THEORIE DES NOMBRES
BESANÇON

Années 1979-1980
et 1980-1981

SUR LA ℓ-STRUCTURE GALOISIENNE DES IDEAUX AMBIGES DANS UNE EXTENSION METACYCLIQUE DE DEGRE $n\ell$ SUR LE CORPS DES RATIONNELS

Jean-François JAULENT

SUR LA ℓ-STRUCTURE GALOISIENNE DES IDEAUX AMBIGES DANS UNE EXTENSION METACYCLIQUE DE DEGRE $n\ell$ SUR LE CORPS DES RATIONNELS

Par Jean-François JAULENT

RESUME. Nous étudions la ℓ-structure galoisienne des idéaux ambiges de l'anneau des entiers A_N d'une extension métacyclique de degré $n\ell$ sur le corps des rationnels. Et nous montrons en particulier que l'anneau A_N est localement libre sur l'ordre qui lui est associé dans l'algèbre du groupe de Galois, indépendamment de la ramification.

INTRODUCTION

Etant donné une extension normale N du corps des rationnels, le groupe de Galois $G = \mathrm{Gal}(N/\mathbb{Q})$ opère sur l'anneau de ses entiers A_N, qui est, de ce fait, un $\mathbb{Z}[G]$-module de rang 1. Et il est bien connu, depuis E. Nœther [11], que A_N est localement libre sur $\mathbb{Z}[G]$ si et seulement si la ramification est modérée.

Une façon d'éliminer l'hypothèse de modération consiste à introduire l'ordre $\mathfrak{O}_N = \{\lambda \in \mathbb{Q}[G] \mid \lambda A_N \subset A_N\}$ des éléments de $\mathbb{Q}[G]$ qui opèrent sur A_N. C'est ainsi que lorsque G est abélien, on sait par un résultat de Leopoldt [9] que A_N est libre sur $\mathfrak{O}_N$, et que ce dernier est engendré sur l'algèbre $\mathbb{Z}[G]$ par les idempotents correspondant aux sous-groupes supérieurs de ramification des idéaux premiers de N.

Dans le cas général, la situation est, bien entendu, moins simple. Par exemple, si G est un groupe métacyclique d'ordre $n\ell$, produit semi-direct de centre trivial d'un groupe cyclique S d'ordre premier impair ℓ par un groupe cyclique T, l'anneau A_N est bien libre sur $\mathbb{Z}[G]$ lorsque la ramification est modérée, d'après un théorème de Fröhlich [6]; mais il existe des extensions galoisiennes de degré 23×47, sauvagement ramifiées sur $\mathbb{Q}$, et telles que le produit $\mathfrak{M}.A_N$ de l'anneau A_N par un ordre maximal $\mathfrak{M}$ de l'algèbre $\mathbb{Q}[G]$ ne soit pas $\mathfrak{M}$-stablement libre (cf [2]).

Nous nous proposons, dans ce travail, de préciser quelque peu la ℓ-structure galoisienne de l'anneau A_N et, plus généralement, celle de ses idéaux ambiges, en particulier lorsque l'extension $N/\mathbb{Q}$ est sauvagement ramifiée en ℓ. Nous nous appuyons pour cela sur une classification des $\mathbb{Z}_\ell[G]$-modules nœthériens sans $\mathbb{Z}_\ell$-torsion, que nous exposons dans une première partie, et qui ramène l'étude de la structure d'un module $\mathcal{M}$ à des calculs de caractères de groupes de cohomologie, c'est-à-dire, dans le cas que nous considérons ici, à des calculs de trace dans une extension cyclique. Et nous déterminons explicitement ceux des idéaux ambiges de A_N qui sont localement libres sur leur ordre associé dans l'algèbre $\mathbb{Q}_\ell[G]$.

1. DESCRIPTION DE L'ALGEBRE DU GROUPE SUR L'ANNEAU $\mathbb{Z}_\ell$

Dans tout ce qui suit, nous nous donnons ℓ un nombre premier impair, et n un entier non nul. Par groupe métacyclique d'ordre $n\ell$ nous entendons tout produit semi-direct G de centre trivial d'un groupe cyclique S d'ordre ℓ, par un groupe T, cyclique d'ordre n.

Si G est un tel groupe, l'entier n divise $(\ell-1)$ et l'application de T dans le groupe Aut S des automorphismes de S, qui définit le produit semi-direct, se factorise par un caractère ℓ-adique primitif du groupe T, conformément à l'identité :

$$\tau\eta\tau^{-1} = \eta^{\chi(\tau)}, \text{ pour tous } \tau \text{ de T et } \eta \text{ de S.}$$

Plus généralement, puisque l'anneau $\mathbb{Z}_\ell$ contient les racines $n^{\text{ièmes}}$ de l'unité, les représentations de T sont réalisables sur $\mathbb{Q}_\ell$. Cela étant, à tout caractère ℓ-adique φ irréductible du groupe T correspond un idempotent e_φ de l'algèbre $\mathbb{Z}_\ell[T]$, défini par :

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

et caractérisé par l'identité :

$$\tau\, e_\varphi = \varphi(\tau)\, e_\varphi , \text{ pour tout } \tau \text{ de T.}$$

Il est bien connu que les $(e_\varphi)_{\varphi\in T^*}$ constituent un système complet d'idempotents orthogonaux de l'algèbre semi-locale $\mathbb{Z}_\ell[T]$, indexé sur le groupe T^* des caractères ℓ-adiques irréductibles de T.

Proposition 1. Les homothéties à droite associées aux idempotents irréductibles e_φ de $\mathbb{Z}_\ell[T]$ sont des projecteurs orthogonaux pour la structure de $\mathbb{Z}_\ell[G]$-module de l'algèbre $\mathbb{Z}_\ell[G]$; ce qui s'écrit :

$$\mathbb{Z}_\ell[G] = \bigoplus_{\varphi\in T^*} \mathbb{Z}_\ell[S]\, e_\varphi .$$

Faisons choix maintenant d'un générateur σ du groupe S ; posons $\delta = \sigma - 1$, et considérons l'élément $\vartheta = \frac{1}{n} \sum_{\tau\in T} \chi^{-1}(\tau)\, \sigma^{\chi(\tau)}$.

Nous obtenons :

Proposition 2. La résolvante ϑ est le générateur de l'idéal d'augmentation de l'algèbre $\mathbb{Z}_\ell[S]$ qui satisfait à la congruence $\vartheta \equiv \delta [\mathrm{mod}\ \delta^2 \mathbb{Z}_\ell[S]]$, ainsi qu'aux relations de décalage $e_\varphi \vartheta = \vartheta e_{\varphi\chi^{-1}}$, pour tout φ de T^*.

Démonstration : Notons $\nu = 1+\sigma+\ldots+\sigma^{\ell-1}$ l'opérateur trace, et remarquons que nous pouvons écrire :

$$\delta^{\ell-1} = \nu - \ell(1+\delta\lambda) \qquad \text{puis} \qquad \delta^\ell = -\ell\delta(1+\delta\lambda),$$

pour un λ convenable de $\mathbb{Z}_\ell[S]$; cela nous prouve que l'élément δ est un nilpotent topologique de l'algèbre $\mathbb{Z}_\ell[S]$, donc que la quantité $(1+\delta\lambda)$ est inversible dans $\mathbb{Z}_\ell[S]$, et, par suite, que $\ell\delta$ appartient à la puissance $\ell^{\text{ième}}$ de l'idéal d'augmentation.

Introduisons alors une section $\bar{\chi}$ du caractère χ, à valeurs dans $\{1, 2, \ldots, \ell-1\}$.

