THEORIE DES NOMBRES
BESANÇON

Années 1979-1980
et 1980-1981

MODULES D'ENTIERS D'UNE EXTENSION ABELIENNE SUR SON ORDRE MAXIMAL

Danièle CHATELAIN

MODULES D'ENTIERS D'UNE EXTENSION ABELIENNE SUR SON ORDRE MAXIMAL

Problème étudié.

Soit $K/\mathbb{Q}$ une extension abélienne de groupe G, O_K l'anneau des entiers de K, $\mathfrak{M}$ l'ordre maximal (unique) de $\mathbb{Q}[G]$ et $\tilde{O}_K$ le plus grand $\mathfrak{M}$-module inclus dans O_K. On montre que $\tilde{O}_K$ est isomorphe à $\mathfrak{M}$.

Ce résultat se situe dans l'étude plus générale du problème suivant : étant donné une extension galoisienne K/k sauvagement ramifiée, de groupe de Galois G, O_K est un $\mathbb{Z}[G]$-module non localement libre. On cherche à lui associer un module localement libre.
Si on choisit un ordre maximal $\mathfrak{M}$ de $k[G]$ ou de $\mathbb{Q}[G]$ on peut considérer le $\mathfrak{M}$-module localement libre $\tilde{O}_{K,\mathfrak{M}}$, défini comme le plus grand $\mathfrak{M}$-module inclus dans O_K et étudier sa structure.
M.J. Taylor obtient ainsi certains résultats pour une extension K/k de Kummer ou pour certains groupes G ($[T_1]$, $[T_2]$).

I.- Rappel des théorèmes de Léopoldt et Jacobinski. Résolution du cas $K/\mathbb{Q}$ modéré.

1°) Notations :

On désigne par $\mathbb{Q}^{(n)}$ le corps des racines de l'unité d'ordre n et par $\mathbb{Z}^{(n)}$ l'anneau des entiers de $\mathbb{Q}^{(n)}$.
On note $\hat{C}$ le groupe des caractères absolument irréductibles d'un groupe abélien C et pour tout $\chi \in \hat{C}$, on note $\bar{\chi}$ le $\mathbb{Q}$-caractère irréductible de C associé à χ ; on a :

$$\overline{\chi} = \sum_{\alpha \in \mathrm{gal}(\mathbb{Q}^{(n)}/\mathbb{Q})} \chi^{\alpha}$$

où n est l'ordre de χ .

Si $\varphi = \chi_1 + \ldots + \chi_k$ est une somme de caractères $\chi_i \in \hat{C}$, deux à deux distincts on pose :

$$1_{\varphi} = \frac{1}{|C|} \sum_{g \in C} \varphi(g^{-1})\, g$$

1_{φ} est un idempotent de $\mathbb{C}[C]$. En particulier pour $\chi \in \hat{C}$, 1_{χ} et $1_{\overline{\chi}}$ sont des idempotents primitifs de $\mathbb{C}[C]$ et $\mathbb{Q}[C]$ respectivement.

2°) Théorème de Léopoldt ([L]) .

a) Définition des caractères de ramification de l'extension abé - lienne $K/\mathbb{Q}$, de groupe G .

Soit $\chi \in \hat{G}$, f_{χ} le conducteur du corps fixe de Ker χ . Les ca - ractères de ramification ϕ de $K/\mathbb{Q}$ sont les sommes des $\chi \in \hat{G}$ apparte- nant à une même classe d'équivalence de $\hat{G}$ pour la relation :
$\chi \sim \chi'$ si et seulement si pour tout p premier tel que p^2 divise f_{χ} ou $f_{\chi'}$, les p-composantes $f_{\chi}^{(p)}$ et $f_{\chi'}^{(p)}$ de f_{χ} et $f_{\chi'}$ sont égales .

Il est clair que chaque caractère de ramification ϕ est rationnel et Léopoldt montre que ϕ est induit par un $\mathbb{Q}$-caractère irréductible $\overline{\psi}$ d'un sous-groupe H_{ϕ} de G .

Rappelons la définition de H_{ϕ} :
soit $G^i(p)$ le i^{eme} groupe de ramification supérieure de l'idéal $\mathfrak{P}$ de K au-dessus de p ; si K est un corps tel que $G^1(2) = G^2(2)$, on a $H_{\phi} = \prod_p G^1(p)$ quel que soit ϕ . Sinon on a soit $H_{\phi} = \prod_p G^1(p)$, soit $H_{\phi} = G^2(2) \prod_{p \neq 2} G^1(p)$ selon que ϕ correspond à la classe d'un caractère χ tel que $f_{\chi}^{(2)}$ divise 2^2 ou tel que 2^3 divise $f_{\chi}^{(2)}$.

