montée dans la $\mathbb{Z}_2$-extension cyclotomique ayant épuisé toute possibilité d'inertie aux places étrangères à 2, la norme N_{N/N_+} est encore surjective de $\mathcal{D}\ell_N$ dans $\mathcal{D}\ell_{N_+}$;

En fin de compte, dans les deux cas, il vient :

$$\mathcal{C}\ell_N^- \simeq \mathcal{D}\ell_N/\mathcal{D}\ell_{N_+}\mathcal{P}\ell_N \simeq (\mathcal{D}\ell_N/\mathcal{D}\ell_{N_+})/(\mathcal{P}\ell_N/(\mathcal{P}\ell_N \cap \mathcal{D}\ell_{N_+})).$$

Maintenant, le groupe $\mathcal{P}\ell_N/(\mathcal{P}\ell_N \cap \mathcal{D}\ell_{N_+})$, qui mesure la capitulation dans l'extension N/N_+, est fini sous la conjecture d'Iwasawa : en effet, son exposant est borné par le degré 2 de l'extension et son rang par la codimention de $\mathcal{C}\ell_{N_+}$ (bien entendu, il est nul pour ℓ impair). Raisonnant à pseudo-isomorphisme près, nous écrirons donc, sans plus de précaution :

$$\mathcal{C}\ell_N^- \sim (\mathcal{D}\ell_N/\mathcal{D}\ell_{N_+})/(\mathcal{P}\ell_N/(\mathcal{P}\ell_{N_+}).$$

Ce point acquis, examinons successivement numérateurs et dénominateurs :

1er point : cohomologie des diviseurs

Le calcul du quotient de Herbrand des numérateurs repose tout entier sur le lemme :

Lemme 1. *Dans une ℓ-extension cyclique élémentaire L/H de corps surcirculaires ou de fonctions la cohomologie des ℓ-groupes de diviseurs relativement au groupe $G = \mathrm{Gal}(L/H)$ est donnée par les formules :*

(i) $H^1(G, \mathcal{D}\ell_L) = 1$, dans chacun des deux cas fondamentaux.

(ii) $H^2(G, \mathcal{D}\ell_L) = {\mathbb{F}_\ell}^t$, où t est soit le nombre de diviseurs premiers ramifiés (dans le cas des corps de fonctions), soit le nombre de premiers ramifiés mais étrangers à ℓ (dans le cas surcirculaire).

[4] Un ℓ-diviseur est ici un idéal de l'anneau des ℓ-entiers de N.

Preuve. L'assertion (i) est exactement le théorème 90 de Hilbert ; l'assertion (ii) résulte de l'isomorphisme $H^2(G, \mathcal{D}\ell_L) \simeq \mathcal{D}\ell_L^G / N_{L/H}(\mathcal{D}\ell_L)$, puisque les hypothèses faites, qui excluent toute inertie (en dehors de ℓ), assurent la surjectivité de la norme : $N_{L/H}(\mathcal{D}\ell_L) = \mathcal{D}\ell_H$.

Corollaire. *Dans les deux cas fondamentaux étudiés, il vient ainsi :*

(a) $q(G, \mathcal{D}\ell_N^0) = t_{N/K} - 1$*, où* $t_{N/K}$ *est le nombre de ramifiés dans* N/K*.*

(b) $q(G, \mathcal{D}\ell_N^-) = t_{N/K}^-$*, où* $t_{N/K}^-$ *est le nombre de diviseurs premiers de* K_+ *qui sont étrangers à* ℓ*, ramifiés dans* N/K *et décomposés dans* K/K_+*.*

Preuve. Dans le cas des corps de fonctions, le ℓ-groupe $\mathcal{D}\ell_N^0$ des diviseurs de degré nul est le noyau du morphisme degré $\deg : \mathcal{D}\ell_N \to \mathbb{Z}_\ell$. L'application directe du lemme à l'extension N/K donne alors le résultat annoncé :

$$q(G, \mathcal{D}\ell_N^0) = q(G, \mathcal{D}\ell_N) - q(G, \mathbb{Z}_\ell) = t_{N/K} - 1$$

