

THEORIE DES NOMBRES  
BESANÇON

Années 1979-1980  
et 1980-1981

MODULES D'ENTRIERS 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 Leopoldt 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  $\chi$ ; on a :

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

où  $n$  est l'ordre de  $\chi$ .

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

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

$1_\varphi$  est un idempotent de  $\mathbb{C}[C]$ . En particulier pour  $\chi \in \hat{C}$ ,  $1_\chi$  et  $1_{\bar{\chi}}$  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 abélienne  $K/\mathbb{Q}$ , de groupe  $G$ .

Soit  $\chi \in \hat{G}$ ,  $f_\chi$  le conducteur du corps fixe de  $\text{Ker } \chi$ . Les caractères de ramification  $\phi$  de  $K/\mathbb{Q}$  sont les sommes des  $\chi \in \hat{G}$  appartenant 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  $f_\chi$  ou  $f_{\chi'}$ , les  $p$ -composantes  $f_\chi^{(p)}$  et  $f_{\chi'}^{(p)}$  de  $f_\chi$  et  $f_{\chi'}$  sont égales.

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

Rappelons la définition de  $H_\phi$  :

soit  $G^i(p)$  le  $i^{\text{eme}}$  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  $\phi$ . 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  $\phi$  correspond à la classe d'un

caractère  $\chi$  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 caractères 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  $\phi$  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 :

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

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

b) Théorème de Léopoldt.

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  $\phi$  de  $K$  ).

Remarques :

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  $\mathbb{Q}[G]$  ( $\mathfrak{M} = \bigoplus_{\chi} \mathbb{Z}[G] 1_{\bar{\chi}}$ ).

c) Corollaire 1.

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

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

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

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

Démonstration :

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

$$\tilde{O} = \bigoplus_{\bar{\chi}} \tilde{O} 1_{\bar{\chi}}$$

$$O \cap Z[G] 1_{\bar{\chi}} = \left( \bigoplus_{\bar{\psi}} Z[G] 1_{\bar{\psi}} \right) \cap Z[G] 1_{\bar{\chi}} = Z[G] 1_{\bar{\psi}} \cap Z[G] 1_{\bar{\chi}} .$$

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

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

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

Montrer que  $\tilde{O}_K$  est isomorphe à  $\mathfrak{M}$ , est donc équivalent à montrer que pour chaque  $\mathbb{Q}$ -caractère irréductible  $\bar{\chi}$  de  $G$ , l'idéal

$\tilde{O} \cdot 1_{\bar{\chi}} = Z[G] 1_{\bar{\psi}} \cap Z[G] 1_{\bar{\chi}}$  est un idéal principal de l'anneau  $Z[G] 1_{\bar{\chi}}$

(anneau isomorphe à l'anneau  $Z^{(n)}$  des entiers de  $\mathbb{Q}^{(n)}$ , pour  $n$  ordre de  $\chi$ ).

On voit que ce résultat est trivial si  $O = \mathfrak{M}$  (car  $Z[G] 1_{\bar{\psi}} = Z[G] 1_{\bar{\chi}}$ )

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 ( $O = Z[G]$ ) 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°) Théorème de Jacobinski ([J]).

Soient  $\mathcal{G}$  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  $k[\mathcal{G}]$  contenant  $\Lambda = O[\mathcal{G}]$ , soit  $A = k[\mathcal{G}]$ . On note :

$$[\mathfrak{M} : \Lambda]_{\mathfrak{g}} = \{ x \in A ; x\mathfrak{M} \subset \Lambda \}$$

$$[\mathfrak{M} : \Lambda]_{\mathfrak{d}} = \{ x \in A ; \mathfrak{M}x \subset \Lambda \}$$

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

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  $A$  .

Théorème de Jacobinski : On a  $[\mathfrak{M} : \Lambda]_{\mathfrak{g}} = [\mathfrak{M} : \Lambda]_{\mathfrak{d}} = \sum_i \frac{n}{n_i} \mathfrak{D}_i^{-1}$

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

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

Remarque : Si  $\mathcal{G}$  est abélien ,  $A_i/k$  est une extension abélienne et

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

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

Corollaire 2 .