De l'égalité :

$$\vartheta = \frac{1}{n}\sum_{\tau\in T}\chi^{-1}(\tau)\sigma^{\bar\chi(\tau)} = \frac{1}{n}\sum_{\tau\in T}\chi^{-1}(\tau)[\sigma^{\bar\chi(\tau)}-1] = \frac{1}{n}\sum_{\tau\in T}\chi^{-1}(\tau)[1+\sigma+\ldots+\sigma^{\bar\chi(\tau)-1}],$$

nous déduisons la congruence :

$$\vartheta = \frac{\delta}{n}\sum_{\tau\in T}\chi^{-1}(\tau)\bar\chi(\tau) \equiv \delta\,[\mathrm{mod}\ \delta^2\mathbb{Z}_\ell[S]],$$ qui nous prouve que

ϑ engendre l'idéal d'augmentation $\delta\mathbb{Z}_\ell[S]$. Et l'identité $e_\varphi\vartheta = \vartheta e_{\varphi\chi^{-1}}$ résulte immédiatement de la relation de commutation : $\tau\vartheta = \chi(\tau)\vartheta\tau$.

Corollaire. Le centre de l'algèbre $\mathbb{Z}_\ell[G]$ est la sous algèbre $C = \mathbb{Z}_\ell[\vartheta^n] + \nu\mathbb{Z}_\ell[T]$.

Démonstration : Remarquons d'abord qu'en vertu de la congruence :

$$\vartheta^{\ell-1} \equiv \delta^{\ell-1} \equiv \nu - \ell\,[\mathrm{mod}\,\ell\delta\,\mathbb{Z}_\ell[S]],$$

l'algèbre $\mathbb{Z}_\ell[S]$ s'écrit, comme somme directe de $\mathbb{Z}_\ell$-modules : $\bigoplus_{i=0}^{\ell-2}\mathbb{Z}_\ell\vartheta^i \oplus \mathbb{Z}_\ell\nu$.

Ecrivons donc $x = \sum_{i=0}^{\ell-2}\sum_{j=0}^{n-1} x_{ij}\vartheta^i e_{\chi^j} + \sum_{j=0}^{n-1} y_j \nu e_{\chi^j}$ un élément de $\mathbb{Z}_\ell[G]$,

et supposons le central.

D'après la proposition précédente, l'identité $\tau x = x\tau$, pour tout τ de T, s'écrit $\chi^i(\tau)x_{ij} = x_{ij}$, ce qui nous prouve que les x_{ij} sont nuls pour $i \not\equiv 0 \pmod n$; tandis que l'égalité $\vartheta x = x\vartheta$ nous montre que x_{ij} est indépendant de j.

Le corollaire en résulte, l'élément ϑ^n étant clairement dans le centre de $\mathbb{Z}_\ell[G]$.

2. ETUDE DES $\mathbb{Z}_\ell[G]$-MODULES INDECOMPOSABLES

La classification des représentations entières d'un groupe métacyclique d'ordre $n\ell$ a fait l'objet d'un travail de Lena Chang Pu, dans le cas où n est premier [8]. Nous précisons ce point lorsque l'anneau d'entiers est celui des nombres ℓ-adiques.

Considérons pour cela un $\mathbb{Z}_\ell[G]$-module nœthérien, sans $\mathbb{Z}_\ell$-torsion, et effectuons son dévissage à l'aide de l'application trace $\nu = 1+\sigma+\ldots+\sigma^{\ell-1}$. Dans la suite exacte : $\quad 0 \longrightarrow P \longrightarrow M \xrightarrow{\nu} Q \longrightarrow 0,$

l'image Q est un $\mathbb{Z}_\ell[T]$-module sur lequel S opère trivialement, donc somme directe de modules indécomposables $\mathbb{Z}_\ell e_\varphi$; tandis que le noyau P est de façon naturelle un module sur l'anneau quotient $\mathbb{Z}_\ell[G]/\nu\mathbb{Z}_\ell[T]$, lequel est isomorphe à l'algèbre à produit croisé $\Lambda = \mathbb{Z}_\ell[\zeta \circ T]$ engendrée sur l'anneau cyclotomique $\mathbb{Z}_\ell[\zeta]$ par le sous-groupe d'ordre n de son groupe de Galois, pour l'action de T sur les racines $\ell^{\text{ièmes}}$ de l'unité définie par le caractère χ.

De plus, l'image Q étant $\mathbb{Z}_\ell[T]$-projective, M s'identifie en tant que $\mathbb{Z}_\ell[T]$-module, à la somme directe $P \oplus Q$. L'action de $\mathbb{Z}_\ell[G]$ sur M peut alors être décrite par les relations : $\theta(x, y) = (\theta x + f_\theta y, \theta y)$, pour tout θ de $\mathbb{Z}_\ell[G]$, où f désigne une application de $\mathrm{Hom}_{\mathbb{Z}_\ell[T]}[\mathbb{Z}_\ell[G], \mathrm{Hom}_{\mathbb{Z}_\ell}(Q,P)]$ satisfaisant aux conditions :

$$f_{\alpha\beta} = \alpha f_\beta + f_\alpha \beta \text{ , pour tous } \alpha, \beta \text{ de } \mathbb{Z}_\ell[G].$$

Et la $\mathbb{Z}_\ell[G]$-structure de M est donc caractérisée, à isomorphisme près, par la classe du cocycle f dans le groupe $\mathrm{Ext}^1_{\mathbb{Z}_\ell[G]}(Q,P)$.

Cela étant, nous obtenons :

<u>Theoreme</u> 1. Si G est un groupe métacyclique d'ordre $n\ell$, tout $\mathbb{Z}_\ell[G]$-module de type fini et sans $\mathbb{Z}_\ell$-torsion s'écrit comme somme directe essentiellement unique d'exemplaires des 3n modules indécomposables non isomorphes suivants :

$$\Gamma_\varphi = \mathbb{Z}_\ell e_\varphi \qquad \Lambda_\varphi = \mathbb{Z}_\ell[\zeta] e_\varphi \qquad \Xi_\varphi = \mathbb{Z}_\ell[S] e_\varphi \quad ;$$

où l'indice φ parcourt le groupe T^* des caractères ℓ-adiques irréductibles de T.

Avant d'établir le théorème, remarquons que les modules Γ_φ sont précisément ceux indécomposables sur lesquels le groupe S opère trivialement ; tandis que les modules Λ_φ, qui sont annulés par l'opérateur trace, correspondent aux idéaux $\mathfrak{L}^i$ de l'anneau cyclotomique $\mathbb{Z}_\ell[\zeta]$: en effet , si $\omega = \frac{1}{n} \sum_{\tau \in T} \chi^{-1}(\tau)\zeta^{\chi(\tau)}$ désigne l'image de la résolvante ϑ dans $\mathbb{Z}_\ell[\zeta]$, l'application $\omega^i P(\zeta) \mapsto P(\zeta)\, e_{\chi^i}$ est un isomorphisme de $\mathfrak{L}^i$ sur Λ_{χ^i}.

Comme, d'après les travaux de Rosen [13], tout Λ-module P est somme directe de tels idéaux, il suit que dans le dévissage :

$$0 \longrightarrow P \longrightarrow M \xrightarrow{\nu} Q \longrightarrow 0 ,$$

d'un $\mathbb{Z}_\ell[G]$-module M, le noyau P est somme directe d'exemplaires de modules Λ_φ, et l'image de modules Γ_φ. Le foncteur Ext étant additif, il suffit donc pour déterminer $\mathrm{Ext}^1_{\mathbb{Z}_\ell[G]}(Q,P)$, d'expliciter celui-ci lorsque P et Q sont indécomposables. Convenons, pour simplifier, d'écrire Hom pour $\mathrm{Hom}_{\mathbb{Z}_\ell[G]}$ et Ext pour $\mathrm{Ext}^1_{\mathbb{Z}_\ell[G]}$.