La description exacte de la correspondance entre les carac - tères de ramification et les $\mathbb{Q}$-caractères irréductibles des groupes $\prod_p G^1(p)$ et $G^2(2) \prod_{p \neq 2} G^1(p)$ ne sera pas utilisée ultérieurement.

Pour la suite on utilise la propriété suivante :

Si ϕ est le caractère de ramification de l'extension $K/\mathbb{Q}$, associé au caractère $\chi \in \hat{G}$, il existe un sous-groupe H de G tel que :

$$\phi = \mathrm{Ind}_H^G \overline{\psi} \quad \text{avec } \psi = \mathrm{Res}_H \chi \quad (\psi \in \hat{H})$$

ϕ est alors la somme de tous les caractères $\chi' \in \hat{G}$ tels que $\mathrm{Res}_H \chi' = \psi^\alpha$ pour les $\mathbb{Q}$-conjugués ψ^α de ψ. On remarque que $\mathrm{Ker}\,\psi \subset \mathrm{Ker}\,\chi$, l'ordre de ψ divise donc l'ordre de χ et $1_\phi = 1_{\overline{\psi}}$.

b) <u>Théorème de Léopoldt</u>.

Soit O_K l'anneau des entiers de K.

1) Soit O l'ordre de $\mathbb{Q}[G]$ associé à O_K (ensemble des $\lambda \in \mathbb{Q}[G]$ tels que $\lambda O_K \subset O_K$) alors O_K est libre sur O.

2) $O = \bigoplus_\phi \mathbb{Z}[G]\, 1_\phi$ (la somme porte sur l'ensemble des caractères de ramification ϕ de K).

<u>Remarques</u> :

1) Si l'extension $K/\mathbb{Q}$ est modérée, on a $\prod_p G^1(p) = \{1\}$ et $O = \mathbb{Z}[G]$.

2) Si $K/\mathbb{Q}$ est totalement ramifiée (et alors nécessairement cyclique) on a $\prod_p G^1(p) = G$ et les caractères de ramification de K coïncident avec les $\mathbb{Q}$-caractères irréductibles de G ; O est égal à l'ordre maximal $\mathfrak{M}$ de $\mathbb{Q}[G]$ $\left(\mathfrak{M} = \bigoplus_{\overline{\chi}} \mathbb{Z}[G]\, 1_{\overline{\chi}}\right)$.

c) <u>Corollaire 1</u>.

Soit $T_K \in O_K$ tel que $O_K = O \,.\, T_K$.

Soit $\tilde{O}_K$ le plus grand $\mathfrak{M}$-module inclus dans O_K et $\tilde{O}$ le plus grand idéal de $\mathfrak{M}$ inclus dans O ; alors

$$\tilde{O}_K = \tilde{O}\, T_K \quad \text{et} \quad \tilde{O} = \bigoplus_{\overline{\chi}} \left[\mathbb{Z}[G]\, 1_{\overline{\psi}_{\overline{\chi}}} \cap \mathbb{Z}[G]\, 1_{\overline{\chi}} \right]$$

où $\overline{\chi}$ décrit l'ensemble des $\mathbb{Q}$-caractères irréductibles de G et $\overline{\psi}_{\overline{\chi}}$ est le $\mathbb{Q}$-caractère irréductible du sous-groupe H_ϕ de G (associé à la classe de ramification ϕ de χ) tel que $\overline{\mathrm{Res}_{H_\phi} \chi} = \overline{\psi}_{\overline{\chi}}$.

Démonstration :

$\tilde{O}$ étant un $\mathfrak{M}$-module avec $\mathfrak{M} = \underset{\bar{\chi}}{\oplus} \mathbb{Z}[G]\, 1_{\bar{\chi}}$, on a :

$$\tilde{O} = \underset{\bar{\chi}}{\oplus} \tilde{O}\, 1_{\bar{\chi}}$$

$$O \cap \mathbb{Z}[G]\, 1_{\bar{\chi}} = \Big(\underset{\bar{\psi}}{\oplus} \mathbb{Z}[G]\, 1_{\bar{\psi}}\Big) \cap \mathbb{Z}[G]\, 1_{\bar{\chi}} = \mathbb{Z}[G]\, 1_{\bar{\psi}_{\bar{\chi}}} \cap \mathbb{Z}[G]\, 1_{\bar{\chi}} .$$

En effet , pour $\bar{\psi} \neq \bar{\psi}_{\bar{\chi}}$ on a $1_{\bar{\chi}} \cdot 1_{\bar{\psi}} = 0$ et $1_{\bar{\psi}_{\bar{\chi}}} \cdot 1_{\bar{\chi}} = 1_{\bar{\chi}}$.