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

En effet on a d'après le théorème de Jacobinski

$$\tilde{O} = [\mathfrak{M} : Z[G]] = \frac{\oplus}{\chi} |G| \mathfrak{D}_{\frac{-1}{\chi}}$$

où  $\mathfrak{D}_{\frac{-1}{\chi}}$  est la différentielle de l'extension cyclotomique  $\mathbb{Q}[G]_{\frac{1}{\chi}}/\mathbb{Q}$  , iso-

morphe à  $\mathbb{Q}^{(n)}/\mathbb{Q}$  ( si  $n$  est l'ordre de  $\chi$  ) . On sait bien que  $\mathfrak{D}_{\frac{-1}{\chi}}$  est

un idéal principal :

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

( où  $\zeta_p$  est une racine primitive  $p^{\text{eme}}$  de 1 ) .

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

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

$$\psi = \text{Res}_H \chi \quad \text{et} \quad \tilde{O} \cdot 1_{\bar{\chi}} = \mathbb{Z}[G] 1_{\bar{\psi}} \cap \mathbb{Z}[G] 1_{\bar{\chi}}$$

1°) Réduction au cas où  $\chi$  est un caractère fidèle de G .

Soit  $K_{\chi}$  le corps fixe de  $\text{Ker } \chi$  ,  $G_0$  le groupe de Galois de  $K_{\chi}/\mathbb{Q}$ , s la surjection canonique ( restriction ) de G sur  $G_0$  et  $\chi_0$  le caractère de  $G_0$  déduit de  $\chi$  (  $\chi_0 \circ s = \chi$  ) . Alors  $\chi_0$  est fidèle . On note :

$$e_0 = \frac{\sum_{h \in \text{Ker } \chi} h}{|\text{Ker } \chi|}$$

On sait alors que s définit un isomorphisme de  $\mathbb{Q}[G] \cdot e_0$  sur  $\mathbb{Q}[G_0]$  .

Cet isomorphisme envoie  $\mathfrak{M} \cdot e_0$  sur l'ordre maximal  $\mathfrak{M}_0$  de  $\mathbb{Q}[G_0]$  .

On a  $1_{\bar{\chi}} = 1_{\bar{\chi}} \cdot e_0 \in \mathfrak{M} \cdot e_0$  . L'image par s de  $\mathbb{Z}[G] 1_{\bar{\chi}}$  est  $\mathbb{Z}[G_0] 1_{\bar{\chi}_0}$

( avec  $\mathbb{Z}[G] 1_{\bar{\chi}} \cong \mathbb{Z}[G_0] 1_{\bar{\chi}_0} \cong \mathbb{Z}^{(n)}$  si n est l'ordre de  $\chi$  ) .

Notons  $O_{K_{\chi}}$  l'anneau des entiers de  $K_{\chi}$  et  $O_0$  l'ordre de  $\mathbb{Q}[G_0]$  asso -

cié à  $O_{K_{\chi}}$  . Soit  $\tilde{O}_{K_{\chi}}$  et  $\tilde{O}_0$  les plus grands  $\mathfrak{M}_0$ -modules inclus res -

pectivement dans  $O_{K_{\chi}}$  et  $O_0$  .

Lemme 1 .

1)  $\tilde{O}_K \cdot e_0 = \tilde{O}_{K_{\chi}}$

2) Les structures de  $\tilde{O} \cdot 1_{\bar{\chi}}$  comme  $\mathbb{Z}[G] 1_{\bar{\chi}}$ -module et de  $\tilde{O}_0 \cdot 1_{\bar{\chi}_0}$

comme  $\mathbb{Z}[G_0] 1_{\bar{\chi}_0}$ -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  $\tilde{O}_K$  :  $\tilde{O}_K e_o \oplus \tilde{O}_K(1 - e_o)$  .

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

$\tilde{O}_{K_\chi}$  est aussi un  $\mathfrak{M} \cdot e_o$  module inclus dans  $O_{K_\chi}$  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  $K \cdot e_o = \text{Tr}_{K/K_\chi} K = K_\chi$

donc dans  $O_{K_\chi} = O_K \cap K_\chi$  ; c'est un  $\mathfrak{M} \cdot e_o$  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 :  $\tilde{O}_K \cdot e_o = \tilde{O}_{K_\chi}$  .