Enfin, dans le cas surcirculaire, l'application du lemme successivement aux extensions N/K et N_+/K_+ donne bien :

$$q(G, \mathcal{D}\ell_N/\mathcal{D}\ell_N^+) = q(G, \mathcal{D}\ell_N/\mathcal{D}\ell_N) - q(G, \mathcal{D}\ell_N^+) = t_{N/K} - t_{N_+/K_+} = t_{N/K}^-.$$

2e point : cohomologie des diviseurs principaux

Le point principal est ici que la cohomologie des diviseurs principaux est duale de celle des "unités" :

Lemme 2. *Dans une* ℓ*-extension cyclique élémentaire* L/H *de corps surcirculaires ou de fonctions, le groupe multiplicatif* $L^\times$ *est cohomologiquement trivial. Le groupe des "unités"* U_L *et le groupe des diviseurs principaux* $P_L \simeq L^\times/U_L$ *sont donc en dualité cohomologique.*

Preuve. Ici encore, l'identité $H^1(G, L^\times) = 1$ n'est autre que le théorème 90 de Hilbert. Quant à l'identité, $H^2(G, L^\times) = 1$, elle affirme simplement la surjectivité de la norme : $H^\times = N_{L/H}(L^\times)$.

Dans le cas des corps de fonctions sur un corps algébriquement clos, cette surjectivité résulte du théorème de Tsen (cf. [La, Tse]) : un tel corps est, en effet, C^1, ce qui implique que son groupe de Brauer est nul (cf. [Ser], §7, Prop. 10).

Dans les autres cas (celui des corps de fonctions dont le corps des constantes est la $\mathbb{Z}_\ell$-extension d'un corps fini, comme celui des corps surcirculaires), la surjectivité de la norme se vérifie localement par une manipulation élémentaire sur les symboles de Hasse (cf. [DM], Lem. 2 & [Ja$_6$], Lem. 4).

Cela étant, la suite exacte courte $1 \to U_L \to L^\times \to P_L \to 1$, qui définit U_L, montre que la cohomologie des groupes P_L (qui est aussi celle de leurs tensorisés $\mathcal{P}\ell_L$) est bien duale de celle des groupes U_L.

Reste maintenant à préciser la nature des groupes U_L.

(i) Dans le cas des corps de fonctions, les unités sont tout simplement les constantes non nulles. Il vient ainsi :

$$H^1(G, U_L) = H^1(G, k^\times) = {}_\ell k^\times \simeq {\mathbb{F}_\ell}^{\delta - 1}$$

où $\delta = 2$ ou 1, suivant que k contient ou non les racines ℓ-ièmes de l'unité (i.e. suivant que l'on a $p \neq \ell$ ou non), d'une part ;

$$H^2(G, U_L) = H^2(G, k^\times) = {}^\ell k^\times = k^\times / {k^\times}^\ell = 1$$

d'autre part, et tout est dit.

(*ii*) dans le cas surcirculaire, les choses sont plus complexes : les "unités" sont les unités de l'anneau des ℓ-entiers de L, c'est-à-dire ce qu'il est convenu d'appeler les ℓ-unités. Et le lemme 2, appliqué successivement avec $L = N$ et $L = N_+$, affirme que le quotient $N^\times/N_+^\times$ est cohomologiquement trivial et que, par suite, la cohomologie de $\mathcal{P}\ell_N/\mathcal{P}\ell_{N_+}$ est duale de celle de U_N/U_{N_+}.

Posons alors $\delta = 1$ ou 0, suivant que N contient ou non les racines 2ℓ-ièmes de l'unité (et donc le groupe $\boldsymbol{\mu}_{\ell^\infty}$ des racines de l'unité d'ordre ℓ-primaire). Le lemme de Herbrand nous permet d'étudier séparément le quotient $U_N/U_{N_+}\boldsymbol{\mu}_{\ell^\infty}^\delta$ d'une part, le sous-groupe $\boldsymbol{\mu}_{\ell^\infty}^\delta/(\boldsymbol{\mu}_{\ell^\infty}^\delta \cap U_{N_+}) = \boldsymbol{\mu}_{\ell^\infty}^\delta/_{\,2}\boldsymbol{\mu}_{\ell^\infty}^\delta$ d'autre part.