Cela étant, nous avons :

__Lemme 1__. Désignons par $\mathfrak{L}_o$ l'unique idéal maximal du sous-anneau $\mathfrak{B}_o$ d'indice n dans l'anneau cyclotomique $\mathfrak{B} = \mathbb{Z}_\ell[\zeta]$; par φ et ψ deux caractères irréductibles de T. Nous obtenons :

$$\text{(i)} \quad \mathrm{Hom}(\Gamma_\varphi, \Lambda_\psi) = \mathrm{Hom}(\Lambda_\varphi, \Gamma_\psi) = 0 \quad ;$$

$$\text{(ii)} \quad \mathrm{Hom}(\Xi_\varphi, \Lambda_\psi) = \mathrm{Hom}(\Lambda_\varphi, \Lambda_\psi) = \mathfrak{L}_o^{\rho(\varphi,\psi)} \quad ;$$

$$\text{(iii)} \quad \mathrm{Hom}(\Xi_\varphi, \Gamma_\psi) = \mathrm{Hom}(\Gamma_\varphi, \Gamma_\psi) = \langle \varphi, \psi \rangle \mathbb{Z}_\ell \quad ;$$

où $\rho(\varphi,\psi)$ est donné par $\rho(\varphi,\psi) = [(t+n-1)/n]$, si t est l'entier de $\{0, 1, \dots, n-1\}$ qui vérifie $\psi\varphi^{-1} = \chi^t$.

Démonstration : (i) Soit, en effet, un $\mathbb{Z}_\ell[G]$-morphisme f de Γ_φ dans Δ_ψ. Par action de l'opérateur trace ν, il vient : $0 = \nu f = f \nu = f \ell$; soit $\ell f = 0$, puis $f = 0$. Un résultat analogue vaut pour $\mathrm{Hom}(\Lambda_\varphi, \Gamma_\psi)$.

(ii) Supposons maintenant $f \in \mathrm{Hom}(\Xi_\varphi, \Lambda_\psi)$. De l'égalité $f\nu = \nu f = 0$, nous concluons que f se factorise par le quotient $\Xi_\varphi / \nu \Xi_\varphi$ isomorphe à Λ_φ ; et un $\mathbb{Z}_\ell[G]$-morphisme de Λ_φ dans Λ_ψ n'est autre qu'une homothétie de rapport dans $\mathfrak{B}_o$.

(iii) Enfin, si f appartient à $\mathrm{Hom}(\Xi_\varphi, \Gamma_\psi)$; l'identité $f\vartheta = \vartheta f = 0$ montre que f se factorise par le quotient $\Xi_\varphi / \vartheta \Xi_\varphi$ isomorphe à Γ_φ ; ce qui achève la démonstration.

Lemme 2. Sous les mêmes hypothèses, il suit :

$$\mathrm{Ext}\,(\Gamma_\varphi, \Lambda_\psi) = \langle \psi, \varphi\chi \rangle\, \mathbb{F}_\ell\,, \qquad \text{et} \qquad \mathrm{Ext}\,(\Lambda_\varphi, \Gamma_\psi) = \langle \varphi, \psi \rangle\, \mathbb{F}_\ell\,.$$

Démonstration : Dans le dévissage canonique du module $\Xi_\varphi = \mathbb{Z}_\ell[S]\,e_\varphi$, l'image $\mathrm{Im}\,\nu$, égale à $\nu\mathbb{Z}_\ell\,e_\varphi$, est isomorphe à Γ_φ ; et le noyau Ker ν, égal à $\vartheta\mathbb{Z}_\ell[S]\,e_\varphi$ s'identifie à $\Lambda_{\varphi\chi} = \mathbb{Z}_\ell[\zeta]\,e_{\varphi\chi}$, en vertu de la relation de décalage donnée à la proposition 2.

Ainsi, de la suite exacte de $\mathbb{Z}_\ell[G]$-modules :

$$0 \longrightarrow \Lambda_{\varphi\chi} \longrightarrow \Xi_\varphi \longrightarrow \Gamma_\varphi \longrightarrow 0,$$

nous déduisons la suite exacte de groupe :

$$0 \longrightarrow \mathrm{Hom}(\Gamma_\varphi, \Lambda_\psi) \longrightarrow \mathrm{Hom}(\Xi_\varphi, \Lambda_\psi) \longrightarrow \mathrm{Hom}(\Lambda_{\varphi\chi}, \Lambda_\varphi) \longrightarrow \mathrm{Ext}\,(\Gamma_\varphi, \Lambda_\psi) \longrightarrow 0\,,$$

qui nous donne immédiatement :

$$\mathrm{Ext}\,(\Gamma_\varphi, \Lambda_\psi) = \mathrm{Hom}\,(\Lambda_{\varphi\chi}, \Lambda_\psi)/\mathrm{Hom}\,(\Lambda_\varphi, \Lambda_\psi) = \langle \varphi\chi, \psi \rangle\, \mathbb{F}_\ell\,.$$

De façon semblable, de la suite exacte courte :

$$0 \longrightarrow \nu\Gamma_\psi \longrightarrow \Xi_\psi \longrightarrow \Lambda_\psi \longrightarrow 0\,,$$

nous déduisons la suite exacte de groupes :

$$0 \longrightarrow \mathrm{Hom}(\Lambda_\psi, \Gamma_\varphi) \longrightarrow \mathrm{Hom}(\Xi_\psi, \Gamma_\varphi) \xrightarrow{\ \ell\ } \mathrm{Hom}(\Gamma_\psi, \Lambda_\varphi) \longrightarrow \mathrm{Ext}(\Lambda_\psi, \Gamma_\varphi) \longrightarrow 0\,,$$

qui nous donne l'isomorphisme :

$$\mathrm{Ext}(\Lambda_\psi, \Gamma_\varphi) = \mathrm{Hom}(\Gamma_\psi, \Gamma_\varphi)/\ell\ \mathrm{Hom}(\Gamma_\psi, \Gamma_\varphi) = \langle \psi, \varphi \rangle\, \mathbb{F}_\ell.$$

Démonstration du théorème : Considérons un $\mathbb{Z}_\ell[G]$-module indécomposable M et dévissons le par action de la trace ν. Posons P = Ker ν et Q = Im ν ; puis notons f l'élément du groupe $\mathrm{Ext}(Q,P)$ qui définit la structure de M.

Supposons d'abord P et Q indécomposables, ce que nous pouvons écrire $P = \Lambda_\psi$ et $Q = \Gamma_\varphi$. Le module M étant lui-même indécomposable, nous avons $\psi = \varphi\chi$ d'après le lemme 2 ; et f est uniquement déterminé par la classe f(1) dans le quotient $\Lambda_\psi/\omega\Lambda_\psi$. Or, celle-ci pouvant être prise arbitrairement par $\mathbb{Z}_\ell[G]$-automorphisme de P, il existe donc à isomorphisme près, et sous la condition nécessaire $\psi = \varphi\chi$, une et une seule extension indécomposable de Λ_ψ par Γ_φ : c'est Ξ_φ.

Dans l'hypothèse où P et Q ne seraient pas indécomposables, écrivons les comme sommes de modules isotypiques $P = \oplus_\varphi P_\varphi$ et $Q = \oplus_\psi Q_\psi$. Par additivité du foncteur Ext, nous obtenons : $\mathrm{Ext}(Q,P) = \bigoplus_{\varphi,\psi} \mathrm{Ext}(Q_\psi, P_\varphi) = \oplus_\varphi \mathrm{Ext}(Q_{\varphi\chi}, P_{\varphi\chi})$ et M est décomposé dès que l'un ou l'autre de P ou de Q n'est pas isotypique. Ecrivons donc : $P = \bigoplus_{i\in I} \Lambda_{\varphi\chi}$ et $Q = \bigoplus_{j \in J} \Gamma_\varphi$ comme sommes directes d'indécomposables du même type. Nous pouvons représenter f matriciellement sous la forme $f = [f_{ij}]$ avec $f_{ij} \in \mathrm{Ext}(\Gamma_\varphi, \Lambda_{\varphi\chi})$, et il suffit de diagonaliser f par automorphismes de P et Q pour constater que M est décomposé avec l'un ou l'autre de P ou Q.

Ainsi, les seuls $\mathbb{Z}_\ell[G]$-modules indécomposables sont bien les 3n modules proposés ; ceci achève la démonstration, puisque l'unicité de la décomposition résulte du théorème de Krull-Schmidt.