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

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

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

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

D'où :

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

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  $\mathbb{Z}[G]$   $1_{\bar{\chi}}$  on suppose que  $\chi$  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  $m = m_0 m'$  avec  $m_0 = \prod_{p/m} p$   
( p premier ) . Soit  $\chi \in \hat{C}$  un caractère fidèle et  $C_0$  l'unique sous -  
groupe de C d'ordre  $m_0$  . Soit  $\chi_0$  la restriction de  $\chi$  à  $C_0$  . Alors

$$\text{Ind}_{C_0}^C \bar{\chi}_0 = \bar{\chi} \quad \text{et} \quad 1_{\bar{\chi}} = 1_{\bar{\chi}_0} \in \mathbb{Q}[C_0]$$

avec  $\chi_0$  d'ordre  $m_0$  sans facteurs carrés .

Démonstration :

On peut calculer directement les valeurs de  $\bar{\chi}$  et de  $\text{Ind}_{C_0}^C \bar{\chi}_0$

et constater l'égalité .

On peut aussi remarquer que d'après la formule de réciprocity de Fröbenius  
 $( \langle \chi', \text{Ind}_{C_0}^C \bar{\chi}_0 \rangle = \langle \text{Res}_{C_0} \chi', \bar{\chi}_0 \rangle )$  , le caractère

$\text{Ind}_{C_0}^C \bar{\chi}_0$  est la somme de tous les  $\chi' \in \hat{C}$  , prolongeant les conjugués

de  $\chi_0$  dans  $\hat{C}_0$  (  $\bar{\chi}_0$  est la somme des  $\mathbb{Q}$  conjugués de  $\chi_0$  )  $\chi$  étant  
fidèle , est d'ordre card C = m ;  $\chi_0$  est aussi fidèle et d'ordre

Card  $C_0 = m_0$  .  $\chi_0$  admet  $\varphi(m_0)$  conjugués qui sont les  $\chi_0^i$  ( $(i, m_0) = 1$ ).

Chaque  $\chi_0^i$  admet  $m'$  prolongements à C qui sont les  $\chi^i \cdot \chi^{m_0^j}$  ( pour  
 $1 \leq j \leq m'$  ) ;  $m_0$  a été choisi de telle sorte que  $m = m' m_0$  et  $m_0$  ad -

mette mêmes diviseurs premiers que m . Les caractères  $\chi^i \chi^{m_0^j}$  sont

donc d'ordre m et l'on a  $m' \varphi(m_0) = \varphi(m)$  . Le caractère  $\text{Ind}_{C_0}^C \bar{\chi}_0$

est donc la somme des  $\varphi(m)$  conjugués de  $\chi$  et est égal à  $\bar{\chi}$  ( d'où  $1_{\bar{\chi}} = 1_{\bar{\chi}_0}$  ).

Remarque :  $C_0$  est le plus petit sous-groupe de  $C$  tel que  $\text{Ind}_{C_0}^C (\overline{\text{Res}_{C_0} \chi})$  reste  $\mathbb{Q}$ -irréductible .

Lemme 3 .

Soit  $G$  un groupe cyclique d'ordre  $n = n_0 n'$  (avec  $n_0 = \prod_{p/n} p$ )  
 $H$  un sous-groupe de  $G$  d'ordre  $m = m_0 m'$  (avec  $m_0 = \prod_{p/m} p$ ) . Soit  $\chi$   
 un caractère fidèle de  $G$  et  $\psi = \text{Res}_H \chi$  . Soit  $H_0$  le sous-groupe de  $G$   
 d'ordre  $m_0$  et  $S$  le sous-groupe de  $G$  d'ordre  $r_0 = \frac{n_0}{m_0}$  ; soit  $\chi_0$  la res-  
 triction de  $\chi$  à  $G_0 = H_0 \cdot S$  ( produit direct ) et  $\psi_0$  la restriction de  $\chi_0$   
 à  $H_0$  . Alors ,  $Z[G] 1_{\bar{\chi}} \cap Z[G] 1_{\bar{\psi}}$  est l'idéal de  $Z[G] 1_{\bar{\chi}}$  engendré  
 par  $Z[G_0] 1_{\bar{\chi}_0} \cap Z[G_0] 1_{\bar{\psi}_0}$  .