On en déduit que $O \cap \mathbb{Z}[G]\, 1_{\bar{\chi}}$ est un $\mathbb{Z}[G] . 1_{\bar{\chi}}$ -module et donc que :

$$\tilde{O}\, 1_{\bar{\chi}} = \mathbb{Z}[G]\, 1_{\bar{\psi}_{\bar{\chi}}} \cap \mathbb{Z}[G]\, 1_{\bar{\chi}} .$$

<u>Montrer que $\tilde{O}_K$ est isomorphe à $\mathfrak{M}$</u> , <u>est donc équivalent à montrer que pour chaque $\mathbb{Q}$-caractère irréductible $\bar{\chi}$ de G</u> , <u>l'idéal</u> $\tilde{O} . 1_{\bar{\chi}} = \mathbb{Z}[G]\, 1_{\bar{\psi}_{\bar{\chi}}} \cap \mathbb{Z}[G]\, 1_{\bar{\chi}}$ <u>est un idéal principal de l'anneau</u> $\mathbb{Z}[G]\, 1_{\bar{\chi}}$ (anneau isomorphe à l'anneau $\mathbb{Z}^{(n)}$ des entiers de $\mathbb{Q}^{(n)}$, pour n ordre de χ) .

On voit que ce résultat est trivial si $O = \mathfrak{M}$ $\Big($car $\mathbb{Z}[G]\, 1_{\bar{\psi}_{\bar{\chi}}} = \mathbb{Z}[G]\, 1_{\bar{\chi}}\Big)$ c'est-à-dire dans le cas où $K/\mathbb{Q}$ est totalement ramifié .

Dans l'autre cas extrême où l'extension $K/\mathbb{Q}$ est modérée ($O = \mathbb{Z}[G]$) le résultat est un cas particulier du théorème de Jacobinski et on verra que le cas général se ramène aussi au théorème de Jacobinski .

3°) <u>Théorème de Jacobinski</u> ([J]) .

Soient $\mathfrak{G}$ un groupe fini d'ordre n (non nécessairement abélien), O un anneau de Dedekind , k son corps de fraction (on suppose que la caractéristique de k ne divise pas n) , $\mathfrak{M}$ un ordre maximal de $k[\mathfrak{G}]$ contenant $\Lambda = O[\mathfrak{G}]$, soit $A = k[\mathfrak{G}]$. On note :

$$[\mathfrak{M} : \Lambda]_g = \{ x \in A \, ; \, x\mathfrak{M} \subset \Lambda \}$$
$$[\mathfrak{M} : \Lambda]_d = \{ x \in A \, ; \, \mathfrak{M}x \subset \Lambda \}$$

$[\mathfrak{M} : \Lambda]_g$, (resp. $[\mathfrak{M} : \Lambda]_d$) est le conducteur à gauche (resp. à droite) de $\mathfrak{M}$ dans Λ , c'est le plus grand $\mathfrak{M}$-module à droite (resp. à gauche) inclus dans Λ .

Soit $A = \bigoplus_i A_i$, la décomposition de A en composantes simples .

Soient K_i le centre de A_i , $n_i^2 = [A_i : K_i]$, O_i la clôture intégrale de O dans K_i ; on a $\mathfrak{M} = \bigoplus_i \mathfrak{M}_i$ avec $\mathfrak{M}_i$ ordre maximal de O_i dans A .

<u>Théorème de Jacobinski</u> : On a $[\mathfrak{M} : \Lambda]_g = [\mathfrak{M} : \Lambda]_d = \sum_i \frac{n}{n_i} \mathfrak{D}_i^{-1}$

où $\mathfrak{D}_i$ est la différente de $\mathfrak{M}_i$ relativement à O

$\left(\mathfrak{D}_i^{-1} = \left\{ x \in A_i \, ; \, T_{\mathrm{red}_{A_i/K}} (x\mathfrak{M}_i) \subset O \right\} \right.$.

