

THEORIE DES NOMBRES

- Besançon -

Année 1976-77

UNE PROPRIETE DE L'ANNEAU DES ENTIERS DES EXTENSIONS  
GALOISIENNES NON ABELIENNES DE DEGRE  $pq$   
DES RATIONNELS

Jean COUGNARD  
Faculté des Sciences. Mathématiques  
E.R.A. CNRS N° 070654  
25030 Besançon Cedex

Une propriété de l'anneau des entiers des extensions galoisiennes non abéliennes  
de degré  $pq$  des rationnels.

ERRATA:

page 7: changer les  $G$  en  $\mathcal{G}$  .

Au bas de la page supprimer la phrase commençant à : " Etant donné que  $H:..$   
et finissant à  $\mathbb{Z}[G]$  modules."

page 8: dans le théorème 1 lire  $O'$ -modules au lieu de  $O$ -modules.

page 9: dans la démonstration du théorème 2 la référence est; [7] page 38 et  
non [6] page 38.

page 15: dans l'énoncé de la proposition 5 remplacer:

$\xi$  est une unité de  $O_{N, \mathcal{F}}$  par  $\xi$  appartient à  $O_{N, \mathcal{F}}$  .

page 23: deux lignes avant la fin de la page

remplacer  $\sum_{i=1}^{q-1}$  par  $\prod_{i=1}^{q-1}$  .

page 24: dans la dernière ligne remplacer  $q-1$  par  $t-1$  .

page 25: dans l'énoncé de la proposition 11 au 3<sup>e</sup> remplacer  $\theta_{i=1}^t$  par  $\theta_{i=1}^{t-1}$  .

Un certain nombre de fois des  $O'$  ont été remplacés par des  $O$ , le lecteur  
rectifiera de lui même!

Une propriété de l'anneau des entiers des extensions  
galoisiennes non abéliennes de degré  $pq$   
des rationnels.

par Jean COUGNARD .

Introduction.

Soit  $N/\mathbb{Q}$  une extension galoisienne de groupe de Galois  $G$ ,  $\mathcal{O}_N$  la clôture intégrale de  $\mathbb{Z}$  dans  $N$  et  $\mathcal{O}$  un ordre maximal de  $\mathbb{Q}[G]$  contenant  $\mathbb{Z}[G]$ . Construisons le  $\mathcal{O}$ -module  $\mathcal{O}\mathcal{O}_N$ ; dans le cas où  $N/\mathbb{Q}$  est modérément ramifiée, A. Fröhlich a démontré que  $\mathcal{O}\mathcal{O}_N$  est  $\mathcal{O}$ -stablement libre [5], ce qui revient à dire que la classe de  $\mathcal{O}\mathcal{O}_N$  dans le groupe des classes projectives de  $\mathcal{O}$  est l'élément neutre. Ce résultat est encore valable, sans hypothèse de ramification, si on suppose que  $G$  est un  $p$ -groupe [3]. Le théorème de Fröhlich ne peut toutefois se généraliser sous cette forme puisque l'on peut construire des extensions non abéliennes de degré  $pq$  du corps des rationnels telles que  $\mathcal{O}\mathcal{O}_N$  ne soit pas stablement libre ([4]).

On peut néanmoins remarquer que dans le cas modérément ramifié  $\mathcal{O}\mathcal{O}_N$  est  $\mathcal{O}$ -isomorphe à  $\mathcal{O} \otimes_{\mathbb{Z}[G]} \mathcal{O}_N$ . On peut donc se proposer d'étudier le  $\mathcal{O}$ -module  $\mathcal{O} \otimes_{\mathbb{Z}[G]} \mathcal{O}_N$  dans les extensions sauvagement ramifiées. Ce  $\mathcal{O}$ -module n'a plus de raison d'être localement libre, il suffit pour s'en convaincre de considérer une extension quadratique de  $\mathbb{Q}$  (cf. une lettre de J. Martinet à J.-P. Serre). Il faut donc étudier son image dans le groupe de Grothendieck  $G_0(\mathcal{O})$  des  $\mathcal{O}$ -modules de type fini; c'est ce que nous nous proposons de faire dans le cas des extensions non abéliennes de degré  $pq$  qui ont servi au contre-exemple de [4].

Nous démontrons que  $\mathcal{O} \otimes_{\mathbb{Z}[G]} \mathcal{O}_N$  est isomorphe à une somme directe  $\mathcal{O}\mathcal{O}_N \oplus T$  où  $T$  est un  $\mathcal{O}$ -module fini. Dans le cas où  $G$  est un groupe non abélien d'ordre  $pq$ , on montre que la classe de  $T$  dans  $G_0(\mathcal{O})$  est l'opposée de celle de  $\mathcal{O}\mathcal{O}_N$  ce qui montre que l'image de  $\mathcal{O} \otimes_{\mathbb{Z}[G]} \mathcal{O}_N$  dans  $G_0(\mathcal{O})$  est l'élément neutre.

Nous montrons que cette propriété est encore vérifiée lorsque  $G$  est un  $p$ -groupe. Le résultat est encore valable lorsque  $G$  est abélien ([1]), ceci est une conséquence des travaux de Leopoldt.

§ 1. Produits tensoriels - Localisation .

L'algèbre  $\mathbb{Q}[G]$  est semi-simple  $\mathbb{Q}[G] \simeq \prod_{i=1}^r A_i$  où les  $A_i$

sont des algèbres simples :  $A_i = e_i \mathbb{Q}[G]$  ,  $e_i$  désignant des idempotents du centre orthogonaux deux à deux . Un ordre maximal  $O$  de  $\mathbb{Q}[G]$  peut s'écrire

$O \simeq \prod_{i=1}^r O_i$  où  $O_i = e_i O$  est un ordre maximal de  $A_i$  ; de l'inclusion

$O \supset \mathbb{Z}[G]$  on déduit  $e_i O \supset e_i \mathbb{Z}[G]$  donc pour tout  $x$  appartenant à  $O$  et tout  $\lambda$  appartenant à  $\mathbb{Z}[G]$  on a

$$(e_i x) \lambda = (e_i x) (e_i \lambda)$$

ce qui munit  $O_i$  d'une structure de  $\mathbb{Z}[G]$ -module ; le produit direct

$O \simeq \prod_{i=1}^r O_i$  est un produit direct de  $\mathbb{Z}[G]$ -modules . On peut donc écrire

$$O \otimes_{\mathbb{Z}[G]} O_N \simeq \left( \prod_{i=1}^r O_i \right) \otimes_{\mathbb{Z}[G]} O_N \simeq \prod_{i=1}^r O_i \otimes_{\mathbb{Z}[G]} O_N$$

comme  $G_0(O) \simeq \prod_{i=1}^r G_0(O_i)$  on est ramené à l'étude de ce qui se passe dans

chaque facteur simple .

Proposition 1 . Le  $O_i$ -module  $O_i \otimes_{\mathbb{Z}[G]} O_N$  est isomorphe à  $O_i O_N \oplus T_i$  où  $T_i$  est un groupe fini .

démonstration :

considérons l'application biadditive  $f$  de  $O_i \times O_N$  dans  $O_i O_N$  définie par  $f(u, x) = ux$  . Elle vérifie  $f(ug, x) = f(u, gx)$  quel que soit  $g$  appartenant à  $G$  ; l'application  $f$  se factorise par  $O_i \otimes_{\mathbb{Z}[G]} O_N$  en une

application  $\tilde{f}$  telle que  $\tilde{f}(u \otimes x) = f(u, x) = ux$ . Les  $u \otimes x$  (resp.  $ux$ ) étant des générateurs de  $O_i \otimes_{Z[G]} O_N$  (resp.  $O_i O_N$ ) l'application  $\tilde{f}$  est surjective. Le  $O_i$ -module  $O_i O_N$  est projectif puisque sans torsion, il existe donc un  $O_i$ -module  $M_i$  tel que

$$O_i \otimes_{Z[G]} O_N \simeq O_i O_N \oplus M_i$$

comparons les dimensions de  $\mathbb{Q} \otimes_Z (O_i \otimes_{Z[G]} O_N)$  et  $\mathbb{Q} \otimes_Z (O_i O_N \oplus M_i)$  :

$$\mathbb{Q} \otimes_Z (O_i \otimes_{Z[G]} O_N) \simeq A_i \otimes_{\mathbb{Q}[G]} N \simeq A_i \simeq A_i N \simeq \mathbb{Q} \otimes_Z O_i O_N$$

d'où l'on déduit que  $\mathbb{Q} \otimes_Z M_i = 0$  ce qui montre que  $M_i$  est un groupe de torsion ; comme il est de type fini la proposition est démontrée.