– Pour le second, un calcul direct donne :

$$q(G, \boldsymbol{\mu}_{\ell^\infty}^\delta/_{\,2}\boldsymbol{\mu}_{\ell^\infty}^\delta) = q(G, \boldsymbol{\mu}_{\ell^\infty}^\delta) = \delta$$

– Quant au premier, un argument de théorie de Kummer, joint au fait que les places au-dessus de ℓ sont finiment décompsées dans une $\mathbb{Z}_\ell$-extension cyclotomique, montre que l'on a :

$$U_N/U_{N_+}\boldsymbol{\mu}_{\ell^\infty}^\delta \simeq U_{\widetilde{N}}/U_{\widetilde{N}_+}\boldsymbol{\mu}_{\ell^\infty}^\delta$$

pour tout corps de nombres $\widetilde{N}$ (de degré fini sur $\mathbb{Q}$) assez gros contenu dans N (cf. [Ja$_6$], Prop. 7 pour ℓ impair, le cas $\ell = 2$, étant sans malice). Associant alors à chaque unité x de $U_{\widetilde{N}}$ l'idéal principal (x) de $Id_{\widetilde{N}}$, nous obtenons un morphisme à noyau et conoyau fini du quotient $U_{\widetilde{N}}/U_{\widetilde{N}_+}\boldsymbol{\mu}_{\ell^\infty}^\delta$ dans le sous-groupe du quotient $Id_{\widetilde{N}}/Id_{wiN_+}$ construit sur les idéaux au-dessus de ℓ. Du pseudo-isomorphisme obtenu

$$U_{\widetilde{N}}/U_{\widetilde{N}_+}\boldsymbol{\mu}_{\ell^\infty}^\delta \;\sim\; \big(\oplus_{\mathfrak{l}_d^-}\mathbb{Z}[G]\big) \oplus \big(\oplus_{\mathfrak{l}_{nd}^-}\mathbb{Z}\big),$$

où la première somme porte sur les places de K_+ au-dessus de ℓ, décomposées dans K/K_+, qui le sont aussi dans N/K, et la seconde sur celles qui ne le sont pas, nous concluons :

$$q(G, U_{\widetilde{N}}/U_{\widetilde{N}_+}\boldsymbol{\mu}_{\ell^\infty}^\delta) \;=\; \Sigma_{\mathfrak{l}_{nd}^-}\, q(G,\mathbb{Z}) \;=\; -l_{N/K}^-,$$

où $l_{N/K}^-$ compte les places au-dessus de ℓ dans K_+ qui sont décomposées dans K/K_+ mais non dans N/K.

Résumant l'ensemble de cette discussion, nous pouvons ainsi énoncer le résultat attendu :

Théorème 1. *Dans chacun des deux cas fondamentaux, les quotient de Herbrand dimensionnels respectifs du ℓ-groupe des classes de diviseurs de degré nul et du ℓ-groupe des ℓ-classes imaginaires sont donnés par :*

(i) $q(G, \mathcal{C}\ell_N^0) = (t_{N/K} - 1) - (\delta - 1) = t_{N/K} - \delta$, *où $t_{N/K}$ est le nombre de places ramifiées et δ vaut 2 ou 1 suivant que N contient ou non les racines ℓ^∞-ièmes de l'unité, lorsque N/K est une ℓ-extension cyclique élémentaire de corps de fonctions d'une variable sur un corps algébriquement clos ou $\mathbb{Z}_\ell$-extension d'un corps fini.*