Scolie. Etant donné un module M sur l'algèbre $\mathbb{Z}_\ell[G]$, les groupes de cohomologie $H^0(S,M) = \mathrm{Ker}\,\vartheta$, puis $H^1(S,M) = \mathrm{Ker}\,\nu/\mathrm{Im}\,\vartheta$ et $H^2(S,M) = \mathrm{Ker}\,\vartheta/\mathrm{Im}\,\nu$ sont, de façon naturelle, des $\mathbb{Z}_\ell[G]$-modules sur lesquels S opère trivialement. En particulier :

(i) $H^0(S,\Xi_\varphi) = \Gamma_\varphi$, $H^1(S,\Xi_\varphi) = 0$; $H^2(S,\Xi_\varphi) = 0$;

(ii) $H^0(S,\Gamma_\varphi) = \Gamma_\varphi$, $H^1(S,\Gamma_\varphi) = 0$; $H^2(S,\Gamma_\varphi) = \mathbb{F}_\ell\, e_\varphi$;

(iii) $H^0(S,\Lambda_\varphi) = 0$, $H^1(S,\Lambda_\varphi) = \mathbb{F}_\ell\, e_\varphi$; $H^2(S,\Lambda_\varphi) = 0$.

Il suit que la G-structure d'un module M, nœthérien et sans $\mathbb{Z}_\ell$-torsion, est uniquement déterminée par l'action de T sur les groupes de cohomologie associés à S.

3. ORDRES DANS $\mathbb{Q}_\ell[G]$

Nous appliquons les résultats qui précèdent à la description des ordres de $\mathbb{Q}_\ell[G]$ qui contiennent $\mathbb{Z}_\ell[G]$.

Précisons en premier lieu la décomposition semi-simple de l'algèbre $\mathbb{Q}_\ell[G]$.

Proposition 3. Les idempotents $\frac{\nu}{\ell} e_\varphi$ attachés aux caractères irréductibles du groupe T et l'élément $\frac{\ell-\nu}{\ell}$ constituent un système complet d'idempotents centraux de l'algèbre semi-simple $\mathbb{Q}_\ell[G]$. En particulier, dans l'isomorphisme :

$$\mathbb{Q}_\ell[G] = \Big(\bigoplus_{\varphi \in T^*} \mathbb{Q}_\ell \frac{\nu}{\ell} e_\varphi \Big) \oplus \mathbb{Q}_\ell[G] \frac{\ell-\nu}{\ell} ,$$

le facteur $\mathbb{Q}_\ell[G] \frac{\ell-\nu}{\ell}$ est isomorphe à l'algèbre simple $\mathbb{Q}_\ell[\zeta \circ T]$ engendrée sur le corps cyclotomique $\mathbb{Q}_\ell[\zeta]$ par le sous-groupe d'ordre n de son groupe de Galois.

__Corollaire__. La sous-algèbre $\mathfrak{M}$ de $\mathbb{Q}_\ell[G]$, engendrée sur $\mathbb{Z}_\ell[G]$ par les idempotents centraux $\frac{\nu}{\ell}e_\varphi$ attachés aux caractères irréductibles de T, est un ordre héréditaire qui admet la décomposition directe :

$$\mathfrak{M} = \Big(\bigoplus_{\varphi\in T^*} \mathbb{Z}_\ell \frac{\nu}{\ell} e_\varphi\Big) \oplus \mathbb{Z}_\ell[G]\frac{\ell-\nu}{\ell},$$ dans laquelle le facteur $\mathbb{Z}_\ell[G]\frac{\ell-\nu}{\ell}$ est isomorphe à l'algèbre héréditaire $\Lambda = \mathbb{Z}_\ell[\zeta \circ T]$.

De plus, tout $\mathfrak{M}$ module nœthérien et sans $\mathbb{Z}_\ell$-torsion s'écrit de façon essentiellement unique comme somme directe d'exemplaires des **2** n modules :

Γ_φ et Λ_φ , où φ parcourt le groupe des caractères irréductibles de T.

Démonstration : La décomposition semi-simple de l'algèbre $\mathbb{Q}_\ell[G]$ est immédiate. Cela étant, le sous anneau $\mathfrak{M}$ de $\mathbb{Q}_\ell[G]$ engendré sur $\mathbb{Z}_\ell[G]$ par les idempotents centraux, est évidemment un ordre de $\mathbb{Q}_\ell[G]$. Il est héréditaire comme composé direct d'algèbres héréditaires ; et les seuls $\mathfrak{M}$-modules nœthériens sans $\mathbb{Z}_\ell$-torsion, qui sont indécomposables, sont bien les modules Γ_φ et Λ_φ, conformément aux décompositions :

$$\mathfrak{M}\Gamma_\varphi = \Gamma_\varphi \quad ; \quad \mathfrak{M}\Lambda_\varphi = \Lambda_\varphi \quad ; \quad \text{et } \mathfrak{M}\Xi_\varphi \simeq \Gamma_\varphi \oplus \Lambda_\varphi .$$

Nous pouvons dès lors décrire les ordres maximaux de l'algèbre $\mathbb{Q}_\ell[G]$ qui contiennent $\mathbb{Z}_\ell[G]$. En effet, si $\mathfrak{O}$ est un tel ordre, il contient les idempotents centraux de $\mathbb{Q}_\ell[G]$ et, par suite, l'ordre $\mathfrak{M}$. Par la décomposition directe :

$$\mathfrak{O} = \Big(\frac{\nu-\ell}{\ell}\Big)\mathfrak{O} \oplus \Big(\bigoplus_{\varphi\in T^*} \frac{\nu}{\ell} e_\varphi \mathfrak{O}\Big),$$

nous sommes ainsi ramenés à déterminer les ordres maximaux de l'algèbre $\mathbb{Q}_\ell[\zeta \circ T]$ qui contiennent $\mathbb{Z}_\ell[\zeta \circ T]$.

Cela étant, $\mathbb{Q}_\ell[\zeta \circ T]$ est une algèbre simple centrale sur le sous corps $\mathbb{Q}_o$ d'indice n dans le corps cyclotomique $\mathbb{Q}_\ell[\zeta]$, de sorte que, conformément aux résultats de Reiner ([12], th. 39. 14), l'algèbre héréditaire $\Lambda = \mathbb{Z}_\ell[\zeta \circ T]$ admet (avec les notations du lemme 1) une description matricielle dans $\mathcal{M}_n(\mathbb{Q}_o)$, de la forme :

$$\Lambda = \bigoplus_{i=0}^{n-1} \mathfrak{L}^i = \begin{bmatrix} \mathfrak{B}_o & \mathfrak{L}_o & \cdots & \mathfrak{L}_o \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \mathfrak{L}_o \\ \mathfrak{B}_o & \cdots & \cdots & \mathfrak{B}_o \end{bmatrix}$$

Dans cet isomorphisme, le radical $\mathfrak{R} = \vartheta\,\Lambda$ s'écrit :

$$\mathfrak{R} = \bigoplus_{i=1}^{n} \mathfrak{L}^i = \begin{bmatrix} \mathfrak{L}_o & \cdots & \cdots & \mathfrak{L}_o \\ \mathfrak{B}_o & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ \mathfrak{B}_o & \cdots & \mathfrak{B}_o & \mathfrak{L}_o \end{bmatrix}$$

Tandis que les ordres maximaux $\mathfrak{O}_{\chi^i}$ de $\mathbb{Q}_\ell[\zeta \circ T]$ s'obtiennent respectivement, à partir de l'anneau cyclotomique $\mathfrak{B} = \mathbb{Z}_\ell[\zeta] = \bigoplus_{j=0}^{n-1} \mathfrak{B}_o \omega^j$, commes ordres associés aux n modules $\mathfrak{R}^i\mathfrak{B}$, pour $i = 0, \ldots, n-1$ ([12], th. 39. 23).

Autrement dit, nous avons $\mathfrak{O}_{\chi^i} = \{x \in \mathbb{Q}_\ell[\zeta \circ T] \mid x\,\mathfrak{R}^i\mathfrak{B} \subset \mathfrak{R}^i\mathfrak{B}\}$.