<u>Remarque</u> : Si $\mathfrak{G}$ est abélien , A_i/k est une extension abélienne et

$$[\mathfrak{M} : \Lambda] = \sum_i |\mathfrak{G}| \, . \, \mathfrak{D}_i^{-1}$$

où $\mathfrak{D}_i$ est la différente de l'extension A_i/k .

<u>Corollaire 2</u> .

Si l'extension $K/\mathbb{Q}$ est modérée , alors $\tilde{O}$ est isomorphe à $\mathfrak{M}$.

En effet on a d'après le théorème de Jacobinski

$$\tilde{O} = [\mathfrak{M} : \mathbb{Z}[G]] = \bigoplus_{\underline{\chi}} |G| \, \mathfrak{D}_{\underline{\chi}}^{-1}$$

où $\mathfrak{D}_{\underline{\chi}}^{-1}$ est la différente de l'extension cyclotomique $\mathbb{Q}[G] \, 1_{\underline{\chi}} / \mathbb{Q}$, isomorphe à $\mathbb{Q}^{(n)}/\mathbb{Q}$ (si n est l'ordre de χ) . On sait bien que $\mathfrak{D}_{\underline{\chi}}^{-1}$ est un idéal principal :

$$\mathfrak{D}_{\underline{\chi}}^{-1} = \left(\frac{1}{n} \prod_{p/n} (1 - \zeta_p) \right)$$

(où ζ_p est une racine primitive p^{eme} de 1) .

II.- Etude de $\tilde{O}.1_{\bar\chi}$ dans le cas général.

Dans la suite on note (sans l'indice $\bar\chi$) , H le sous-groupe de G , et ψ le Q-caractère irréductible de H , associés à $\bar\chi$ (par le corollaire 1) et tels que

$\psi = \mathrm{Res}_H \chi$ et $\tilde{O}.1_{\chi} = \mathbb{Z}[G]\,1_{\bar\psi} \cap \mathbb{Z}[G]\,1_{\bar\chi}$

1°) Réduction au cas où χ est un caractère fidèle de G .

Soit K_χ le corps fixe de Ker χ , G_o le groupe de Galois de $K_\chi/\mathbb{Q}$, s la surjection canonique (restriction) de G sur G_o et χ_o le caractère de G_o déduit de χ ($\chi_o \circ s = \chi$) . Alors χ_o est fidèle . On note :

$$e_o = \frac{\sum\limits_{h \in \mathrm{Ker}\,\chi} h}{|\,\mathrm{Ker}\,\chi\,|}$$

On sait alors que s définit un isomorphisme de $\mathbb{Q}[G].e_o$ sur $\mathbb{Q}[G_o]$. Cet isomorphisme envoie $\mathfrak{M}.e_o$ sur l'ordre maximal $\mathfrak{M}_o$ de $\mathbb{Q}[G_o]$. On a $1_{\bar\chi} = 1_{\bar\chi}.e_o \in \mathfrak{M}.e_o$. L'image par s de $\mathbb{Z}[G]\,1_{\bar\chi}$ est $\mathbb{Z}[G_o]\,1_{\bar\chi_o}$ $\left(\text{avec } \mathbb{Z}[G]\,1_{\bar\chi} \cong \mathbb{Z}[G_o]\,1_{\bar\chi_o} \cong \mathbb{Z}^{(n)} \text{ si n est l'ordre de } \chi\right)$.

Notons O_{K_χ} l'anneau des entiers de K_χ et O_o l'ordre de $\mathbb{Q}[G_o]$ associé à O_{K_χ} . Soit $\tilde{O}_{K_\chi}$ et $\tilde{O}_o$ les plus grands $\mathfrak{M}_o$-modules inclus respectivement dans O_{K_χ} et O_o .

Lemme 1 .

1) $\tilde{O}_K . e_o = \tilde{O}_{K_\chi}$

2) Les structures de $\tilde{O}.1_{\bar\chi}$ comme $\mathbb{Z}[G]\,1_{\bar\chi}$ - module et de $\tilde{O}_o.1_{\bar\chi_o}$ comme $\mathbb{Z}[G_o]\,1_{\bar\chi_o}$ - module sont les mêmes .

Démonstration :

1) D'après J. Cougnard - séminaire de Besançon .

$\mathfrak{M}$ étant maximal et e_o un idempotent de $\mathbb{Q}[G]$ on a :

$$\mathfrak{M} = \mathfrak{M} e_o \oplus \mathfrak{M}(1 - e_o)$$

d'où pour le $\mathfrak{M}$-module $\tilde{O}_K$: $\tilde{O}_K e_o \oplus \tilde{O}_K (1 - e_o)$.