(ii) $q(G, \mathcal{C}\ell_N^-) = t_{N/K}^- - (\delta - l_{N/K}^-) = (t_{N/K}^- + l_{N/K}^-) - \delta$, *où $t_{N/K}^- + l_{N/K}^-$ compte le nombre de places de K_+ décomposées dans K/K_+ et ramifiées dans N/K, et δ vaut 1 ou 0 suivant que N contient ou non les racines ℓ^∞-ièmes de l'unité, lorsque N/K est une ℓ-extension cyclique élémentaire de corps surcirculaires à conjugaison complexe qui satisfont la conjecture d'Iwasawa, de sous-extension réelle associée N_+/K_+.*

4. Appendice : le cas non galoisien

Nous nous plaçons ici dans le cas où l'extension L/H considérée, supposée encore séparable de degré ℓ, n'est plus, en revanche, normale mais admet cependant une clôture galoisienne N/H à groupe métacyclique d'ordre $n\ell$ (avec $n \mid (\ell-1)$).[5]

Lorsque cette hypothèse est satisfaite, le groupe de galois $G = \mathrm{Gal}(N/H)$ s'écrit commeproduit semi-direct de son ℓ-sous-groupe deSylow S, d'ordre ℓ, par le sous-groupe cyclique $T = \mathrm{Gal}(N/L)$, d'ordre n, qui fixe L ; et l'homomorphisme de T dans $\mathrm{Aut}(S)$ qui détermine la loi sur G se factorise via un caractère ℓ-adique χ du groupe T (à valeurs dans $\boldsymbol{\mu}_{\ell-1} \subset {\mathbb{Z}_\ell}^\times$) conformément à l'identité :

$$\tau\sigma\tau^{-1} = \sigma^{\chi(\tau)},$$

pour $\tau \in T$ et σ générateur arbitraire de S.

Dans ce contexte, Gold et Madan (cf. [GM$_4$]) ont proposé une généralisation de la formule de Kida que l'on peut aisément transcrire, à l'aide des correspondances entre invariants d'Iwasawa données dans [Ja$_5$], sous la forme suivante :

(i) $\lambda_N^0 = \lambda_L^0 + \frac{\ell-1}{n}(\lambda_K^0 + t_{N/K} - \delta)$, dans le cas des corps de fonctions,

(ii) $\lambda_N^- = \lambda_L^- + \frac{\ell-1}{n}(\lambda_K^- + t_{N/K}^- + l_{N/K}^- - \delta)$, dans le cas surcirculaire,

les notations étant celles du Théorème 1 et $K = N^S$ étant ce qu'il est convenu d'appeler l'arête cyclique de l'extension étudiée.

Sous la forme (i), ce résultat a été établi par voie analytique par Rück (cf. [Rü]). Sous la forme (ii), il peut également s'établir par passage à la limite à partir de la formule des classes pour les extensions métabéliennes de corps de nombres établie dans (cf. [Ja$_1$]) . Gold et Madan (op. cit.) en donnent deux preuves indépendantes, l'une arithmetico-algébrique, l'autre analytique.

Nous proposons de montrer ici que ce résultat, apparemment plus général, résulte encore du théorème 1, pour des raisons purement algébriques où l'arithmétique n'a point part.

Tout comme dans la section 3, notre point de départ sera un théorème de structure pour les $\mathbb{Z}_\ell[G]$-modules $\mathbb{Z}_\ell$-divisibles et de cotype fini : les résultats de Jaulent (cf. [Ja$_2$, Ja$_3$]) montrent que tout $\mathbb{Z}_\ell[G]$-module noethérien $\mathbb{Z}_\ell$-projectif s'écrit de façon essentiellement unique comme somme d'exemplaires des $3n$ modules indécomposables suivants :

(i) Les n modules $\mathbb{Z}_\ell[S]e_\varphi$, attachés aux idempotents primitifs

$$e_\varphi = \frac{1}{n}\sum_{\tau\in T}\varphi(\tau^{-1})\tau$$

de l'algèbre semi-locale $\mathbb{Z}_\ell[T]$; lesquels sont $\mathbb{Z}_\ell[G]$-projectifs ;

(ii) Les n modules $\mathbb{Z}_\ell e_\varphi \simeq \mathbb{Z}_\ell[S]\nu e_\varphi$, images des précédents par l'opérateur norme $\nu := 1 + \sigma + \cdots + \sigma^{\ell-1}$; sur lesquels S agit trivialement ;

(iii) Les n modules $\mathbb{Z}_\ell[\zeta]e_\varphi \simeq \mathbb{Z}_\ell[S]e_\varphi/\mathbb{Z}_\ell[S]\nu e_\varphi$, quotients des deux précédents.