Démonstration :

$G$  est cyclique et  $\chi$  fidèle d'ordre  $n = n_0 n'$  . Le groupe  $H$  est donc cyclique et  $\psi$  est fidèle d'ordre  $m = m_0 m'$  . On a donc d'après le

lemme 2  $1_{\bar{\psi}_0} = 1_{\bar{\psi}}$  et  $1_{\bar{\chi}_0} = 1_{\bar{\chi}}$  .

Par ailleurs on peut écrire :

$$\mathbb{Q}[G] = \mathbb{Q}[G_0] \otimes_{Z[G_0]} Z[G] ,$$

en définissant le produit tensoriel de  $x \in \mathbb{Q}[G_0]$  par  $y \in Z[G]$  comme le produit  $x.y$  dans  $\mathbb{Q}[G]$  .

Comme  $Z[G]$  est un  $Z[G_0]$ -module libre ( de base un système de représentants de  $G/G_0$  ) , on en déduit que pour tout sous- $Z[G_0]$ -module  $V$  de  $\mathbb{Q}[G_0]$  , on peut identifier  $V \otimes_{Z[G_0]} Z[G]$  au sous-module  $V \cdot Z[G]$  de  $\mathbb{Q}[G]$  et on sait que l'on a pour des sous-modules

$V_1$  et  $V_2$  de  $\mathbb{Q}[G_0]$  :

$$(V_1 \otimes_{\mathbb{Z}[G_0]} \mathbb{Z}[G]) \cap (V_2 \otimes_{\mathbb{Z}[G_0]} \mathbb{Z}[G]) = (V_1 \cap V_2) \otimes_{\mathbb{Z}[G_0]} \mathbb{Z}[G]$$

D'où en considérant  $V_1 = \mathbb{Z}[G_0] \cdot 1_{\bar{\chi}}$  et  $V_2 = \mathbb{Z}[G_0] \cdot 1_{\bar{\psi}}$

$$\begin{aligned} & [(\mathbb{Z}[G_0] \cdot 1_{\bar{\chi}}) \otimes_{\mathbb{Z}[G_0]} \mathbb{Z}[G]] \cap [(\mathbb{Z}[G_0] \cdot 1_{\bar{\psi}}) \otimes_{\mathbb{Z}[G_0]} \mathbb{Z}[G]] = \\ & = [\mathbb{Z}[G_0] \cdot 1_{\bar{\chi}} \cap \mathbb{Z}[G_0] \cdot 1_{\bar{\psi}}] \otimes_{\mathbb{Z}[G_0]} \mathbb{Z}[G] \end{aligned}$$

c'est-à-dire :

$$\mathbb{Z}[G] \cdot 1_{\bar{\chi}} \cap \mathbb{Z}[G] \cdot 1_{\bar{\psi}} = [\mathbb{Z}[G_0] \cdot 1_{\bar{\chi}} \cap \mathbb{Z}[G_0] \cdot 1_{\bar{\psi}}] \cdot \mathbb{Z}[G] .$$

### 3°) Réduction au théorème de Jacobinski .

#### Lemme 4 .

Soit  $G$  un groupe cyclique d'ordre  $n$  sans facteurs carrés,  $\chi$  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  $\psi$  et  $\eta$  les restrictions de  $\chi$  à  $H$  et  $S$ . Alors :

$$\mathbb{Z}[G] \cdot 1_{\bar{\chi}} \cap \mathbb{Z}[G] \cdot 1_{\bar{\psi}} = [\mathbb{Z}[S] \cap \mathbb{Z}[S] \cdot 1_{\bar{\eta}}] \cdot \mathbb{Z}[H] \cdot 1_{\bar{\psi}}$$

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

#### Démonstration :

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

On peut alors écrire :