On peut trouver un  $O_i$ -module libre  $E$  et un sous-module  $E'$  de  $E$  tels que l'on ait une suite exacte

$$0 \rightarrow E' \rightarrow E \rightarrow O_i \otimes_{Z[G]} O_N \rightarrow 0$$

Or, on peut déduire du théorème I-2 de [8] que la classe de  $E$  dans

$\mathbb{G}_0(O_i)$  est l'élément neutre. On a donc :

$\text{cl}(O_i \otimes_{Z[G]} O_N) = -\text{cl}(E')$  or  $E' \simeq O_i^n \oplus I$  où  $I$  est un idéal à gauche de  $O_i$ , la classe de  $E'$  est égale à celle de  $I$ , laquelle est déterminée par sa norme réduite ; ceci justifie l'étude par des méthodes locales. Pour tout  $O_i$ -module  $M$  et toute place  $p$  de  $Z$  on a :

$$\begin{aligned} Z_p \otimes_Z (O_i \otimes_{Z[G]} O_N) &\simeq (Z_p \otimes_Z O_i) \otimes_{Z[G]} O_N \simeq (Z_p \otimes_Z Z[G] \otimes_{Z[G]} O_i) \otimes_{Z[G]} O_N \\ &\simeq (Z_p[G] \otimes_{Z[G]} O_i) \otimes_{Z[G]} O_N \simeq Z_p[G] \otimes_{Z[G]} (O_i \otimes_{Z[G]} O_N) \\ &\simeq (Z_p[G] \otimes_{Z[G]} O_i) \otimes_{Z_p[G]} (Z_p[G] \otimes_{Z[G]} O_N) \\ &\simeq (Z_p \otimes_Z O_i) \otimes_{Z_p[G]} (Z_p \otimes_Z O_N) \end{aligned}$$

Proposition 2.    Les facteurs premiers de l'ordre de  $T_i$  sont des places sauvagement ramifiées.

démonstration :

d'après la remarque précédente et la proposition 1 on a les iso-

morphismes :

$$\begin{aligned} \mathbb{Z}_p \otimes_{\mathbb{Z}} (O_i \otimes_{\mathbb{Z}[G]} O_N) &\simeq (\mathbb{Z}_p \otimes_{\mathbb{Z}} O_i \otimes_{\mathbb{Z}[G]} O_N) \oplus (\mathbb{Z}_p \otimes_{\mathbb{Z}} T_i) \\ &\simeq (\mathbb{Z}_p \otimes_{\mathbb{Z}} O_i) \otimes_{\mathbb{Z}_p[G]} (\mathbb{Z}_p \otimes_{\mathbb{Z}} O_N) \end{aligned}$$

or si  $p$  est modérément ramifié dans  $N/\mathbb{Q}$ ,  $\mathbb{Z}_p \otimes_{\mathbb{Z}} O_N$  est  $\mathbb{Z}_p[G]$ -libre de rang 1 donc  $\mathbb{Z}_p \otimes_{\mathbb{Z}} T_i = 0$  si  $p$  est modérément ramifié.

Corollaire 1.     Si  $G$  est un  $p$ -groupe, l'image de  $O \otimes_{\mathbb{Z}[G]} O_N$  dans  $G_0(O)$  est l'élément neutre.

démonstration :

On a  $cl(O_i \otimes_{\mathbb{Z}[G]} O_N) = cl(O_i \otimes_{\mathbb{Z}[G]} O_N) + cl(T_i)$ , or d'après [3]  $O_i \otimes_{\mathbb{Z}[G]} O_N$  est stablement libre donc  $cl(O_i \otimes_{\mathbb{Z}[G]} O_N) = cl(T_i)$ . On

peut trouver un entier  $r \geq 1$  et un idéal fractionnaire à gauche  $I$  de  $O_i$  tels que l'on ait une suite exacte

$$0 \rightarrow O_i^{r-1} \oplus I \rightarrow O_i^r \rightarrow T_i \rightarrow 0$$

d'où l'on déduit  $cl(O_i \otimes_{\mathbb{Z}[G]} O_N) = cl(I)$ . Comme  $T_i$  est un  $p$ -groupe, la norme réduite de  $I$  ne fait apparaître que la composante au-dessus de  $p$  dans le centre du facteur simple ;  $G$  étant un  $p$ -groupe, la norme réduite de  $I$  est un idéal principal (principal totalement positif le cas échéant) ce qui démontre le résultat.

Intéressons nous maintenant aux groupes non abéliens d'ordre  $pq$ . L'algèbre  $\mathbb{Q}[G]$  comporte trois facteurs ([4]) et on doit étudier  $O_1 \otimes_{\mathbb{Z}[G]} O_N$ ,  $O_2 \otimes_{\mathbb{Z}[G]} O_N$ ,  $O_3 \otimes_{\mathbb{Z}[G]} O_N$ , avec  $O_1 \simeq \mathbb{Z}$ ,  $O_2 \simeq \mathbb{Z}[\omega]$  ( $\omega$  racine primitive  $q$ -ième de l'unité) et  $O_3$  un ordre maximal de  $M_q(K)$  où  $K$  est le sous-corps du  $p$ -ième corps cyclotomiques de degré  $\frac{p-1}{q}$ .

Il est clair que  $O_1 \otimes_{\mathbb{Z}[G]} O_N$  ne pose pas de problème. Pour  $O_3 \otimes_{\mathbb{Z}[G]} O_N$ , appliquons la méthode précédente.

Corollaire 2.     Si  $O_3$  est un ordre maximal de  $M_q(K)$  contenant la projection de  $\mathbb{Z}[G]$ , la classe de  $O_3 \otimes_{\mathbb{Z}[G]} O_N$  dans  $G_0(O_3)$  est l'élément neutre.

démonstration :

Soit  $\Lambda$  la projection de  $Z[G]$  sur  $M_q(K)$ . On peut montrer que  $\Lambda$  contient la clôture intégrale de  $Z$  dans  $K$  et que le conducteur de  $O_3$  dans  $\Lambda$  est une puissance de l'idéal premier principal de  $K$  au-dessus de  $p$  ([2]). On a donc pour toute place  $\ell$  première à  $p$  :

$$Z_\ell \otimes_Z O_3 \simeq \Lambda_\ell$$

ce qui donne :

$$\begin{aligned} Z_\ell \otimes_Z (O_3 \circlearrowleft O_N \oplus T_3) &\simeq Z_\ell \otimes_Z (O_3 \otimes_{Z[G]} O_N) \simeq (Z_\ell \otimes_Z O_3) \otimes_{Z_\ell[G]} (Z_\ell \otimes_Z O_N) \\ &\simeq Z_\ell \otimes_Z (O_3 \circlearrowleft O_N) \end{aligned}$$

ce qui montre que l'ordre de  $T_3$  est une puissance de  $p$ . On peut conclure comme dans le corollaire 1. Car  $O_3 \circlearrowleft O_N$  est stablement libre (cela se déduit des calculs de [2]).

Dans le cas des groupes non abéliens d'ordre  $pq$ , il reste à étudier  $O_2 \otimes_{Z[G]} O_N$ . Le facteur simple  $O_2$  est associé aux caractères  $\chi$  de degré 1 de  $G$  non triviaux.