Par dualité, nous voyons ici que tout $\mathbb{Z}_\ell[G]$-module qui est de cotype fini et $\mathbb{Z}_\ell$-divisible s'écrit donc de façon essentiellement unique :

$$M = \textstyle\sum_\varphi M_\varphi$$

avec

$$M_\varphi \simeq [(\mathbb{Q}_\ell/\mathbb{Z}_\ell)e_\varphi]^{\alpha_\varphi} \oplus [(\mathbb{Q}_\ell/\mathbb{Z}_\ell)\otimes_{\mathbb{Z}_\ell}\mathbb{Z}_\ell[\zeta]e_\varphi]^{\beta_\varphi} \oplus [(\mathbb{Q}_\ell/\mathbb{Z}_\ell)\otimes_{\mathbb{Z}_\ell}\mathbb{Z}_\ell[S]e_\varphi]^{\gamma_\varphi}$$

[5] Cette condition, automatiquement remplie pour $\ell = 3$, est évidemment restrictive pour $\ell = 5$.

les entiers α_φ, β_φ, γ_φ étant, comme plus haut, caractérisés par les identités :

$$\alpha_\varphi + \gamma_\varphi = \mathrm{codim}_{\mathbb{Z}_\ell} M_\varphi^S \; ; \qquad \alpha_\varphi = \dim_{\mathbb{F}_\ell} H^1(S, M_\varphi) \; ; \qquad \beta_\varphi = \dim_{\mathbb{F}_\ell} H^2(S, M_\varphi) \; ;$$

qui donnent en particulier : $\beta_\varphi - \alpha_\varphi = q(S, M_\varphi)$.

On prendra garde ici au fait que les composantes canoniques M_φ ne sont nullement les φ-composantes de M au sens usuel, c'est-à-dire les projections $e_\varphi M$ obtenues par multiplication à gauche par les idempotents e_φ : en effet, le groupe G n'étant pas abélien, les e_φ ne commutent pas à l'action de S. Plus précisément, si l'on désigne par

$$\vartheta = \frac{1}{n} \sum_{\tau \in T} \varphi(\tau^{-1}) \sigma^{\chi(\tau)} \; \in \mathbb{Z}_\ell[S]$$

la résolvante construite sur le générateur σ du groupe cyclique S (respectivement par θ la classe de ϑ dans $\mathbb{Z}_\ell[\zeta] = \mathbb{Z}_\ell[S]/\nu\mathbb{Z}_\ell$), un calcul facile montre que l'on a la décomposition directe :

$$\mathbb{Z}_\ell[S] \; = \bigoplus_{i=0}^{\ell-1} \mathbb{Z}_\ell \vartheta^i \qquad \big(\text{resp. } \mathbb{Z}_\ell[\zeta] \; = \bigoplus_{i=0}^{\ell-2} \mathbb{Z}_\ell \theta^i\big),$$

ainsi que les identités de commutation (pour tout caractère φ du groupe T) :

$$e_{\varphi\chi}\vartheta = \vartheta e_\varphi \qquad \big(\text{resp. } \; e_{\varphi\chi}\theta = \theta e_\varphi\big).$$

Les relations d'orthogonalité entre idempotents conduisent alors, pour chaque couple (ψ, φ) de caractères primitifs du groupe T, aux décompositions :

(i) $\quad e_\psi \mathbb{Z}_\ell[S] e_\varphi = \bigoplus_{i=0}^{\ell-1} \mathbb{Z}_\ell \, e_\psi \vartheta e_\varphi = \bigoplus_{i=0}^{\ell-1} < \psi, \varphi\chi^i > \mathbb{Z}_\ell \, \vartheta^i e_{\varphi^i}$;

(ii) $\quad e_\psi \mathbb{Z}_\ell[\zeta] e_\varphi = \bigoplus_{i=0}^{\ell-2} \mathbb{Z}_\ell \, e_\psi \theta e_\varphi = \bigoplus_{i=0}^{\ell-2} < \psi, \varphi\chi^i > \mathbb{Z}_\ell \, \theta^i e_{\varphi^i}$;

(iii) $\quad e_\psi \; \mathbb{Z}_\ell \; e_\varphi \; = < \psi, \varphi > \mathbb{Z}_\ell \, e_\varphi$.