$\tilde{O}_K . e_o$ est donc le plus grand $\mathfrak{M}.e_o$ module inclus dans O_K .

$\tilde{O}_{K_\chi}$ est aussi un $\mathfrak{M}.e_o$ module inclus dans O_{K_χ} donc dans O_K .

On en déduit $\tilde{O}_{K_\chi} \subset \tilde{O}_K e_o$.

$\tilde{O}_K e_o$ est inclus dans $\tilde{O}_K$ donc dans O_K et dans $K.e_o = Tr_{K/K_\chi} K = K_\chi$

donc dans $O_{K_\chi} = O_K \cap K_\chi$; c'est un $\mathfrak{M}.e_o$ module donc un $\mathfrak{M}_o$-module .

Par définition de $\tilde{O}_{K_\chi}$ on a donc $\tilde{O}_K e_o \subset \tilde{O}_{K_\chi}$.

D'où : $$\tilde{O}_K . e_o = \tilde{O}_{K_\chi} .$$

2) Soient $T_K \in O_K$ et $T_{K_\chi} \in O_{K_\chi}$ tels que $O_K = O . T_K$ et

$O_{K_\chi} = O_o T_{K_\chi}$. On a d'après le corollaire 1 , $\tilde{O}_K = \tilde{O}\, T_K$ et

$\tilde{O}_{K_\chi} = \tilde{O}_o T_{K_\chi}$ d'où :

$$\tilde{O}_o . T_{K_\chi} = \tilde{O} . e_o . T_K = \tilde{O} . e_o . (e_o T_K) = s(\tilde{O} e_o) . (e_o T_K)$$

Or $$e_o T_K = \frac{Tr_{K/K_\chi}(T_K)}{|\mathrm{Ker}\ \chi|} \in K_\chi = \mathbb{Q}[G_o] . T_{K_\chi} .$$

Il existe donc $a_o \in \mathbb{Q}[G_o]$ tel que $e_o . T_K = a_o . T_{K_\chi}$.

D'où :

$$\tilde{O}_o = s(\tilde{O} e_o) a_o \quad \text{et} \quad \tilde{O}_o . 1_{\bar{\chi}_o} = s\left(\tilde{O} . 1_{\bar{\chi}}\right)\left(a_o 1_{\bar{\chi}_o}\right) \simeq s\left(\tilde{O}\, 1_{\bar{\chi}}\right) \simeq \tilde{O} . 1_{\bar{\chi}} .$$

Dans la suite , pour l'étude de $\tilde{O}\, 1_{\bar{\chi}} = \mathbb{Z}[G]\, 1_{\bar{\chi}} \cap \mathbb{Z}[G]\, 1_{\bar{\psi}}$, comme module sur $\mathbb{Z}[G]\, 1_{\overline{\chi}}$ on suppose que χ est un caractère fidèle de G (et donc que G est cyclique) .

2°) Réduction au cas $G = H.S$ (produit direct) avec card G sans facteurs carrés .

Lemme 2 .

Soit C un groupe cyclique d'ordre $m = m_o m'$ avec $m_o = \prod_{p/m} p$ (p premier) . Soit $\chi \in \hat{C}$ un caractère fidèle et C_o l'unique sous - groupe de C d'ordre m_o . Soit χ_o la restriction de χ à C_o . Alors

$$\mathrm{Ind}_{C_o}^{C} \overline{\chi}_o = \overline{\chi} \quad \text{et} \quad 1_{\overline{\chi}} = 1_{\overline{\chi}_o} \in \mathbb{Q}[C_o]$$

avec χ_o d'ordre m_o sans facteurs carrés .

Démonstration :

On peut calculer directement les valeurs de $\overline{\chi}$ et de $\mathrm{Ind}_{C_o}^{C} \overline{\chi}_o$ et constater l'égalité .