Ainsi, de la décomposition directe $\mathfrak{R}^i\mathfrak{B} = \bigoplus_{j=0}^{n-1} \mathfrak{B}_o \omega^{i+j}$, nous déduisons immédiatement la description matricielle :

$$\mathfrak{O}_{\chi^i} = \bigoplus_{j=0}^{i-1} \mathfrak{L}^{i-n} \oplus \bigoplus_{j=i}^{n-1} \mathfrak{L}^i = \left[\begin{array}{ccc|ccc} \mathfrak{B}_o & \cdots & \mathfrak{B}_o & \mathfrak{L}_o & \cdots & \mathfrak{L}_o \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathfrak{B}_o & \cdots & \mathfrak{B}_o & \mathfrak{L}_o & \cdots & \mathfrak{L}_o \\ \hline \mathfrak{L}_o^{-1} & \cdots & \mathfrak{L}_o^{-1} & \mathfrak{B}_o & \cdots & \mathfrak{B}_o \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathfrak{L}_o^{-1} & \cdots & \mathfrak{L}_o^{-1} & \mathfrak{B}_o & \cdots & \mathfrak{B}_o \end{array}\right]$$

En particulier le $\mathfrak{O}_{\chi^i}$-module $\mathfrak{R}^i\mathfrak{B} = \mathfrak{L}^i$ est, à isomorphisme près, le seul qui soit indécomposable.

Récapitulant ces résultats, nous obtenons :

Théorème 2. Etant donné un groupe métacyclique G, d'ordre $n\ell$, il existe exactement n ordres maximaux $\mathfrak{M}_\varphi$ dans l'algèbre $\mathbb{Q}_\ell[G]$, qui contiennent $\mathbb{Z}_\ell[G]$. Plus précisément, pour tout caractère ℓ-adique irréductible φ du groupe T, l'ordre $\mathfrak{M}_\varphi$, qui est associé au module Λ_φ, est engendré sur $\mathbb{Z}_\ell[G]$ par le nilpotent $e_\varphi \frac{\vartheta}{\ell}^{\ell-n}$.

Sa décomposition indécomposable sur l'algèbre $\mathbb{Z}_\ell[G]$ est ainsi :

$$\mathfrak{M}_\varphi \simeq \Big(\bigoplus_{j=0}^{n-1} \Lambda_\varphi\Big) \oplus \Big(\bigoplus_{\psi \in T^*} \Gamma_\psi\Big).$$

Démonstration : Il suffit de vérifier que les éléments $e_{\varphi\chi^j} \frac{\vartheta^{i+j}}{\ell}$ qui opèrent sur Λ_φ sont ceux pour lesquels i est supérieur à $\ell-n$, lorsque j décrit $0,\ldots,n-1$; et qu'ils s'obtiennent tous à partir de $e_\varphi \frac{\vartheta}{\ell}^{\ell-1}$ par multiplication par une puissance de ϑ. En particulier, $\mathfrak{M}_\varphi$ contient les éléments $e_\psi \frac{\vartheta}{\ell}^{\ell-1}$ et donc les idempotents centraux $\frac{\vartheta}{\ell} e_\psi$.

Corollaire. Pour tout caractère ℓ-adique irréductible φ du groupe T, l'ordre $\mathfrak{N}_\varphi$, associé au module Ξ_φ, est engendré sur $\mathbb{Z}_\ell[G]$ par le nilpotent $\vartheta e_\varphi \frac{\vartheta}{\ell}^{\ell-n}$. Il contient $\vartheta\mathfrak{M}_\varphi$, ainsi que les idempotents centraux $\frac{\gamma}{\ell} e_\psi$, pour $\psi \neq \varphi$; sa décomposition s'écrit :

$$\mathfrak{N}_\varphi \simeq \Xi_\varphi \oplus \Big(\bigoplus_{j=1}^{n-1} \Lambda_{\varphi\chi^j}\Big) \oplus \Big(\bigoplus_{\psi\neq\varphi} \Gamma_\psi\Big).$$

Cela étant, l'ordre associé à un $\mathbb{Z}_\ell[G]$-module de rang 1, s'obtient immédiatement comme intersection des ordres associés à ses composantes. C'est ainsi que l'ordre $\mathfrak{M}$ est l'intersection des $\mathfrak{M}_\varphi$, et $\mathbb{Z}_\ell[G]$ celle des $\mathfrak{N}_\varphi$.

4. APPLICATION AUX ENTIERS D'UN CORPS LOCAL

Dans ce paragraphe N désigne une extension métacyclique de degré $n\ell$, sauvagement ramifiée sur le corps $\mathbb{Q}_\ell$ des nombres ℓ-adiques, $\mathfrak{A}$ l'anneau de ses entiers et $\mathfrak{P}$ son idéal maximal. Nous notons G le groupe de Galois, S le sous-groupe dérivé, T un relèvement de G/S en un sous-groupe de G, et χ le caractère de l'action de T sur S.

Le sous-corps K des invariants de S est une extension cyclique, modérément ramifiée, de degré n sur $\mathbb{Q}_\ell$, et dont le groupe de Galois est isomorphe à T. L'anneau de ses entiers $\mathfrak{a}$ est donc libre sur l'algèbre $\mathbb{Z}_\ell[T]$:

$$\mathfrak{a} \simeq \mathbb{Z}_\ell[T] = \bigoplus_{\varphi\in T^*} \Gamma_\varphi \quad ;$$

tandis que si f désigne l'indice d'inertie de ℓ dans K, le quotient de $\mathfrak{a}$ par son idéal maximal $\mathfrak{p}$, qui s'identifie au corps $\mathbb{F}_{\ell^f}$, est isomorphe, comme $\mathbb{Z}_\ell[T]$-module, à l'algèbre $\mathbb{F}_\ell[T/I]$ du quotient de T par le sous-groupe d'inertie de ℓ dans K :

$$\mathfrak{a}/\mathfrak{p} \simeq \mathbb{F}_\ell[T/I] = \bigoplus_{\varphi \in (T/I)^*} F_\varphi,$$ où nous avons écrit F_φ pour $\Gamma_\varphi/\ell\Gamma_\varphi$.

Introduisons l'indice de ramification e de ℓ dans K, puis t le saut de ramification sauvage ; et, puisque le corps $\mathbb{Q}_\ell$ contient les racines $n^{\text{ièmes}}$ de l'unité, faisons choix dans $\mathfrak{A}$ d'une uniformisante π dont la puissance $n^{\text{ième}}$ soit invariante par T. Notons $\rho = \pi^\nu$ sa norme sur K et ψ le caractère de T défini par l'identité :

$$\pi^{\tau-1} = \psi(\tau), \text{ pour tout } \tau \text{ de } T.$$

<u>Lemme 3.</u> Le saut de ramification t est lié à l'indice e par la relation : $t \leq [\frac{e\ell}{\ell-1}] \leq \ell$; et l'égalité $t = \ell$ n'a lieu que pour $e = n = \ell - 1$.

Démonstration : Voir [10] lemme III.1 .

<u>Lemme 4.</u> Le caractère $\chi\psi^{-t}$ est trivial sur le sous-groupe d'inertie I.

Démonstration : D'après ce qui précède, nous pouvons écrire

$$\vartheta\pi \equiv a\pi^{t+1} [\bmod \mathfrak{P}^{t+2}], \text{ pour un a de } \mathfrak{a}\setminus\mathfrak{p} \text{ fixé par I.}$$

De l'identité $\tau\vartheta = \chi(\tau)\vartheta\tau$ donnée par la proposition 2, nous déduisons immédiatement :

$$\psi^{t+1}(\tau)\, a^\tau \pi^{t+1} \equiv \chi(\tau)\,\psi(\tau)\, a\pi^{t+1} [\bmod \mathfrak{P}^{t+2}], \text{ soit } a^\tau \equiv \chi\psi^{-t}(\tau)\, a [\bmod \mathfrak{P}] \text{ ;}$$

ce qui nous prouve que $\chi\psi^{-t}(\tau)$ vaut 1, pour tout τ de I.

En particulier, l'élément $\pi^{-1-t}\vartheta\pi$ est invariant par le groupe d'inertie I, de sorte que nous avons en fait l'égalité :

$$\vartheta\pi = a\pi^{1+t},$$ pour un choix convenable de a dans le sous-corps d'inertie ; et, bien sûr : $\vartheta\pi^k \equiv k\, a\pi^{k+t} [\bmod \mathfrak{P}^{k+t+1}]$, pour tout k de $\mathbb{Z}$.