Appliquant ainsi ce résultat aux modules M_φ définis plus haut, nous obtenons :

$$\begin{aligned} \mathrm{codim}_{\mathbb{Z}_\ell}(e_\psi M_\varphi) &= < \psi, \varphi > \alpha_\varphi + \frac{\ell-1}{n} \, \beta_\varphi + \big(< \psi, \varphi > + \frac{\ell-1}{n} \, \big) \gamma_\varphi \\ &= \big(< \psi, \varphi > + \frac{\ell-1}{n} \, \big) \, (\alpha_\varphi + \gamma_\varphi) + \frac{\ell-1}{n} \, (\beta_\varphi - \alpha_\varphi) \; ; \end{aligned}$$

c'est-à-dire, finalement :

$$\mathrm{codim}_{\mathbb{Z}_\ell}(e_\psi M_\varphi) = \big(< \psi, \varphi > + \frac{\ell-1}{n} \big) \, \mathrm{codim}_{\mathbb{Z}_\ell}(M_\varphi^S) + \frac{\ell-1}{n} \, q(S, M_\varphi) \; ;$$

puis, en sommant sur tous les φ :

$$\mathrm{codim}_{\mathbb{Z}_\ell}(e_\psi M) = \mathrm{codim}_{\mathbb{Z}_\ell} M_\psi^S + \frac{\ell-1}{n} \, \big(\mathrm{codim}_{\mathbb{Z}_\ell} M^S + q(S, M) \big).$$

Appliquant enfin ce résultat en prenant pour M le ℓ-groupe des classes $\mathcal{C}\ell_N^0$ (resp. $\mathcal{C}\ell_N^-$), nous déduisons du théorème 1 la formule suivante :

Théorème 2. *Soit N/K une ℓ-extension cyclique élémentaire de groupe de Galois S, métacyclique de degré ℓn (avec $n \mid (\ell - 1)$) sur un sous-corps H, qui provient par passage à la clôture normale d'une extension séparable L/H de degré ℓ.*

Alors, avec les conventions et notations du théorème 1, les codimensions respectives des φ-composantes $(\mathcal{C}\ell^0)^{e_\varphi}$ (resp. $(\mathcal{C}\ell^-)^{e_\varphi}$) des ℓ-groupes de classes sont données, pour chaque caractère ℓ-adique irréductible φ du groupe $T = \mathrm{Gal}(N/L) \simeq \mathrm{Gal}(K/H)$ par la formule :

(i) $\lambda^0_{N,\varphi} = \lambda^0_{K,\varphi} + \frac{\ell-1}{n}\left(\lambda^0_K + t_{N/K} - \delta_K\right)$, *dans le cas des corps de fonctions ;*

(ii) $\lambda^-_{N,\varphi} = \lambda^-_{K,\varphi} + \frac{\ell-1}{n}\left(\lambda^-_K + t^-_{N/K} + l^-_{N/K} - \delta_K\right)$, *dans le cas surcirculaire.*

Bien entendu, ce dernier résultat contient aussi bien les formules non galoisiennes de Gold et Madan (que l'on obtient en spécialisant en $\varphi = 1$), que celles citées dans l'introduction (qui correspondent, elles, au cas $n = 1$). Enfin, par empilement d'extensions élémentaires, il se généralise sans peine aux ℓ-extensions N/K de degré arbitraire. Plus précisément :