§ 2. Quelques remarques sur un caractère non fidèle.

On est dans la situation suivante : Soient  $k/\mathbb{Q}$  une extension galoisienne de groupe de Galois  $g$  et  $O'$  un ordre maximal d'un facteur simple de  $\mathbb{Q}[g]$ , contenant  $Z[g]$ . On considère  $N/\mathbb{Q}$  une extension galoisienne de groupe de Galois  $G$  telle que  $N$  contienne  $k$ . On s'intéresse au  $O'$ -module  $O' \otimes_{Z[G]} O_N$ . Notons  $H = \text{Gal}(N/k)$ .

On a un isomorphisme de  $O'$ -modules fourni par les propriétés élémentaires du produit tensoriel :

$$O' \otimes_{Z[G]} O_N \simeq O' \otimes_{Z[g]} (Z[g] \otimes_{Z[G]} O_N) .$$

On est donc conduit à étudier en premier lieu  $Z[g] \otimes_{Z[G]} O_N$ . Il y a une surjection de  $Z[g] \otimes_Z O_N \longrightarrow Z[g] \otimes_{Z[g]} O_N$  dont le noyau est le sous- $Z$ -module engendré par les éléments de la forme  $(\tau g \otimes x) - (\tau \otimes gx)$ . On peut toujours trouver  $g'$  tel que  $\tau = 1.g'$  d'où

$$\tau \otimes x = 1 \cdot g \otimes x - 1 \otimes gx + 1 \otimes gx$$

ce qui montre que tout élément de  $Z[g] \otimes_{Z[G]} O_N$  peut s'écrire sous la forme  $1 \otimes x$ . Avec les notations précédentes, on peut énoncer:

Proposition 3 . Il y a un isomorphisme de  $Z[g]$ -modules entre  $Z[g] \otimes_{Z[G]} O_N$  et  $O_N/I_H O_N$  où  $I_H$  est l'idéal de  $Z[H]$  engendré par les éléments  $(h-1)$

( $h \in H$ ) . L'isomorphisme est défini de la façon suivante : pour l'élément  $\tau \otimes x$ , il existe  $g$  tel que  $\tau = 1 \cdot g$  ; l'image de  $\tau \otimes x$  par l'isomorphisme est la classe de  $gx$  dans  $O_N/I_H O_N$  .

démonstration :

Considérons l'application  $p : Z[G] \times O_N \longrightarrow O_N/I_H O_N$  définie

de la façon suivante : pour  $\tau \in g$ , il existe  $g \in G$  tel que  $\tau = 1 \cdot g$  ; posons  $p(\tau, x) = \overline{gx}$ . Si on remplace  $g$  par  $g_1$ , on a  $gg_1^{-1} \in H$  d'où  $g = hg_1$  et  $gx - g_1x = (h-1)g_1x \in I_H O_N$  ce qui montre que l'application  $p$  est bien définie . Remarquons que par construction, quel que soit  $g' \in G$  on a  $p(\tau g', x) = p(\tau, g'x)$ . On en déduit l'existence d'un homomorphisme  $\bar{p}$  de  $Z[g]$ -modules de  $Z[g] \otimes_{Z[G]} O_N$  dans  $O_N/I_H O_N$ . L'application  $p$  étant surjective, il en est de même de  $\bar{p}$ . Montrons que cet homomorphisme est injectif :

$$\bar{p}(\tau \otimes x) = \bar{p}(1g \otimes x) = \bar{p}(1 \otimes gx) = p(1, gx) = \overline{gx} ;$$

si  $\overline{gx} = 0$  c'est que  $gx \in I_H O_N$  donc peut s'écrire  $gx = \sum_i (h_i - 1)x_i$  d'où

$$\tau \otimes x = \sum_i 1 \otimes (h_i - 1)x_i = \sum_i h_i \otimes x_i - 1 \otimes x_i = 0 .$$

On est donc amené à étudier le  $O$ -module  $O' \otimes_{Z[g]} O_N/I_H O_N$ .

Revenons au cas qui nous intéresse :  $H$  est cyclique d'ordre une puissance de  $p$ ,  $g$  est cyclique d'ordre  $q$  avec  $q \neq p$ . Le module  $O_N/I_H O_N$  intervient dans la suite exacte de  $Z[g]$ -module :



$$(1) \quad 0 \longrightarrow \frac{\text{Ker } T}{I_H \mathcal{O}_N} \longrightarrow \frac{\mathcal{O}_N}{I_H \mathcal{O}_N} \longrightarrow T_{N/k}(\mathcal{O}_N) \longrightarrow 0$$

où  $\text{Ker } T$  désigne le noyau de la trace dans l'extension  $N/k$  restreinte à  $\mathcal{O}_N$ . De (1) on déduit la suite exacte :

$$(2) \quad \text{Tor}_1^{\mathbb{Z}[G]}(\mathcal{O}', T_{N/k}(\mathcal{O}_N)) \longrightarrow \mathcal{O}' \otimes_{\mathbb{Z}[G]} \frac{\text{Ker } T}{I_H \mathcal{O}_N} \longrightarrow \dots$$

$$\dots \longrightarrow \mathcal{O}' \otimes_{\mathbb{Z}[G]} \frac{\mathcal{O}_N}{I_H \mathcal{O}_N} \longrightarrow \mathcal{O}' \otimes_{\mathbb{Z}[G]} T_{N/k}(\mathcal{O}_N) \longrightarrow 0.$$

La suite (2) reste exacte si on lui applique  $\mathbb{Z}_\ell \otimes_{\mathbb{Z}}$ , ce qui donne, compte-tenu du calcul qui précède la proposition 2 :

$$(3) \quad \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \text{Tor}_1^{\mathbb{Z}[G]}(\mathcal{O}', T_{N/k}(\mathcal{O}_N)) \longrightarrow (\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{O}') \otimes_{\mathbb{Z}_\ell[G]} \left( \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \frac{\text{Ker } T}{I_H \mathcal{O}_N} \right) \longrightarrow \dots$$

$$\dots \longrightarrow (\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{O}') \otimes_{\mathbb{Z}_\ell[G]} \left( \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \frac{\mathcal{O}_N}{I_H \mathcal{O}_N} \right) \longrightarrow \dots$$

$$\dots \longrightarrow (\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{O}') \otimes_{\mathbb{Z}_\ell[G]} (\mathbb{Z}_\ell \otimes_{\mathbb{Z}} T_{N/k}(\mathcal{O}_N)) \longrightarrow 0$$

Mais  $T_{N/k}(\mathcal{O}_N)$  est un idéal de  $\mathcal{O}_k$ , si  $\ell \neq q$   $\mathcal{O}_\ell \otimes_{\mathbb{Q}} k$  est une algèbre de Galois modérément ramifiée donc  $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} T_{N/k} \mathcal{O}_N$  est  $\mathbb{Z}_\ell[g]$ -projectif. Cela se déduit du théorème I de [9]. On en déduit que la suite exacte de  $\mathbb{Z}[g]$  modules :

$$(4) \quad 0 \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \frac{\text{Ker } T}{I_H \mathcal{O}_N} \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \frac{\mathcal{O}_N}{I_H \mathcal{O}_N} \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} T_{N/k}(\mathcal{O}_N) \longrightarrow 0$$

est scindée. Etant donné que  $H$  opère trivialement sur ces modules, la suite est une suite exacte scindée de  $\mathbb{Z}[G]$  modules.

Elle le reste quand on lui applique  $(\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{O}') \otimes_{\mathbb{Z}_\ell[G]}$ .