On peut aussi remarquer que d'après la formule de réciprocité de Frö- benius $\left(\langle \chi' , \mathrm{Ind}_{C_o}^{C} \overline{\chi}_o \rangle = \langle \mathrm{Res}_{C_o} \chi' , \overline{\chi}_o \rangle \right)$, le caractère $\mathrm{Ind}_{C_o}^{C} \overline{\chi}_o$ est la somme de tous les $\chi' \in \hat{C}$, prolongeant les conjugués de χ_o dans $\hat{C}_o$ ($\overline{\chi}_o$ est la somme des $\mathbb{Q}$ conjugués de χ_o) χ étant fidèle , est d'ordre card $C = m$; χ_o est aussi fidèle et d'ordre Card $C_o = m_o$. χ_o admet $\varphi(m_o)$ conjugués qui sont les χ_o^i $((i, m_o) = 1)$. Chaque χ_o^i admet m' prolongements à C qui sont les $\chi^i \cdot \chi^{m_o j}$ (pour $1 \leq j \leq m'$) ; m_o a été choisi de telle sorte que $m = m' m_o$ et m_o ad - mette mêmes diviseurs premiers que m . Les caractères $\chi^i \chi^{m_o j}$ sont donc d'ordre m et l'on a $m' \varphi(m_o) = \varphi(m)$. Le caractère $\mathrm{Ind}_{C_o}^{C} \overline{\chi}_o$

est donc la somme des $\varphi(m)$ conjugués de χ et est égal à $\overline{\chi}$ $\Big($ d'où $1_{\overline{\chi}} = 1_{\overline{\chi}_o}$ $\Big)$.

<u>Remarque</u> : C_o est le plus petit sous-groupe de C tel que $\mathrm{Ind}_{C_o}^{C}\left(\overline{\mathrm{Res}_{C_o}\chi}\right)$ reste Q-irréductible.

<u>Lemme 3</u>.

Soit G un groupe cyclique d'ordre $n = n_o n'$ $\left(\text{avec } n_o = \prod_{p/n} p\right)$ H un sous-groupe de G d'ordre $m = m_o m'$ $\left(\text{avec } m_o = \prod_{p/m} p\right)$. Soit χ un caractère fidèle de G et $\psi = \mathrm{Res}_H \chi$. Soit H_o le sous-groupe de G d'ordre m_o et S le sous-groupe de G d'ordre $r_o = \frac{n_o}{m_o}$; soit χ_o la restriction de χ à $G_o = H_o . S$ (produit direct) et ψ_o la restriction de χ_o à H_o. Alors, $\mathbb{Z}[G]\,1_{\overline{\chi}} \cap \mathbb{Z}[G]\,1_{\overline{\psi}}$ est l'idéal de $\mathbb{Z}[G]\,1_{\overline{\chi}}$ engendré par $\mathbb{Z}[G_o]\,1_{\overline{\chi}_o} \cap \mathbb{Z}[G_o]\,1_{\overline{\psi}_o}$.

<u>Démonstration</u> :

G est cyclique et χ fidèle d'ordre $n = n_o n'$. Le groupe H est donc cyclique et ψ est fidèle d'ordre $m = m_o m'$. On a donc d'après le lemme 2 $\quad 1_{\overline{\psi}_o} = 1_{\overline{\psi}}$ et $1_{\overline{\chi}_o} = 1_{\overline{\chi}}$.

Par ailleurs on peut écrire :

$$\mathbb{Q}[G] = \mathbb{Q}[G_o] \otimes_{\mathbb{Z}[G_o]} \mathbb{Z}[G] ,$$

en définissant le produit tensoriel de $x \in \mathbb{Q}[G_o]$ par $y \in \mathbb{Z}[G]$ comme le produit $x.y$ dans $\mathbb{Q}[G]$.

Comme $\mathbb{Z}[G]$ est un $\mathbb{Z}[G_o]$-module libre (de base un système de représentants de G/G_o), on en déduit que pour tout sous-$\mathbb{Z}[G_o]$-module V de $\mathbb{Q}[G_o]$, on peut identifier $V \otimes_{\mathbb{Z}[G_o]} \mathbb{Z}[G]$ au sous-module $V.\mathbb{Z}[G]$ de $\mathbb{Q}[G]$ et on sait que l'on a pour des sous-modules

V_1 et V_2 de $\mathbb{Q}[G_o]$:

$$\left(V_1 \otimes_{\mathbb{Z}[G_o]} \mathbb{Z}[G]\right) \cap \left(V_2 \otimes_{\mathbb{Z}[G_o]} \mathbb{Z}[G]\right) = (V_1 \cap V_2) \otimes_{\mathbb{Z}[G_o]} \mathbb{Z}[G]$$