Cela étant :

Proposition 4. Pour tout entier relatif s, l'idéal fractionnaire $\mathfrak{P}^s$ s'écrit comme somme directe de $\mathbb{Z}_\ell$ [T]-modules sous la forme :

$$\mathfrak{P}^s = \mathfrak{a}\pi^{t+\ell u} \oplus \vartheta(\mathfrak{P}^{s-t}), \quad \text{avec } u = 1 + \left[\frac{s-t-1}{\ell}\right]$$

Démonstration (d'après J. Cougnard [3]) : Il suffit d'écrire :

$$\mathfrak{P}^s = \bigoplus_{k=s}^{s+(\ell-1)} \mathfrak{a}\pi^k = \mathfrak{a}\pi^{t+\ell u} + \sum_{\substack{k=s \\ \ell \nmid (k-t)}}^{s+(\ell-1)} \mathfrak{a}\pi^k \subset \mathfrak{a}\pi^{t+\ell u} + \vartheta\Big(\sum_{k=s-t}^{s-t+(\ell-1)} \mathfrak{a}\pi^k\Big),$$

en vertu des congruences qui précèdent ; puis de vérifier que la somme est directe, par exemple en appliquant l'opérateur trace ν.

Corollaire 1. Pour tout s de $\mathbb{Z}$, le noyau, dans l'idéal fractionnaire $\mathfrak{P}^s$, de l'opérateur trace ν est le sous-module : $\mathfrak{P}^{s*} = \vartheta(\mathfrak{P}^{s-t})$;
tandis que l'image de ν est l'idéal fractionnaire :

$$\nu(\mathfrak{P}^s) = \mathfrak{p}^v, \quad \text{avec } v = \left[\frac{s+(t+1)(\ell-1)}{\ell}\right].$$

Démonstration : la première partie résulte de la proposition ; la seconde de [14] (Ch. V, § 3, lemme 4).

Corollaire 2. Pour tout s de $\mathbb{Z}$, les groupes de cohomologie attachés à l'idéal fractionnaire $\mathfrak{P}^s$ sont donnés par les $\mathbb{F}_\ell$[T]-isomorphismes :

$$H^1(S, \mathfrak{P}^s) \simeq (\mathfrak{P}^s/\mathfrak{P}^{s+t})/(\mathfrak{p}^v/\mathfrak{p}^{w+t}) \;;$$

$$H^2(S, \mathfrak{P}^s) \simeq \mathfrak{p}^w/\mathfrak{p}^v \;; \quad \text{avec } v = t+1+\left[\frac{s-t-1}{\ell}\right] \text{ et } w = 1+\left[\frac{s-1}{\ell}\right].$$

Ils ont même ordre $\ell^{(t-1)+([\frac{s-1+(\ell-t)}{\ell}]-[\frac{s-1}{\ell}])}$ et s'annulent simultanément pour tous les s, en ramification modérée ; et pour tous les seuls $s \equiv 1 \pmod{\ell}$, lorsque t vaut 1.

Démonstration : Puisque le corps N est un K[S]-module libre, il existe dans $\mathfrak{P}^s$ un sous-module ouvert, qui est libre sur $\mathfrak{a}$[S]. Le quotient de Herbrand de $\mathfrak{P}^s$ est donc trivial, et les groupes $H^i(S, \mathfrak{P}^s)$ ont ainsi le même ordre.

Maintenant, d'après le corollaire 1, le premier groupe de cohomologie est donné par la formule : $H^1(S, \mathfrak{P}^s) = \vartheta(\mathfrak{P}^{s-t})/\vartheta(\mathfrak{P}^s)$; et ce dernier quotient est l'image par l'opérateur $\vartheta\pi^{-t}$ du groupe $\mathfrak{P}^s/(\mathfrak{P}^{s+t} + (K \cap \mathfrak{P}^{s-t})\pi^t)$, que nous pouvons encore écrire $(\mathfrak{P}^s/\mathfrak{P}^{s+t})/\pi^t\left((K \cap \mathfrak{P}^{s-t})/(K \cap \mathfrak{P}^s)\right)$. Sous cette forme, le dénominateur s'écrit $\pi^t[\mathfrak{p}^{v-t}/\mathfrak{p}^w]$; et il est donc isomorphe à $\mathfrak{p}^v/\mathfrak{p}^{w+t}$.

Cela étant, convenons, pour tout caractère irréductible φ de T, de noter Φ le caractère de degré f défini par la formule $\Phi = \sum_{\theta \in (T/I)^*} \theta\varphi$. Le lemme 4 nous prouve que l'image bijective par l'opérateur $\vartheta\pi^{-t}$ d'un $\mathbb{F}_\ell[T]$-module de caractère Φ est un $\mathbb{F}_\ell[T]$-module de même caractère. Comme les quotients $\mathfrak{P}^s/\mathfrak{P}^{s+t}$ et $\mathfrak{p}^s/\mathfrak{p}^{w+t}$ sont sommes de tels modules, la première partie du corollaire se trouve ainsi établie.

Quant au second groupe de cohomologie, il s'écrit immédiatement :

$$H^2(S, \mathfrak{P}^s) = \mathfrak{p}^w/\mathfrak{p}^v \quad ; \text{ ce qui achève la démonstration.}$$

D'après le scolie au théorème 1, le corollaire 2 ci-dessus détermine complètement la structure galoisienne de l'idéal $\mathfrak{P}^s$. En effet, si nous convenons d'écrire Ψ^k pour Φ lorsque φ est égal à ψ^k, le caractère du $\mathbb{F}_\ell[T]$-module $H^1(S, \mathfrak{P}^s)$ est exactement :

$$\Phi_1 = \Psi^s + \Psi^{s+1} + \ldots + \Psi^{s+t-1} - \left([\tfrac{s-1}{\ell}] - [\tfrac{s-t-1}{\ell}]\right)\Psi^v \quad ;$$

tandis que le caractère de $H^2(S, \mathfrak{P}^s)$ s'écrit :

$$\Phi_2 = \Psi^w + \Psi^{w+1} + \ldots + \Psi^{v-1} .$$

La $\mathbb{Z}_\ell[G]$-structure de l'idéal $\mathfrak{P}^s$ est donc donnée par la formule :

$$\mathfrak{P}^s \simeq [\bigoplus_{\varphi | \Phi_1} \Lambda_\varphi] \oplus [\bigoplus_{\varphi | \Phi_2} \Gamma_\varphi] \oplus [\bigoplus_{\varphi | \Phi_2} \Xi_\varphi] \text{ ; conformément à l'iso-}$$

morphisme :

$$\mathfrak{p}^w \simeq [\bigoplus_{\varphi | \Phi_2} \Gamma_\varphi] \oplus [\bigoplus_{\varphi | \Phi_2} \Gamma_\varphi] = \mathbb{Z}_\ell[T].$$

Tandis que son ordre associé $\mathfrak{O}^s$ n'est autre que l'intersection :

$$\mathfrak{O}^s = \left(\bigcap_{\varphi | \Phi_1} \mathfrak{M}_\varphi\right) \cap \left(\bigcap_{\varphi \nmid \Phi_2} \mathfrak{N}_\varphi\right).$$

Théorème 3. Pour tout entier relatif s, le quotient $\mathfrak{P}^s/\mathrm{Tr}_{N/K}(\mathfrak{P}^s)$ est libre sur l'algèbre Λ si et seulement si les groupes de cohomologie de l'idéal $\mathfrak{P}^s$ relativement au groupe S ont même caractère Φ ; ce qui a lieu exactement dans les cas suivants :

en ramification modérée, pour toute valeur de s ;

en ramification sauvage, pour tous les s de $r+\ell\mathbb{Z}$, si r est un entier de $[1,\ell]$ qui vérifie la congruence $r \equiv 1 \pmod e$.

Lorsque c'est le cas, l'idéal $\mathfrak{P}^s$ est libre sur son ordre associé $\mathfrak{O}^s$, qui est engendré sur $\mathbb{Z}_\ell[G]$ par les idempotents $e_\varphi \frac{\nu}{\ell}$, pour les φ divisant Φ.