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

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

$$\begin{aligned}
 Z[S]_{\bar{\eta}} \otimes_Z Z[H]_{\bar{\psi}} &= (Z[S]_{\bar{\eta}}) \cdot (Z[H]_{\bar{\psi}}) = Z[G]_{\bar{\chi}} \\
 Z[S] \otimes_Z Z[H]_{\bar{\psi}} &= Z[S] \cdot Z[H]_{\bar{\psi}} = Z[G]_{\bar{\psi}} \\
 (Z[S]_{\bar{\eta}} \otimes_Z Z[H]_{\bar{\psi}}) \cap (Z[S] \otimes_Z Z[H]_{\bar{\psi}}) &= \\
 &= (Z[S]_{\bar{\eta}} \cap Z[S]) \otimes_Z Z[H]_{\bar{\psi}}
 \end{aligned}$$

d'où :

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

D'après le théorème de Jacobinski ( corollaire 2 ) on sait que

$Z[S]_{\bar{\eta}} \cap Z[S]$  est un idéal principal de l'anneau  $Z[S]_{\bar{\eta}}$  . On en déduit que  $Z[G]_{\bar{\chi}} \cap Z[G]_{\bar{\psi}}$  est un idéal principal de  $Z[G]_{\bar{\chi}}$  .

#### 4°) Théorème .

Soit  $K/\mathbb{Q}$  une extension abélienne de groupe  $G$  .

Soit  $\mathfrak{M}$  l'ordre maximal de  $Z$  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  $\mathfrak{M}$  .

#### Démonstration :

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

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

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

$$Z[G]_{\bar{\psi}} \cap Z[G]_{\bar{\chi}} \cong Z[G_0]_{\bar{\psi}_0} \cap Z[G_0]_{\bar{\chi}_0} \quad (\text{ lemme 1 } )$$

où  $G_0 = \text{Gal}(K_{\chi}/\mathbb{Q})$  avec  $K_{\chi}$  corps fixe de  $\text{Ker } \chi$  ( $G_0$  cyclique d'ordre  $n$ )

$\chi_0$  caractère de  $G_0$  correspondant à  $\chi$  ( $\chi_0$  fidèle)

$\phi_0$  caractère de ramification de l'extension  $K_{\chi}/\mathbb{Q}$  correspondant à  $\chi_0$

$H$  sous-groupe de  $G_0$  tel que  $\phi_0 = \text{Ind}_H^{G_0} \bar{\psi}_0$  avec  $\bar{\psi}_0 = \text{Res}_H \chi_0$  .

(3) Si  $n = n_0 n'$  avec  $n_0 = \prod_{p/n} p$  et si  $\text{card } H = m_0 m'$

(avec  $m_0 = \prod_{p/\text{card } H} p$ ) on a vu (lemmes 3 et 4) que

$Z[G_0]_{\bar{\psi}_0} \cap Z[G_0]_{\bar{\chi}_0}$  est l'idéal de  $Z[G_0]_{\bar{\chi}_0}$  engendré par

$Z[S]_{\bar{\eta}} \cap Z[S]$  où  $S$  est le sous-groupe de  $G_0$  d'ordre  $r_0 = \frac{n_0}{m_0}$

et  $\eta = \text{Res}_S \chi_0$ .

(4) Enfin d'après le théorème de Jacobinski (corollaire 2), on a

$Z[S]_{\bar{\eta}} \cap Z[S] = \text{card } S \cdot \mathfrak{D}_{\bar{\eta}}^{-1} = \left( \prod_{p/r_0} (1 - \zeta_p) \right)$  (avec  $\zeta_p$  racine primitive  $p^{\text{eme}}$  de 1 dans  $\mathbb{Q}[G_0]_{\bar{\chi}_0}$  et  $\mathfrak{D}_{\bar{\eta}}^{-1}$  codifférente de l'extension cyclotomique  $\mathbb{Q}[S]_{\bar{\eta}}/\mathbb{Q}$  - isomorphe à  $\mathbb{Q}^{(r_0)}/\mathbb{Q}$ ).

On peut remarquer que dans  $r_0$  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<sub>1</sub>] M.J. TAYLOR :

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

[T<sub>2</sub>] M.J. TAYLOR :

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