Corollaire. *Soit N/K une ℓ-extension (galoisienne) de groupe S et de degré ℓ^s, provenant par passage à la clôture normale d'une extension séparable L/H de même degré ℓ^s, avec K/H cyclique, telle que le groupe de Galois $G = \mathrm{Gal}(N/H)$ s'écrive comme produit semi-direct de son ℓ-sous-groupe de Sylow $S = \mathrm{Gal}(N/K)$ par le sous-groupe $T = \mathrm{Gal}(K/H)$, avec action fidèle de T sur les quotients de Jordan-Hölder d'une suite sous-normale de S. Alors les codimensions respectives des φ-composantes des ℓ-groupes de classes sont données, dans les deux cas fondamentaux étudiés, par les formules suivantes :*

(i) $\lambda^0_{N,\varphi} = \lambda^0_{K,\varphi} + \frac{\ell^s-1}{[N:L]}(\lambda_K - \delta) + \sum_{\mathfrak{p}} \frac{d_{\mathfrak{p}}-1}{[N:L]}$;

(ii) $\lambda^-_{N,\varphi} = \lambda^-_{K,\varphi} + \frac{\ell^s-1}{[N:L]}(\lambda_K - \delta) + \sum_{\mathfrak{p}^-} \frac{d_{\mathfrak{p}}-1}{[N:L]}$;

où δ a la même signification que plus haut ; la sommation porte sur toutes les places $\mathfrak{p}$ de K dans le cas des corps de fonctions, sur celles du sous-corps réel K_+ décomposées par la conjugaison complexe dans le cas surcirculaire ; et l'indice $d_{\mathfrak{p}}$ étant dans l'un et l'autre cas le degré local en $\mathfrak{p}$ de l'extension N/K.

Références

[CW] C. Chevalley & A. Weil, *Über das Verhalten der Integrale Erster Gattung bei Automorphismen des Functionenkörpers*, Ham. Ann. **10** (1934), 358–361.

[DM] J. D'mello & M. Madan, *Class group rank relations in $\mathbb{Z}_\ell$-extensions*, Manuscripta Math. **41** (1983), 75–107.

[Deu] M. Deuring, *Automorphismen und Divisorenklassen der Ordnung ℓ in algebraischen Funktionenkörpern*, Math. Ann. **113** (1936), 208–215.

[GM$_1$] R. Gold & M. Madan, *Iwasawa invariants*, Communications in Algebra **13** (1985), 1559–1578.

[GM$_2$] R. Gold & M. Madan, *Galois representation of Iwasawa modules*, Acta Arith. **46** (1986), 243–255.

[GM$_3$] R. Gold & M. Madan, *An application of a theorem of Deuring and Šafarevič*, Math. Z. **191** (1986), 247–251.

[GM$_4$] R. Gold & M. Madan, *Kida's theorem for a class of non-normal extensions*, Proc. Am. Math. Soc. **104** (1988), 55–59.

[Her] J. Herbrand, *Nouvelle démonstration et généralisation d'un théorème de Minkovski*, C. R. Acad. Sci. Paris **191** (1930), 1282–1285.

[Hur] A. Hurwitz, *Über algebraische Gebilde mit eindeutigen Transformationen in sich*, Math. Ann. **41** (1893), 403–442.

[Gr$_1$] G. Gras, *Sur les invariants lambda d'Iwasawa des corps abéliens*, Pub. Math. Fac. Sci. Besançon Théor. Nombres 1978-79 (1979).

[Gr$_2$] G. Gras, *Théorie des genres analytique des corps de nombres*, Inv. Math. **86** (1986), 1-17.

[Iw$_1$] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Ann. of Maths **98** (1973), 246-326.

[Iw$_2$] K. Iwasawa, *Riemann-Hurwitz formula and p-adic representations for number fields*, Tôhoku Math. J. **33** (1984), 263–288.

[Ja$_1$] J.-F. Jaulent, *Unités et classes dans les extensions métabéliennes de corps de nombres*, Ann. Sci. Inst. Fourier **31** (1981), 39–62.

[Ja$_2$] J.-F. Jaulent, *Sur la structure galoisienne des idéaux ambiges dans une extension métacyclique de degré nℓ sur le corps des rationnels*, Pub. Math. Fac. Sci. Besançon Théor. Nombres 1979-80, (1980).