Pour  $\ell = q$ ,  $\frac{\text{Ker } T}{I_H \mathcal{O}_N}$  a pour ordre une puissance de  $p$ , par conséquent

on a  $\mathbb{Z}_q \otimes_{\mathbb{Z}} \frac{\text{Ker } T}{I_H \mathcal{O}_N} = 0$ . On en déduit que la  $\ell$ -composante de l'image de

$\text{Tor}_1^{\mathbb{Z}[G]}(O', T_{N/k}(O_N))$  dans  $O' \otimes_{\mathbb{Z}[g]} \frac{\text{Ker } T}{I_H O_N}$  est nulle quel que soit  $\ell$ ,

soit :

Théorème 1 .      La suite de O-modules :

$$0 \longrightarrow O' \otimes_{\mathbb{Z}[g]} \frac{\text{Ker } T}{I_H O_N} \longrightarrow O' \otimes_{\mathbb{Z}[g]} \frac{O_N}{I_H O_N} \longrightarrow O' \otimes_{\mathbb{Z}[g]} T_{N/k}(O_N) \longrightarrow 0$$

est exacte .

Par définition des groupes de Grothendieck , l' image de  $O' \otimes_{\mathbb{Z}[G]} O_N$  est égale à la somme de celles de  $O' \otimes_{\mathbb{Z}[g]} \frac{\text{Ker } T}{I_H O_N}$  et  $O' \otimes_{\mathbb{Z}[g]} T_{N/k}(O_N)$  . Nous allons faire les calculs lorsque l'ordre de  $H$  est égal à  $p$  . Auparavant rappelons des résultats de Shankar Sen ([7]) qui nous seront utiles .

§ 3. Rappels des résultats de S. Sen .

Rappelons quelques notations :  $K$  et  $F$  désignent des corps locaux tels que  $K$  soit une extension cyclique de  $F$  de degré  $p^n$  ,  $A$  désigne l'anneau de valuation de  $K$  ,  $B$  celui de  $F$  (on suppose  $K/F$  totalement ramifiée); soient  $\sigma$  un générateur de  $\text{Gal}(K/F)$  ,  $\pi$  (resp.  $\Pi$ ) une uniformisante de  $F$  (resp.  $K$ ) (pour faciliter les calculs on choisira ultérieurement ces uniformisantes) .

On note  $i(r) = v_K \left( \frac{(\sigma^r - 1) \Pi}{\Pi} \right)$  et  $i_s = i(p^s)$  .

Lemme 1. ([7] lemme 1) . Quel que soit  $\mu \in \mathbb{Z}$  , il existe  $x_\mu$  tel que  $v_K(x_\mu) = \mu$

et  $v((\sigma - 1)x_\mu) = \mu + i(\mu)$  (on choisit  $x_\mu = \prod_{i=0}^{\mu-1} \sigma^i(\Pi)$ ) .

Lemme 2 . ([7] lemme 2) . Tout élément  $x$  de  $K$  peut être écrit comme somme

d'une série  $x = \sum_{\mu = v_K(x)}^{\infty} x_{\mu}$  , les  $x_{\mu}$  vérifiant les conditions du

lemme 1 .

Lemme 3 . ([7] lemme 3) . Soit  $s$  tel que  $i_{s-1} < \infty$  , si quel que soit  $j$ ,  $0 < j < s$   
on a  $i_{j-1} \equiv i_j \pmod{p^j}$  alors les entiers  $\mu + i(\mu)$  avec  $v_{\mathbb{Q}}(\mu) < s$  sont tous  
distincts et distincts de  $i_{s-1}$  .

On déduit de ces lemmes :

Théorème 2 . ([7] Th. 1) . Pour  $1 \leq r \leq n$  la congruence  $i_{r-1} \equiv i_r \pmod{p^r}$  est  
vérifiée .

Ces résultats permettent de déterminer la structure du groupe

$\text{Ker } T_{K/F} / (1-\sigma)A$  de la façon suivante . Pour  $\mu$  tel que  $1 \leq \mu \leq p^n - 1$  chois-

sons des  $x_{\mu}$  dans  $K$  vérifiant les conditions du lemme 1 . Les  $x_{\mu}$  et 1 for-  
 ment une B-base de  $A$  ; posons  $y_{\mu} = (\sigma - 1)x_{\mu}$  , du théorème et du lemme 3  
 on déduit que les  $y_{\mu}$  ont des valuations distinctes et même que les entiers  
 $v_K(y_{\mu})$  sont distincts modulo  $p^n$  ([6] p. 38) donc les  $y_{\mu}$  forment une B-  
 base de  $(1-\sigma)A$  . Il en résulte que les  $y_{\mu}$  forment une F-base de  $(1-\sigma)K$  .  
 Soit  $z \in A$  tel que  $T_{K/F}(z) = 0$  ; cet élément appartient à  $(1-\sigma)K \cap A$  ,

il s'écrit donc  $z = \sum_{\mu=1}^{p^n-1} b_{\mu} y_{\mu}$  avec  $v_K(z) \geq 0$  ,  $v_K(b_{\mu}) \equiv 0 \pmod{p^n}$  ; les

$v_K(y_{\mu})$  étant deux à deux distincts modulo  $p^n$  on voit que

$v_K(z) = \inf_{\mu} v_K(b_{\mu} y_{\mu})$  par conséquent , quel que soit  $\mu$  on a

$p^n v_F(b_{\mu}) + \mu + i(\mu) \geq 0$  ce qui équivaut à  $v_F(b_{\mu}) \geq - \left[ \frac{\mu + i(\mu)}{p^n} \right]$  .

Une B-base de  $\text{Ker } T_{K/F}$  est donc formée des  $\frac{y_{\mu}}{\pi^{(\mu)}}$  où  $(\mu) = \left[ \frac{\mu + i(\mu)}{p^n} \right]$

est le plus grand entier inférieur ou égal à  $\frac{\mu+i(\mu)}{p^n}$ .

Revenons à la situation du § 2 :  $N$  est une extension non abélienne de degré  $pq$  ; son groupe de Galois  $G$  est engendré par deux éléments  $\sigma$  et  $\tau$  tels que  $\sigma^p = \tau^q = 1$  ;  $\tau\sigma\tau^{-1} = \sigma^r$  où  $r \not\equiv 1 (p)$ ,  $r^q \equiv 1 (p)$  ce qui implique  $p \equiv 1 (q)$ . On note  $H$  le sous-groupe distingué engendré par  $\sigma$ ,  $k$  le sous-corps de  $N$  formé des éléments invariants par  $H$  et  $g = G/H$ .

Nous voulons étudier  $O' \otimes_{\mathbb{Z}[g]} \frac{\text{Ker } T}{I_H O_N} = O' \otimes_{\mathbb{Z}[g]} \frac{\text{Ker } T}{(\sigma-1)O_N}$

où  $O'$  est isomorphe à  $\mathbb{Z}[\omega]$  ( $\omega$  racine primitive  $q$ -ième de l'unité).

§ 4. Etude de  $O' \otimes_{\mathbb{Z}[g]} \frac{\text{Ker } T}{(\sigma-1)O_N}$ .

On sait que  $\frac{\text{Ker } T}{(\sigma-1)O_N}$  est un  $p$ -groupe. On a donc

$$\frac{\text{Ker } T}{(\sigma-1)O_N} \simeq \mathbb{Z}_p \otimes_{\mathbb{Z}} \frac{\text{Ker } T}{(\sigma-1)O_N}; \text{ or on a la suite exacte de } \mathbb{Z}\text{-modules}$$

$$0 \longrightarrow (\sigma-1)O_N \longrightarrow \text{Ker } T \longrightarrow \frac{\text{Ker } T}{(\sigma-1)O_N} \longrightarrow 0$$

qui reste exacte quand on la tensorise par  $\mathbb{Z}_p$  ce qui donne :

$$(5) \quad 0 \longrightarrow (\sigma-1)\mathbb{Z}_p \otimes_{\mathbb{Z}} O_N \longrightarrow \frac{\text{Ker } T_{\mathbb{Z}_p \otimes_{\mathbb{Z}} O_N}}{\mathbb{Z}_p \otimes_{\mathbb{Z}} O_k} \longrightarrow \frac{\text{Ker } T}{(\sigma-1)O_N} \longrightarrow 0.$$

On sait que si  $N/k$  est non ramifiée en  $p$ ,  $\frac{\text{Ker } T}{(\sigma-1)O_N} = 0$ .