Démonstration : D'après ce qui précède, la $\mathbb{Z}_\ell[G]$-structure du quotient $\mathfrak{P}^s/\mathrm{Tr}_{N/K}(\mathfrak{P}^s)$ est donnée par l'isomorphisme :

$$\mathfrak{P}^s/\mathrm{Tr}_{N/K}(\mathfrak{P}^s) \simeq \Big(\bigoplus_{\varphi | \Phi_1} \Lambda_\varphi\Big) \oplus \Big(\bigoplus_{\varphi | \Phi_2} \Lambda_\varphi\Big).$$

L'égalité $\Phi_1 = \Phi_2$ caractérise donc ceux de ces quotients qui sont libres sur $\Lambda = \mathbb{Z}_\ell[\zeta \circ T]$.

Lorsqu'elle a lieu, le module $\mathfrak{M}\mathfrak{P}^s$ s'écrit comme somme directe :

$$\mathfrak{M}\mathfrak{P}^s \simeq \Big(\bigoplus_{\varphi | \Phi} \Lambda_\varphi\Big) \oplus \Big(\bigoplus_{\varphi \nmid \Phi} \Lambda_\varphi\Big) \oplus \mathbb{Z}_\ell[T] \simeq \mathfrak{M} ;$$

de sorte que l'ordre $\mathfrak{O}^s$ associé à $\mathfrak{P}^s$ est contenu dans $\mathfrak{M}$. Un calcul immédiat montre qu'il est engendré sur $\mathbb{Z}_\ell[G]$ par les idempotents centraux attachés aux φ divisant Φ.

Corollaire. L'anneau $\mathfrak{A}$ et l'idéal $\mathfrak{P}$ sont libres sur leurs ordres respectifs dans l'algèbre $\mathbb{Q}_\ell[G]$. L'ordre $\mathfrak{O}(\mathfrak{P})$ est engendré sur $\mathbb{Z}_\ell[G]$ par les idempotents $\frac{\nu}{\ell} e_{\theta\psi^k}$, pour $\theta \in (T/I)^*$ et $k = 1, \ldots, t-1$; et l'ordre $\mathfrak{O}(\mathfrak{A})$ contient en outre les idempotents correspondant à $k = 0$.

En tant que $\mathbb{Z}_\ell[G]$-module, l'anneau des entiers $\mathfrak{A}$ s'écrit comme somme directe :

$$\mathfrak{A} \simeq \bigoplus_{\theta \in (T/I)^*} \Big[\Big(\bigoplus_{\substack{k=0 \\ k \neq e}}^{t-1} \big(\Gamma_{\theta\psi^k} \oplus \Lambda_{\theta\psi^k}\big)\Big) \oplus \Big(\bigoplus_{k=t}^{e-1} \Xi_{\theta\psi^k}\Big)\Big],$$

Et, dans cet isomorphisme, l'idéal maximal $\mathfrak{P}$ est représenté par le sous-module :

$$\mathfrak{P} \simeq \bigoplus_{\theta \in (T/I)^*} \Big[\ell\,\Xi_{\theta\psi^0} \oplus \Big(\bigoplus_{k=1}^{t-1} \big(\Gamma_{\theta\psi^k} \oplus \Lambda_{\theta\psi^k}\big)\Big) \oplus \Big(\bigoplus_{k=t}^{e-1} \Xi_{\theta\psi^k}\Big)\Big],$$

lorsque le saut de ramification est strictement inférieur à ℓ ;

$$\mathfrak{P} \simeq \bigoplus_{\theta \in (T/I)^*} \Big[\big(\ell\,\Gamma_{\theta\psi^0} \oplus \Lambda_{\theta\psi^0}\big) \oplus \Big(\bigoplus_{k=1}^{\ell-2} \big(\Gamma_{\theta\psi^k} \oplus \Lambda_{\theta\psi^k}\big)\Big) \simeq \mathfrak{A},$$

sinon.

5. EXTENSION AUX ENTIERS D'UN CORPS GLOBAL

Etudions maintenant le cas d'une extension globale N, métacyclique de degré $n\ell$ sur le corps des rationnels, sauvagement ramifiée au-dessus de ℓ.

Comme plus haut, notons G le groupe de Galois $\mathrm{Gal}(N/\mathbb{Q})$, puis S le sous-groupe dérivé, T un relèvement du quotient G/S en un sous-groupe de G, et χ le caractère définissant l'action de T sur S.

Introduisons le sous-corps K des invariants de S, qui est une extension cyclique de degré n sur $\mathbb{Q}$ et dont le groupe de Galois est isomorphe à T ; puis désignons par D le sous-groupe de décomposition de ℓ dans K, par I le sous-groupe d'inertie, et par H le sous-groupe métacyclique de G, produit semi-direct de S et de D. Notons enfin :

A_N l'anneau des entiers de N ; et $\mathcal{P}$ l'idéal ambige maximal au dessus de ℓ ;

$\mathfrak{A}$ le complété de A_N en $\mathcal{P}$, et $\mathfrak{P}$ son idéal maximal ;

$\mathcal{A}$ le tensorisé $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} A_N$, et $P = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{P}$;

puis, de façon semblable :

A_K l'anneau des entiers de K ; et p la trace de $\mathcal{P}$ sur A_K ;

$\mathfrak{a}$ le complété de A_K en p, et $\mathfrak{p}$ son idéal maximal ;

a le tensorisé $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} A_K$, et $p = \mathbb{Z}_\ell \otimes_{\mathbb{Z}}$ p.

A l'anneau $\mathfrak{A}$ qui est métacyclique de degré $m\ell$ (divisant $n\ell$) sur $\mathbb{Z}$, et dont le groupe de Galois s'identifie à H, nous pouvons appliquer les résultats de l'étude précédente. C'est ainsi que nous avons les isomorphismes de $\mathbb{Z}_\ell[D]$-modules :

$$\mathfrak{a}/\mathfrak{p} \simeq \mathbb{F}_\ell[D/I] \qquad \text{et} \qquad \mathfrak{a} \simeq \mathbb{F}_\ell[D] \ ;$$

puis par passage à la représentation induite :

$$a/p \simeq \mathbb{F}_\ell[T/I] \qquad \text{et} \qquad a \simeq \mathbb{F}_\ell[T].$$

Il est bien connu en effet que l'anneau $\mathcal{A} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} A_N$ s'obtient par induction à partir de $\mathfrak{A}$; autrement dit que l'on a :

$$\mathfrak{a} = \mathbb{Z}_\ell[G] \otimes_{\mathbb{Z}_\ell[H]} \mathfrak{A}$$

En particulier nous obtenons immédiatement à partir du théorème 3 :

Theoreme 4. Etant donnée une extension métacyclique de degré $n\ell$ sur le corps des rationnels, le tensorisé $\mathfrak{a} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} A_N$ de l'anneau de ses entiers s'écrit comme somme directe de $\mathbb{Z}_\ell[G]$ modules :

$$\mathfrak{a} \simeq \bigoplus_{\theta \in (D/I)^*} \left[\left(\bigoplus_{k=0}^{t-1} \left(\Gamma_{\Theta\Psi^k} \oplus \Lambda_{\Theta\Psi^k}\right)\right) \oplus \left(\bigoplus_{k=t}^{e-1} \Xi_{\Theta\Psi^k}\right)\right]$$

lorsque le saut de ramification est strictement inférieur à ℓ ; l'écriture $\Theta\Psi^k$ représentant l'induit dans T du caractère $\theta\psi^k$ du sous-groupe de décomposition D :

$$\mathfrak{a} \simeq \bigoplus_{\theta \in T^*} \left(\Gamma_\theta \oplus \Lambda_\theta\right) \quad \text{sinon.}$$

En particulier $\mathfrak{a}$ est toujours libre sur son ordre associé dans $\mathbb{Z}_\ell[G]$.

Démonstration : Le cas sauvage s'obtient par induction ; tandis que le cas modéré résulte de la surjectivité de l'application trace $\nu = Tr_{N/K}$ qui entraine $\mathfrak{a} \simeq \mathbb{Z}_\ell[G]$.