[Ja$_3$] J.-F. Jaulent, *Remarques sur la structure galoisienne des entiers d'une extension métacyclique de* $\mathbb{Q}$, C. R. Acad. Sci. Paris **293** (1981), 231–233.

[Ja$_4$] J.-F. Jaulent, *$\mathcal{S}$-classes infinitésimales d'un corps de nombres algébriques*, Ann. Sci. Inst. Fourier **34** (1984), 1–27.

[Ja$_5$] J.-F. Jaulent, *L'arithmétique des ℓ-extensions (Thèse d'Etat)*, Pub. Math. Fac. Sci. Besançon Théor. Nombres 1985-86, (1986), vii+348 pp.

[Ja$_6$] J.-F. Jaulent, *Genre des corps surcirculaires*, Pub. Math. Fac. Sci. Besançon Théor. Nombres 1985-86, (1986).

[Ja$_7$] J.-F. Jaulent, *Dualité dans les corps surcirculaires*, Sém. Théor. Nombres Paris 1986-87, Progress in Math. **75** (1988), 183–220.

[Ki$_1$] Y. Kida, *ℓ-extensions of CM-fields and Iwasawa invariants*, J. Number Th. **12** (1980), 519–528.

[Ki$_2$] Y. Kida, *Cyclotomic $\mathbb{Z}_\ell$-extensions and J-fields*, J. Number Th. **14** (1982), 340–352.

[Ku] L. Kuz'min, *Some duality theorems for cyclotomic Γ-extensions over algebraic number fields*, Math. USSR Izv. **14** (1980), 441-480.

[La] S. Lang, *On quasi algebraic closure*, Ann. of Math. **55** (1952), 373–390.

[Ma] M. Madan, *On a theorem of M. Deuring and I.R. Šafarevič*, Manuscripta Math. **23** (1977), 91–102.

[MZ] M. Madan & H. Zimmer, *Relations among Iwasawa invariants*, J. Number Th. **25** (1987), 213–219.

[Mo] M. Moriya, *Über die Struktur der Divisorenclassen einer zyklischen Erweiterung von Primzahlgrad über einem algebraischen Funktionkörper*, Tôhoku Mat. J. **48** (1941), 43–54.

[Ro] M. Rosen, *Representation of twisted groups (Ph. D. Thesis)*, Princeton, 1963.

[Rü] H.G. Rück, *Hasse-Witt invariants and dihedral extensions*, Math. Z. **191** (1986), 513–517.

[Ša] I.R. Šafarevič, *Onp-extensions*, AM. Math. Soc. Trans. **4** (1954), 59–73.

[Ser] J.-P. Serre, *Corps locaux (deuxième édition*, Paris, 1973

[Sin] W. Sinnot, *On p-adic L-functions and the Riemann-Hurwitz genus formula*, Compositio Math. **51** (1984), 3–17.

[Su] D. Subrao, *The p-rank of Artin-Schreier curves*, Manuscripta Math. **16** (1975), 169–193.

[Tse] C.C. Tsen, *Divisionalgebren über Funktionenkörpen (Dissertation)*, Göttingen, 1933.

[Wa] L. Washington, *Introduction to cyclotomic fields.* Second edition. Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1997, xiv+487 pp.

[W$_1$] K. Wingberg, *Duality theorems for Γ-extensions of algebraic number fields*, Compositio Math. **55** (1985), 333–381.

[W$_2$] K. Wingberg, *A Riemann-Hurwitz formula for the Selmer group of an elliptic curve with complex multiplication*, Comment. Math. Helvetici **63** (1988), 587–592.

Jean-François Jaulent
Université Bordeaux 1
Institut de Mathématiques
351, cours de la Libération
F-33405 TALENCE Cedex
jaulent@math.u-bordeaux1.fr

Alexis Michel
Université Bordeaux 1
Institut de Mathématiques
351, cours de la Libération
F-33405 TALENCE Cedex
michel@math.u-bordeaux1.fr