Nous ne nous intéressons donc qu'aux cas où  $N/k$  est ramifiée en  $p$ . Soient  $\mathfrak{p}_i$  les idéaux de  $O_k$  au-dessus de  $p$ ,  $\mathfrak{P}_i$  désigne l'idéal de  $O_N$  au-dessus de  $\mathfrak{p}_i$ . Dans ces conditions, on a :

$$(6) \quad \frac{\text{Ker } T}{(\sigma-1)O_N} \simeq \bigoplus_i \frac{\text{Ker } T_i}{(\sigma-1)O_{N_{\mathfrak{P}_i}}},$$

où  $N_{\mathfrak{p}_i}$  ( resp.  $k_{\mathfrak{p}_i}$  ) désigne le complété de  $N$  ( resp.  $k$  ) pour la valuation associée à  $\mathfrak{p}_i$  ( resp.  $\mathfrak{p}_i$  ) ,  $O_{N_{\mathfrak{p}_i}}$  est la clôture intégrale de  $Z_p$  dans  $N_{\mathfrak{p}_i}$  et  $\text{Ker } T_i$  le noyau de l'application trace dans  $N_{\mathfrak{p}_i}/k_{\mathfrak{p}_i}$  restreinte à  $O_{N_{\mathfrak{p}_i}}$  .

L'extension  $N/k$  étant ramifiée en  $p$  , on a  $\text{Gal}(N_{\mathfrak{p}_i}/k_{\mathfrak{p}_i}) = H$

ce qui justifie l'écriture au second membre de (6) . Déterminons les groupes  $\frac{\text{Ker } T_i}{(\sigma-1)O_{N_{\mathfrak{p}_i}}}$  . D'après la discussion de la fin du § 3 , on a :

$$(7) \quad \frac{\text{Ker } T_i}{(\sigma-1)O_{N_{\mathfrak{p}_i}}} \simeq \bigoplus_{\mu=1}^{p-1} \frac{O_{k_{\mathfrak{p}_i}}}{\mathfrak{p}_i^{(\mu)}} .$$

Il faut calculer  $(\mu)$  et pour cela connaître  $i(\mu)$  . Mais , par définition des groupes de ramification ,  $\sigma^\mu \in H_u \Rightarrow i(\mu) \geq u$  ; or la longueur de la suite des groupes de ramification est bornée de la façon suivante : Soit  $t$  tel que  $H_t \neq \{1\}$  ,  $H_{t+1} = \{1\}$  , l'extension  $N/k$  étant sauvagement ramifiée, on a  $1 \leq t \leq \left[ \frac{pe}{p-1} \right]$  où  $e$  est l'indice de ramification de  $p$  dans  $k/\mathbb{Q}$  . On a donc deux possibilités suivant que  $e = 1$  ou  $e = q$  . Pour  $e = 1$  , on a  $t = 1$ , donc pour  $1 \leq \mu \leq p-1$  ,  $i(\mu) = 1$  et l'indice  $(\mu)$  est égal à  $\left[ \frac{\mu+1}{p} \right]$  , il est donc nul sauf pour  $\mu = p-1$  où il vaut 1 . Pour  $e = q$  , on a  $1 \leq t \leq \left[ \frac{pq}{p-1} \right]$ . On peut alors montrer par des considérations sur le groupe des commutateurs de  $G$  ( même raisonnement que dans [6] ) que si  $p \neq 3$   $1 \leq t < q$  , si  $p = 3$   $t = 1$  ou  $t = 3$  .

Etudions les différents cas :

1<sup>er</sup> cas :  $e = 1$  ,  $p$  décomposé dans  $k/\mathbb{Q}$  .

D'après (6) et (7) on a  $\frac{\text{Ker } T}{(\sigma-1)O_N} \simeq \bigoplus_{i=1}^q V_i$  , chacun des  $V_i$

étant isomorphe à  $\mathbb{F}_p$  et  $g$  opérant transitivement sur les  $V_i$ . On en déduit que  $\frac{\text{Ker } T}{(\sigma-1)O_N}$  est un  $\mathbb{F}_p[g]$ -module qui donne la représentation régulière or :

$$O \otimes_{\mathbb{Z}[g]} \frac{\text{Ker } T}{(\sigma-1)O_N} \simeq \frac{\mathbb{Z}[g]}{1+\tau+\dots+\tau^{q-1}} \otimes_{\mathbb{Z}[g]} \frac{\text{Ker } T}{(\sigma-1)O_N} \simeq \frac{\frac{\text{Ker } T}{(\sigma-1)O_N}}{(1+\tau+\dots+\tau^{q-1})}$$

ce qui revient à retrancher la représentation triviale de la représentation régulière, soit :

$$(8) \quad O \otimes_{\mathbb{Z}[g]} \frac{\text{Ker } T}{(\sigma-1)O_N} \simeq \frac{\mathbb{Z}[w]}{(p)}$$

où  $w$  désigne pour toute la suite une racine primitive  $q$ -ième de l'unité qui sera précisée ultérieurement.

2<sup>ème</sup> cas :  $e = 1$ ,  $p$  inerte dans  $k/\mathbb{Q}$ .

Soit un relèvement de  $g$  dans  $\text{Gal}(N/\mathbb{Q})$  ( ce groupe est en effet produit semi-direct de  $H$  par  $g$  ) et  $K$  son corps des invariants. On note  $\Pi$  une uniformisante pour la place au-dessus de  $p$  dans  $K$ ; c'est également une uniformisante dans  $N$ .

Puisque  $K/\mathbb{Q}$  est totalement ramifiée en  $p$ , choisissons pour uniformisante dans  $O_p$  l'élément  $N_{K/\mathbb{Q}}(\Pi) = a$ . Construisons les  $x_\mu$

$$(1 \leq \mu \leq p-1) \text{ comme dans le lemme 1, on a donc } x_{p-1} = \frac{a}{\sigma^{-1}(\Pi)},$$

$$y_{p-1} = (\sigma-1)x_{p-1} = x_{p-1} \frac{(\sigma^{-1}-1)\Pi}{\Pi} \text{ et posons } v = \frac{y_{p-1}}{a} = \frac{\sigma^{-1}(\Pi) - \Pi}{\Pi \sigma^{-1}(\Pi)}.$$

Soit  $f$  l'application de  $O_{N_p}/\mathfrak{p}$  dans  $O_{N_p}$  qui donne le système de représentants multiplicatifs de  $O_{N_p}/\mathfrak{p}$ ; ce système est également le système de représentants multiplicatifs de  $O_{k_p}/\mathfrak{p}$ . Le groupe  $g$  opère à la fois

sur  $O_{k_p}/p$  et sur  $O_{k_p}$ , l'unicité du système de représentants implique  $f(\tau\beta) = \tau f(\beta)$ . On sait que  $\text{Ker } T$  admet pour  $O_{k_p}$ -base les éléments  $y_i = (\sigma-1)x_i$  ( $1 \leq i \leq p-2$ ) et  $v = \frac{y_{p-1}}{a}$ , d'autre part  $(\sigma-1)O_{N_{\mathbb{P}}}$  admet pour  $O_{k_p}$ -base les  $y_i$  ( $1 \leq i \leq p-1$ ). Tout élément de  $\frac{\text{Ker } T}{(\sigma-1)O_N}$  peut être représenté par un élément de la forme  $bv$  avec  $b = \sum_{n=0}^{\infty} f(\beta_n) a^n$  donc

$$bv = f(\beta_0)v + \left( \sum_{n=1}^{\infty} f(\beta_n) a^{n-1} \right) y_{p-1}.$$

On peut donc choisir dans  $O_{N_{\mathbb{P}}}$

des représentants des éléments de  $\frac{\text{Ker } T}{(\sigma-1)O_N}$  sous la forme  $f(\beta)v$ .