Tout comme dans le cas local, nous obtenons ainsi :

Corollaire 1. Le quotient $\mathfrak{a}/a$ est isomorphe à l'algèbre héréditaire $\Lambda = \mathbb{Z}_\ell[\zeta \circ T]$.

Ce qui est une version affaiblie d'un résultat plus général, puisqu'on peut montrer que le quotient A_N/A_K est en fait libre sur $\mathbb{Z}[\zeta \circ T]$ (cf [4]).

Corollaire 2. L'ordre $\mathfrak{O}(\mathfrak{a})$ est engendré sur $\mathbb{Z}_\ell[G]$ par les idempotents $\frac{\nu}{\ell}\, e_\varphi$ associés aux facteurs irréductibles φ des caractères induits $\Theta\Psi^k$ par les $\theta\psi^k$ lorsque θ décrit le groupe $(T/I)^*$ et k le segment $0, 1, \ldots, (t-1)$.

Corollaire 3. L'anneau des entiers d'une extension métacyclique de degré $n\ell$ sur le corps des rationnels est localement libre sur son ordre associé dans l'algèbre du groupe de Galois.

Démonstration : Compte tenu du théorème, il suffit de regarder $\mathfrak{a}_q = \mathbb{Z}_q \otimes_{\mathbb{Z}} A_N$, pour les q différents de ℓ. Or, pour un tel premier q, le tensorisé $\mathfrak{a}_q$ se scinde en deux termes :

$$\mathfrak{a}_q = \left(\frac{\nu - \ell}{\ell}\right) \mathfrak{a}_q \oplus \frac{\nu}{\ell}\, \mathfrak{a}_q .$$

Le premier terme s'identifie au produit tensoriel $\mathbb{Z}_q \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta \circ T]$; et le second, $\mathbb{Z}_q \otimes_{\mathbb{Z}} A_K$ est bien libre sur son ordre associé dans $\mathbb{Z}_q[T]$, d'après le résultat de Leopoldt.

Rappelons que pour $n = 2$ ce dernier corollaire entraine que l'anneau A_N est en fait libre sur son ordre associé dans $\mathbb{Q}[G]$ (cf. [1]).

Pour illustrer les résultats qui précèdent, considérons le cas des extensions kummeriennes de degré ℓ sur le corps cyclotomique $\mathbb{Q}[\zeta]$, qui sont non ramifiées en dehors de ℓ.

Supposons, pour simplifier, ℓ régulier et notons K le corps cyclotomique $\mathbb{Q}[\zeta]$, $T = \mathrm{Gal}(K/\mathbb{Q})$ son groupe de Galois, T/T_o celui de son sous-corps réel maximal et ω le caractère de l'action de T sur le groupe des racines $\ell^{\text{ièmes}}$ de l'unité. Cela étant, pour tout caractère pair $\varphi = \omega^{2h}$ de T, faisons choix d'une section $\bar{\varphi}$ modulo ℓ, à valeurs dans $\mathbb{Z}$, et telle que la somme $\sum_{\tau \in T} \bar{\varphi}(\tau)$ soit nulle.

Définissons alors N_φ par $K[\sqrt[\ell]{\varepsilon_{\bar{\varphi}}}]$ en prenant pour $\varepsilon_{\bar{\varphi}}$

- l'entier ℓ si φ est le caractère unité,

- l'unité cyclotomique $\prod_{\tau \in T} \left(\zeta^{\omega(\tau)} - \zeta^{-\omega(\tau)}\right)^{\bar{\varphi}(\tau^{-1})}$ sinon.

Il est bien connu que les $\frac{\ell-1}{2}$ corps N_φ ainsi définis engendrent, avec le corps cyclotomique $\mathbb{Q}[\zeta_{\ell^2}]$, la ℓ-extension abélienne maximale ℓ-ramifiée de $\mathbb{Q}[\zeta]$.

Cela étant, la congruence :

$\varepsilon_{\bar{\varphi}}^{\tau} \equiv \varepsilon_{\bar{\varphi}}^{\bar{\varphi}(\tau)}$ [mod E_K^ℓ] dans le groupe des unités E_K, nous prouve

que le corps K_φ est une extension normale de degré $\ell(\ell-1)$ sur $\mathbb{Q}$, qui est métacyclique, de caractère :

$$\chi = \omega\,\varphi^{-1} = \omega^{\ell-2h}.$$

Or, puisque N_φ est totalement et sauvagement ramifiée sur $\mathbb{Q}$, son complété ℓ-adique est une extension métacyclique de degré $\ell(\ell-1)$ sur $\mathbb{Q}_\ell$. D'après le lemme 4, la relation précédente nous assure que le saut de ramification t est égal à $\ell-2h$.

La structure de l'anneau des entiers est donc donnée par l'isomorphisme :

$$\mathfrak{A} \simeq \left(\Gamma_{\omega^0} \oplus \Lambda_{\omega^0}\right) \oplus \left(\Gamma_\omega \oplus \Lambda_\omega\right) \oplus \ldots \oplus \left(\Gamma_{\varphi-1} \oplus \Lambda_{\varphi-1}\right) \oplus \Xi_{\omega\varphi-1} \oplus \ldots \oplus \Xi_{\omega^{\ell-2}} ;$$

tandis que celle de l'idéal maximal s'écrit :

$$\mathfrak{P} \simeq \Xi_{\omega^0} \oplus \left(\Gamma_\omega \oplus \Lambda_\omega\right) \oplus \ldots \oplus \left(\Gamma_{\varphi-1} \oplus \Lambda_{\varphi-1}\right) \oplus \Xi_{\omega\varphi-1} \oplus \ldots \oplus \Xi_{\omega^{\ell-2}} .$$

BIBLIOGRAPHIE

[1] A.-M. BERGE
Sur l'arithmétique d'une extension diédrale.
Ann. Sc. Inst. Fourier, 22 (1972), p. 31-59.

[2] J. COUGNARD
Un contre exemple à une conjecture de J. Martinet.
Algebraic Number Fields, Academic Press, London (1977), p. 539-560.

[3] J. COUGNARD
Une propriété de l'anneau des entiers des extensions galoisiennes non abéliennes de degré pq des rationnels.
Comp. Mathematica (à paraitre).

[4] J. COUGNARD
Remarques sur l'arithmétique de certaines extensions métacycliques.
(à paraitre).

[5] M.-J. FERTON
Sur les idéaux d'une extension cyclique de degré premier d'un corps local.
Sém. Th. Nombres, Grenoble (1972-1973).

[6] A. FROHLICH
A normal integral basis theorem.
J. of Alg., 39 (1976), p. 131-137.

[7] J.-F. JAULENT
Remarques sur la structure galoisienne des entiers d'une extension métacyclique de $\mathbb{Q}$.
C.R. Acad. Sc. Paris.

[8] LENA CHANG PU
Integral representations of non abelian groups of order pq.
Mich. math. J., 15 (1975).

[9] H.-W. LEOPOLDT
Uber die Hauptordnung der ganzen Elementen eines abelshen Zahlkörpers.
J. für die reine und angew. Math., 201 (1959), p. 119-149.

[10] J. MARTINET
Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre 2p.
Ann. Sc. Inst. Fourier, 19 (1969), p. 1-80.

[11] E. NŒTHER
Normalbasis bei Körpern ohne höhere Verzweigung.
J. für die reine und angew. Math., 167 (1931), p. 147-152.

[12] I. REINER
Maximal orders.
Academic Press, London (1975).

[13] M. ROSEN
Representations of twisted group rings.
Ph. D. Thesis, Princeton (1963).

[14] J.-P. SERRE
Corps locaux.
Hermann, Paris (1968).

[15] S. ULLOM
Integral normal basis in Galois extensions of local fields.
Nagoya Math. J., 39 (1970), p. 141-148.

Jean-François JAULENT
E.R.A. n°070654
Université de Franche-Comté
Faculté des Sciences - Mathématiques
Route de Gray - La Bouloie
25030 BESANCON CEDEX