D'où en considérant $V_1 = \mathbb{Z}[G_o]\, 1_{\overline{\chi}}$ et $V_2 = \mathbb{Z}[G_o]\, 1_{\overline{\psi}}$

$$\left[\left(\mathbb{Z}[G_o].\, 1_{\overline{\chi}}\right) \otimes_{\mathbb{Z}[G_o]} \mathbb{Z}[G]\right] \cap \left[\left(\mathbb{Z}[G_o].\, 1_{\overline{\psi}}\right) \otimes_{\mathbb{Z}[G_o]} \mathbb{Z}[G]\right] =$$

$$= \left[\mathbb{Z}[G_o].\, 1_{\overline{\chi}} \cap \mathbb{Z}[G_o].\, 1_{\overline{\psi}}\right] \otimes_{\mathbb{Z}[G_o]} \mathbb{Z}[G]$$

c'est-à-dire :

$$\mathbb{Z}[G]\, 1_{\overline{\chi}} \cap \mathbb{Z}[G]\, 1_{\overline{\psi}} = \left[\mathbb{Z}[G_o]\, 1_{\overline{\chi}} \cap \mathbb{Z}[G_o]\, 1_{\overline{\psi}}\right].\mathbb{Z}[G] \quad .$$

3°) <u>Réduction au théorème de Jacobinski</u> .

<u>Lemme 4</u> .

Soit G un groupe cyclique d'ordre n <u>sans facteurs carrés</u> , χ un caractère fidèle de G ; soit H un sous-groupe de G d'ordre m , S le sous-groupe de G d'ordre $\frac{n}{m}$. Soient ψ et η les restrictions de χ à H et S . Alors :

$$\mathbb{Z}[G]\, 1_{\overline{\chi}} \cap \mathbb{Z}[G]\, 1_{\overline{\psi}} = \left[\mathbb{Z}[S] \cap \mathbb{Z}[S]\, 1_{\overline{\eta}}\right] .\ \mathbb{Z}[H]\, 1_{\overline{\psi}}$$

et $\mathbb{Z}[G]\, 1_{\overline{\chi}} \cap \mathbb{Z}[G]\, 1_{\overline{\psi}}$ est un idéal principal de l'anneau $\mathbb{Z}[G]\, 1_{\overline{\chi}}$.

<u>Démonstration</u> :

L'ordre n de G étant sans facteurs carrés on a $G = H.S$ (produit direct) d'où $\chi = \psi.\eta$ et $1_{\overline{\chi}} = 1_{\overline{\psi}} .\ 1_{\overline{\eta}}$.

On peut alors écrire :

$$\mathbb{Q}[G] = \mathbb{Q}[S] \otimes_{\mathbb{Z}} \mathbb{Z}[H]\, 1_{\overline{\psi}}$$

en définissant le produit tensoriel à partir du produit dans $\mathbb{Q}[G]$ et puisque $\mathbb{Z}[H]\, 1_{\overline{\psi}}$ est un $\mathbb{Z}$-module libre (isomorphe à $\mathbb{Z}^{(m)}$) on peut écrire comme dans la démonstration du lemme 3 :

$$\mathbb{Z}[S]1_{\bar\eta} \otimes_{\mathbb{Z}} \mathbb{Z}[H]1_{\bar\psi} = \left(\mathbb{Z}[S].1_{\bar\eta}\right).\left(\mathbb{Z}[H]1_{\bar\psi}\right) = \mathbb{Z}[G]1_{\bar\chi}$$

$$\mathbb{Z}[S] \otimes_{\mathbb{Z}} \mathbb{Z}[H]1_{\bar\psi} = \mathbb{Z}[S].\mathbb{Z}[H]1_{\bar\psi} = \mathbb{Z}[G]1_{\bar\psi}$$

$$\left(\mathbb{Z}[S]1_{\bar\eta} \otimes_{\mathbb{Z}} \mathbb{Z}[H]1_{\bar\psi}\right) \cap \left(\mathbb{Z}[S] \otimes_{\mathbb{Z}} \mathbb{Z}[H]1_{\bar\psi}\right) =$$

$$= \left(\mathbb{Z}[S]1_{\bar\eta} \cap \mathbb{Z}[S]\right) \otimes_{\mathbb{Z}} \mathbb{Z}[H]1_{\bar\psi}$$

d'où :

$$\mathbb{Z}[G]1_{\bar\chi} \cap \mathbb{Z}[G]1_{\bar\psi} = \left(\mathbb{Z}[S]1_{\bar\eta} \cap \mathbb{Z}[S]\right).\mathbb{Z}[H]1_{\bar\psi}\ .$$

D'après le théorème de Jacobinski (corollaire 2) on sait que $\mathbb{Z}[S]1_{\bar\eta} \cap \mathbb{Z}[S]$ est un idéal principal de l'anneau $\mathbb{Z}[S]1_{\bar\eta}$. On en déduit que $\mathbb{Z}[G]1_{\bar\chi} \cap \mathbb{Z}[G]1_{\bar\psi}$ est un idéal principal de $\mathbb{Z}[G]1_{\bar\chi}$.