Pour connaître l'action de  $g$  sur  $\frac{\text{Ker } T}{(\sigma-1)O_N}$  il suffit de connaître  $\tau(v)$ .

Posons  $\sigma^{-1}(\pi) = \pi + f(\alpha)\pi^2 + \dots$ . Les conditions de ramification imposent  $t = 1$  donc  $v(\sigma^{-1}(\pi) - \pi) = 2$  soit  $\alpha \neq 0$ . On a donc

$$v = f(\alpha) + \sum_{n=1}^{\infty} f(u_n)\pi^n \quad \text{et} \quad \tau(v) = f(\tau(\alpha)) + \sum_{n=1}^{\infty} f(\tau(u_n))\pi^n.$$

Comme  $v$  appartient à  $\text{Ker } T$ , il en est de même de  $\tau(v)$  qui s'écrit par

conséquent sous la forme :  $\tau(v) = \sum_{i=1}^{p-2} b_i y_i + b_{p-1} v$  et dont l'image dans

$\frac{\text{Ker } T}{(\sigma-1)O_N}$  admet un représentant de la forme  $f(\beta)v$ . On sait que la va-

luation de  $\tau(v)$  est égale à celle de  $v$ , que les valuations des  $y_i$  et de  $v$  sont deux à deux distinctes modulo  $p$  et que celles des  $b_i$  sont congrues à zéro mod  $p$ . On en déduit que  $f(\beta)$  est le représentant tel que  $\tau(v) - f(\beta)v$  ait une valuation distincte de celle de  $v$ ; la comparaison des développements de  $v$  et  $\tau(v)$  montre que  $f(\beta) = \frac{f(\tau(\alpha))}{f(\alpha)} = f\left(\frac{\tau(\alpha)}{\alpha}\right)$ .

Considérons l'application de  $\frac{\text{Ker } T}{(\sigma-1)O_N}$  à valeurs dans  $O_{k_p}/p$  définie par

$$\varphi(\overline{f(\beta)v}) = \beta\alpha.$$

Proposition 4.    L'application  $\varphi$  est un homomorphisme de  $Z[g]$ -modules.

démonstration :

Montrons tout d'abord que  $\varphi$  est un homomorphisme de groupes.

Soient  $\beta_1$  et  $\beta_2$  deux éléments de  $\mathcal{O}_{k_p}/\mathfrak{p}$ , calculons  $\overline{\varphi(f(\beta_1)v + f(\beta_2)v)}$   
 $= \overline{\varphi((f(\beta_1) + f(\beta_2))v)}$  or  $f(\beta_1) + f(\beta_2) = f(\beta_1 + \beta_2) + u\alpha$  où  $u$  est une  
 unité de  $\mathcal{O}_{k_p}$  donc  $(f(\beta_1) + f(\beta_2))v = f(\beta_1 + \beta_2)v + u y_{p-1}$  par conséquent

$$\overline{(f(\beta_1) + f(\beta_2))v} = \overline{f(\beta_1 + \beta_2)v} \text{ d'où } \overline{\varphi(f(\beta_1)v + f(\beta_2)v)} = \beta_1\alpha + \beta_2\alpha.$$

Montrons maintenant que  $\varphi$  commute avec l'action de  $g$  :

$$\begin{aligned} \overline{\varphi(\tau(f(\beta)v))} &= \overline{\varphi(f(\tau(\beta))\tau(v))} = \overline{\varphi(f(\tau(\beta))f(\frac{\tau(\alpha)}{\alpha})v)} = \overline{\varphi(f(\frac{\tau(\beta\alpha)}{\alpha})v)} \\ &= \tau(\beta)\tau(\alpha) = \tau\overline{\varphi(f(\beta)v)}; \text{ ce qui démontre la proposition.} \end{aligned}$$

On constate immédiatement que  $\varphi$  est un isomorphisme d'où

$$\begin{aligned} \mathcal{O}'_{\otimes} \frac{\text{Ker } \tau}{Z[g](\sigma-1)\mathcal{O}_N} &\simeq \frac{Z[g]}{1+\tau+\dots+\tau^{q-1}} \otimes_{Z[G]} \frac{\mathcal{O}_{k_p}}{\mathfrak{p}} \simeq \frac{Z[g]}{1+\tau+\dots+\tau^{q-1}} \otimes_{Z[g]} \mathbb{F}_p[g] \\ &\simeq \frac{Z[w]}{(p)} \end{aligned}$$

3<sup>eme</sup> cas :  $e = q$ .

On désigne par  $\mathfrak{p}$  l'idéal premier de  $k$  au-dessus de  $p$ , par  $\mathfrak{P}$  l'idéal premier de  $N$  au-dessus de  $\mathfrak{p}$  et par  $\mathfrak{p}'_i$  les idéaux premiers de  $Z[w]$  au-dessus de  $(\mathfrak{p})$ . On localise en  $\mathfrak{p}$  et on choisit des uniformisantes de la façon suivante : dans  $k_p$  on choisit  $\pi$  tel que  $\pi^q \in \mathcal{O}_p$ ; on choisit ensuite une uniformisante  $\Pi_K$  dans  $K \cdot \mathcal{O}_p$ , l'élément  $\Pi = \Pi_K^{-\frac{p-1}{q}} \pi$  est une uniformisante de  $\mathfrak{P}$ . Pour le générateur  $\tau$  de  $g$ , l'élément  $\frac{\tau(\pi)}{\pi} = \frac{\tau(\Pi)}{\Pi}$  est une racine primitive  $q$ -ième de l'unité. Les résultats précédents qui faisaient appel à une racine primitive  $q$ -ième de l'unité ne changent pas si on la remplace par une de ses conjuguées. Il n'y a donc pas d'inconvénient à écrire  $\frac{\tau(\pi)}{\pi} = \omega$ , cet élément étant dans  $\mathcal{O}_p$ .

Soit  $t$  la longueur de la suite des groupes de ramification en numérotation inférieure,  $\sigma^\mu \in H_u \Leftrightarrow i(\mu) \geq u$  donc ici pour  $\mu \neq 0 \pmod{p}$  on a  $i(\mu) = t$ , d'où :



$$(\mu) = \left[ \frac{\mu+t}{p} \right] = \begin{cases} 0 & \text{si } 1 \leq \mu \leq p-t-1 \\ 1 & \text{si } p-t \leq \mu \leq p-1 \end{cases}$$

sauf si  $p=t=3$  auquel cas on a toujours  $(\mu) = 1$   
on a dans tous les cas  $p+t-1 < 2p$ .

Soit  $f$  l'application de  $O_{N_{\mathbb{P}}}/\mathbb{P}$  dans  $O_{N_{\mathbb{P}}}$  qui donne le système de représentants multiplicatifs de  $O_{N_{\mathbb{P}}}/\mathbb{P}$ ; ce système est le même que celui de  $Z_p/(p)$ , ses éléments sont invariants par  $G$ .

De la relation  $i(\mu) = v\left(\frac{(\sigma^\mu - 1)\Pi}{\Pi}\right) = t$ , on déduit l'existence d'un élément  $\alpha \neq 0$  tel que  $\sigma(\Pi) - \Pi = f(\alpha)\Pi^{t+1} \pmod{\Pi^{t+2}}$ .

Proposition 5. Avec les notations précédentes et celles du § 3 on a les relations :

$$y_\mu = \mu f(\alpha)\Pi^{\mu+t} + \epsilon \Pi^{\mu+t+1} \text{ où } \epsilon \text{ est une unité de } O_{N_{\mathbb{P}}} \text{ et } 1 \leq \mu \leq p-1$$

$$\tau^j(y_\mu) \equiv f(\alpha) \mu \omega^{j(\mu+t)} \Pi^{\mu+t} \pmod{\Pi^{\mu+t+1}}; \quad 1 \leq \mu \leq p-1.$$

Lemme 1. Pour  $1 \leq \mu \leq p-1$  on a  $\frac{\sigma^\mu(\Pi) - \Pi}{\Pi} \equiv \mu f(\alpha)\Pi^t \pmod{\Pi^{t+1}}$ .

démonstration :

$$\text{On a } \sigma(\Pi) - \Pi \equiv f(\alpha)\Pi^{t+1} \pmod{\Pi^{t+2}}$$

$$\text{d'où } \sigma^2(\Pi) - \sigma(\Pi) \equiv f(\alpha)(\Pi + f(\alpha)\Pi^{t+1})^{t+1} \pmod{\Pi^{t+2}}$$

$$\equiv f(\alpha)\Pi^{t+1} \pmod{\Pi^{t+2}}$$

$$\text{on en déduit : } \sigma^\mu(\Pi) - \sigma^{\mu-1}(\Pi) = f(\alpha)\Pi^{t+1} \pmod{\Pi^{t+2}}$$

$$\text{soit } \sigma^\mu(\Pi) - \Pi \equiv \mu f(\alpha)\Pi^{t+1} \pmod{\Pi^{t+2}}$$

Lemme 2 . On a les congruences : suivantes pour  $1 \leq \mu \leq p-1$

$$x_\mu \equiv \pi^\mu + f(\alpha) \frac{\mu \cdot (\mu-1)}{2} \pi^{\mu+t} \quad (\pi^{\mu+t+1})$$

démonstration :

Remarquons que  $(p) = (\pi^{pq})$  et que  $\mu+t < 2p \leq pq$  donc il n'est pas nécessaire de prendre le reste modulo  $p$  des coefficients de  $\pi^{\mu+t}$ . Au

§ 3 nous avons choisi  $x_\mu = \prod_{i=0}^{\mu-1} \sigma^i(\pi)$  ce qui entraîne :

$$\begin{aligned} x_\mu &= \prod_{i=0}^{\mu-1} (\pi + \sigma^i(\pi) - \pi) \equiv \prod_{i=0}^{\mu-1} (\pi + i f(\alpha) \pi^{t+1}) \quad (\pi^{\mu+t+1}) \\ &\equiv \pi^\mu + f(\alpha) \left( \sum_{i=0}^{\mu-1} i \right) \pi^{\mu+t} \quad (\pi^{\mu+t+1}) \end{aligned}$$

ce qui démontre la congruence

Démonstration de la proposition :

Nous pouvons écrire d'une part :

$$\begin{aligned} y_\mu &= (\sigma-1)x_\mu = x_\mu \frac{(\sigma^\mu - 1)\pi}{\pi} = x_\mu (\mu f(\alpha) \pi^t + \epsilon_1 \pi^{t+1}) \quad \text{où } \epsilon_1 \in \mathcal{O}_{N_{\mathfrak{p}}} \\ &= (\pi^\mu + f(\alpha) \frac{\mu(\mu-1)}{2} \pi^{\mu+t} + \epsilon_2 \pi^{\mu+t+1}) (\mu f(\alpha) \pi^t + \epsilon_1 \pi^{t+1}) \\ &= \mu f(\alpha) \pi^{\mu+t} + \epsilon \pi^{\mu+t+1} \end{aligned}$$

comme d'autre part  $\tau(\pi) = \alpha \pi$  on obtient la deuxième congruence;

la proposition 5 est donc démontrée.

On veut connaître  $O \otimes \frac{\text{Ker } T}{Z[g] (\sigma-1)O_N} \simeq \frac{\frac{\text{Ker } T_{\mathbb{P}}}{(\sigma-1)O_{N_{\mathbb{P}}}}}{1 + \tau + \dots + \tau^{q-1}}$ .

$\frac{\text{Ker } T_{\mathbb{P}}}{(\sigma-1)O_{N_{\mathbb{P}}}}$  est un  $\mathbb{F}_p[g]$ -module ; on peut le décomposer de la façon sui-

vante :  $\frac{\text{Ker } T_{\mathbb{P}}}{(\sigma-1)O_{N_{\mathbb{P}}}} = V_0 \oplus V$  où  $V_0$  est le sous-espace invariant par

$g$ . On aura  $O \otimes \frac{\text{Ker } T_{\mathbb{P}}}{Z[g] (\sigma-1)O_{N_{\mathbb{P}}}} \simeq V$ .

Pour connaître cette décomposition, déterminons le caractère

$\psi$  de la représentation de  $g$  sur  $\mathbb{F}_p$  fournie par  $\frac{\text{Ker } T_{\mathbb{P}}}{(\sigma-1)O_{N_{\mathbb{P}}}}$ . Pour ce

faire reprenons un raisonnement utilisé dans le deuxième cas.

On a une  $O_{k_p}$ -base de  $\text{Ker } T_{\mathbb{P}}$  formée par les  $\frac{y_{\mu}}{\pi^{(\mu)}} (1 \leq \mu \leq p-1)$  et une

$O_{k_p}$ -base de  $(\sigma-1)O_{N_{\mathbb{P}}}$  formée par les  $y_{\mu} (1 \leq \mu \leq p-1)$ . Un élément de

$O_{k_p}$  s'écrit  $\sum_{n=0}^{\infty} f(\beta_n) \pi^n$ , étant données les valeurs de  $(\mu)$ , tout élé-

ment de  $\frac{\text{Ker } T_{\mathbb{P}}}{(\sigma-1)O_{N_{\mathbb{P}}}}$  admet un représentant de la forme  $\sum_{\mu=p-t}^{p-1} f(b_{\mu}) \frac{y_{\mu}}{\pi}$ .

si  $p \neq 3$  et si  $p=3$ ; lorsque  $p=t=3$  ce représentant est de la

forme  $\sum_{\mu=1}^2 f(b_{\mu}) \frac{y_{\mu}}{\pi}$

On a remarqué que  $g$  opère trivialement sur les  $f(b_{\mu})$ , il suffit donc de

connaître l'action de  $g$  sur les  $\frac{y_{\mu}}{\pi}$ , plus précisément, pour connaître le

caractère  $\psi$  associé à cette représentation de  $g$ , il suffit, si on écrit

$$\tau^j \left( \frac{\overline{y_{\mu}}}{\pi} \right) = \sum_{i=p-t}^{p-1} b_{\mu,i}^j \frac{\overline{y_i}}{\pi},$$

$$\left( \text{sauf si } p=t=3 \text{ où l'on écrit } \tau^j\left(\frac{y_\mu}{\pi}\right) = \sum_{i=1}^2 b_{\mu+1}^j \frac{y_1}{\pi} \right)$$

de déterminer  $b_{\mu,\mu}^j$  et on a  $\psi(\tau^j) = \sum_{\mu} b_{\mu,\mu}^j$ . Mais on connaît

$$\tau^j(\pi^{(\mu)}) = w^{j(\mu)} \pi \text{ et on sait que l'on peut écrire } \tau^j(y_\mu) = \sum C_{\mu,i}^j y_i$$

avec les coefficients  $C_{\mu,i}^j$  dans  $O_{K_p}$  on peut également écrire d'après la

proposition 5  $\tau^j(y_\mu) = f(\alpha) \mu \omega^{j(\mu+t)\mu+t} + \epsilon \pi^{\mu+t+1}$ . On sait que les va-

luations des  $y_i$  sont deux à deux distinctes modulo  $p$  et que les coefficients