4°) <u>Théorème</u> .

Soit $K/\mathbb{Q}$ une extension abélienne de groupe G . Soit $\mathfrak{M}$ l'ordre maximal de $\mathbb{Z}$ dans $\mathbb{Q}[G]$. Alors le plus grand $\mathfrak{M}$-module $\tilde{O}_K$ inclus dans l'anneau O_K des entiers de K est isomorphe à $\mathfrak{M}$.

<u>Démonstration</u> :

C'est une conséquence immédiate des lemmes 1 , 3 , 4 .

(1) On a vu que $\tilde{O}_K = \left[\bigoplus_{\chi} \mathbb{Z}[G]1_{\bar\psi} \cap \mathbb{Z}[G]1_{\bar\chi}\right].T_K$ (corollaire 1)

(2) Pour un caractère χ de G fixé , d'ordre n on a vu que

$$\mathbb{Z}[G]1_{\bar\psi} \cap \mathbb{Z}[G]1_{\bar\chi} \cong \mathbb{Z}[G_o]1_{\bar\psi_o} \cap \mathbb{Z}[G_o]1_{\bar\chi_o} \qquad \text{(lemme 1)}$$

où $G_o = \mathrm{Gal}(K_\chi/\mathbb{Q})$ avec K_χ corps fixe de Ker χ (G_o cyclique d'ordre n)
χ_o caractère de G_o correspondant à χ (χ_o fidèle)
ϕ_o caractère de ramification de l'extension $K_\chi/\mathbb{Q}$ correspondant à χ_o
H sous-groupe de G_o tel que $\phi_o = \mathrm{Ind}_H^{G_o}\, \bar\psi_o$ avec $\psi_o = \mathrm{Res}_H\, \chi_o$.

(3) Si $n = n_o n'$ avec $n_o = \prod_{p/n} p$ et si card $H = m_o m'$ $\left(\text{avec } m_o = \prod_{p/\text{card } H} p\right)$ on a vu (lemmes 3 et 4) que $\mathbb{Z}[G_o]\,1_{\overline{\psi}_o} \cap \mathbb{Z}[G_o]\,1_{\overline{\chi}_o}$ est l'idéal de $\mathbb{Z}[G_o]\,1_{\overline{\chi}_o}$ engendré par $\mathbb{Z}[S]\,1_{\overline{\eta}} \cap \mathbb{Z}[S]$ où S est le sous-groupe de G_o d'ordre $r_o = \dfrac{n_o}{m_o}$ et $\eta = \mathrm{Res}_S\, \chi_o$.

(4) Enfin d'après le théorème de Jacobinski (corollaire 2) , on a $\mathbb{Z}[S]\,1_{\overline{\eta}} \cap \mathbb{Z}[S] = \text{card } S \,.\, \mathfrak{D}^{-1}_{\overline{\eta}} = \left(\prod_{p/r_o} (1-\zeta_p)\right)$ $\left(\text{avec } \zeta_p\right.$ racine primitive p^{eme} de 1 dans $\mathbb{Q}[G_o]\,1_{\overline{\chi}_o}$ et $\mathfrak{D}^{-1}_{\overline{\eta}}$ codifférente de l'extension cyclotomique $\mathbb{Q}[S]\,1_{\overline{\eta}}/\mathbb{Q}$ - isomorphe à $\left.\mathbb{Q}^{(r_o)}/\mathbb{Q}\right)$.

On peut remarquer que dans r_o n'interviennent que les nombres premiers p modérément ramifiés dans l'extension $K_\chi/\mathbb{Q}$.

Références .

[J] H. JACOBINSKI :

On extensions of lattices .
Michigan Math. J. 13 (1966) 471-475 .

[L] H.N. LEOPOLDT :

Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers .
J. reine angew. Math. 201 (1959) 119-149 .

[T_1] M.J. TAYLOR :

Galois module structure of rings of integers in Kummer extensions .
Bull. of the London Math. Soc. 12 (1980) 96-98 .

[T_2] M.J. TAYLOR :

Monomial representations and rings of integers .
(à paraître dans Journal für die reine und angewandte Mathematik)

Danièle CHATELAIN
Faculté des Sciences, Mathématiques
ERA CNRS 070 654
25030 BESANCON CEDEX