$C_{\mu,i}^j$  ont des valuations congrues à 0 modulo  $p$ . Le représentant  $f(b_{\mu,\mu}^j)$

est donc tel que  $v\left(\tau^j\left(\frac{y_\mu}{\pi}\right) - f(b_{\mu,\mu}^j) \frac{y_\mu}{\pi}\right) \neq v\left(\frac{y_\mu}{\pi}\right)$ . En comparant

les développements de  $y_\mu$  et  $\tau^j(y_\mu)$  donnés dans la proposition 5, on voit

que  $b_{\mu,\mu}^j$  est la classe de  $(w^{\mu-1+t})^j$ . On trouve donc que

$$b_{\mu,\mu}^j = \bar{w}^{(\mu+t-1)j} \text{ où } \bar{w} \text{ est la classe de } w \text{ dans } \mathbb{Z}_p / (\mathfrak{p}) = \mathbb{F}_p, \text{ ce qui}$$

nous donne :

$$\psi(\tau^j) = \sum_{\mu=p-t}^{p-1} \bar{w}^{(\mu+t-1)j}$$

$$\text{sauf si } p=t=3 \text{ où l'on a } \psi(\tau^j) = \sum_{i=1}^2 \bar{w}^{ij}$$

soit en tenant compte de la congruence  $p \equiv 1 \pmod{q}$

$$\psi(\tau^j) = \sum_{\ell=0}^{t-1} \bar{w}^{\ell j} \text{ sauf si } p=t=3 \text{ où } \psi(\tau^j) = \sum_{i=0}^1 \bar{w}^{ij}$$

Les caractères irréductibles de  $g$  à valeurs dans  $\mathbb{F}_p$  sont des caractères  $\psi_s$  de degré 1 définis par  $\psi_s(\tau^j) = \bar{w}^{sj}$ . On a donc :

$$\psi = \sum_{s=0}^{t-1} \psi_s \text{ sauf si } p=t=3 \text{ où } \psi = \psi_0 + \psi_1$$

D'après ce qui a été dit plus haut, le caractère de  $g$  fourni par le  $\mathbb{F}_p[g]$ -

module  $V = O \otimes \frac{\text{Ker } T}{(\sigma-1)O_N}$  est  $\sum_{\ell=1}^{t-1} \psi_\ell$  sauf si  $p=t=3$  où il est

égal à  $\psi_1$ . Le  $g$ -module  $V$  se décompose en une somme de  $(t-1)g$ -modules

irréductibles (sauf si  $p=t=3$  où l'on en a un seul), chacun de ces

facteurs étant isomorphe à un quotient  $\frac{\mathbb{Z}[w]}{\mathfrak{p}_i}$ . Définissons  $\mathfrak{p}'_1$  comme

étant l'idéal premier de  $Z[w]$  au-dessus de  $p$  associé au caractère  $\psi_1$ , ce qui revient à dire que  $\psi_1(\tau)$  est l'image de  $w$  dans  $\frac{Z[w]}{p'_1}$ ; soit  $\rho_\ell$  le  $Q$ -automorphisme de  $Q(w)$  défini par  $\rho_\ell(w) = w^\ell$  ( $1 \leq \ell \leq q-1$ ) on a  $\psi_\ell(\tau) = \psi_1(\tau)^\ell$  c'est donc l'image de  $\rho_\ell(w)$  dans  $\frac{Z[w]}{p'_1}$  c'est-à-dire l'image de  $w$  dans  $\frac{Z[w]}{\rho_\ell^{-1}(p'_1)}$ . Avec ces notations on peut donc énoncer :

Proposition 6. Lorsque  $N/Q$  est totalement ramifiée en  $p$ , le  $Z[w]$ -module

$$O \otimes_{Z[g]} \frac{\text{Ker } T}{(\sigma-1)O_N} \text{ est isomorphe à } \bigoplus_{i=1}^{t-1} \frac{Z[w]}{\rho_i^{-1}(p'_1)} \quad \cdot \text{sauf si } p=t=3$$

où  $O \otimes_{Z[g]} \frac{\text{ker } T}{(\sigma-1)O_N} = Z/3Z$

§5. Etude de  $O \otimes_{Z[g]} T_{N/k}(O_N)$  :

Comme  $O = \frac{Z[g]}{1+\tau+\dots+\tau^{q-1}}$ , le  $O$ -module  $O \otimes_{Z[g]} T_{N/k}(O_N)$

est isomorphe à  $\frac{T_{N/k}(O_N)}{(1+\tau+\dots+\tau^{q-1})T_{N/k}(O_N)}$  c'est-à-dire à  $\frac{T_{N/k}(O_N)}{T_{N/Q}(O_N)}$

Le  $Z[g]$ -module  $\frac{T_{N/k}(O_N)}{T_{N/k}(O_N) \cap Z}$  est annulé par  $1+\tau+\dots+\tau^{q-1}$  c'est

donc en fait un  $O$ -module, il est sans torsion, donc projectif. L'application canonique de

$$\frac{T_{N/k}(O_N)}{T_{N/Q}(O_N)} \longrightarrow \frac{T_{N/k}(O_N)}{T_{N/k}(O_N) \cap Z} \text{ est donc}$$

scindée. On en déduit :

Proposition 7 . Le O-module  $\frac{T_{N/k}(O_N)}{T_{N/Q}(O_N)}$  est O-isomorphe à la somme

directe des O-modules  $\frac{T_{N/k}(O_N)}{T_{N/k}(O_N) \cap Z}$  et  $\frac{T_{N/k}(O_N) \cap Z}{T_{N/Q}(O_N)}$  , ce dernier

étant son groupe de torsion .

1°) Détermination de  $\frac{T_{N/k}(O_N) \cap Z}{T_{N/Q}(O_N)}$  .

Rappelons que  $T_{N/k}(O_N) = \prod_{p|p} p^t$  avec  $0 \leq t < q$  ([4] proposition IV 1) sauf si  $p=t=3$  où  $T_{N/k}(O_N) = p^2 = (p)$  . On a, par conséquent:

$$T_{N/k}(O_N) \cap Z = \begin{cases} (p) & \text{si les idéaux } p \text{ sont ramifiés dans } N/k \\ Z & \text{sinon} \end{cases}$$

Calculons maintenant, lorsque l'on n'a pas  $p=t=3$ , l'idéal  $T_{N/Q}(O_N) = T_{k/Q} \left( \prod_{p|p} p^t \right)$  . Soit  $\mathfrak{D}$  la différentielle de l'extension  $k/Q$  , l'idéal  $T_{N/Q}(O_N)$  est le plus petit des idéaux  $\mathfrak{A}$  de  $Z$  tels que  $\prod_{p|p} p^t \subset \mathfrak{A} \mathfrak{D}^{-1}$  . On décompose  $\mathfrak{D}$  sous la forme :

$$\mathfrak{D} = Q^{2\epsilon(q-1)} \prod_{(\mathfrak{Q}, q) = 1} \mathfrak{Q}^{e_{\mathfrak{Q}} - 1}$$

où  $\epsilon = 0$  sauf lorsque  $q$  est ramifié dans  $k/Q$  auquel cas  $\epsilon = 1$  .  
 $Q$  est le produit des idéaux premiers de  $O_k$  au-dessus de  $q$  .  
 $\mathfrak{Q}$  parcourt les idéaux premiers de  $O_k$  , premiers avec  $q$  .  
 $e_{\mathfrak{Q}}$  est l'indice de ramification de  $\mathfrak{Q}$  .

L'inclusion qui définit  $\mathfrak{A}$  montre que  $\mathfrak{A}$  est divisible par  $q^{\epsilon}$  exactement ; la comparaison des deux membres montre que :

$$u = \begin{cases} q^\epsilon & \text{si } t = 0 \\ pq^\epsilon & \text{si } 1 \leq t < q \end{cases}$$

ce qui prouve que  $\frac{T_{N/k}(O_N) \cap Z}{T_{N/k}(O_N)} \simeq \frac{Z}{q^\epsilon Z}$  ; lorsque  $p=t=3$

$$T_{N/Q}(O_N) = T_{k/Q}(pO_k) = (q^\epsilon p) \frac{T_{N/k}(O_N) \cap Z}{T_{N/k}(O_N)}$$

Proposition 8 . Le O-module  $\frac{T_{N/k}(O_N) \cap Z}{T_{N/Q}(O_N)}$  est isomorphe à  $\frac{Z[u]}{(1-w)^\epsilon Z[w]}$

2°) Détermination de  $\frac{T_{N/k}(O_N)}{T_{N/k}(O_N) \cap Z}$  .

Soit  $\chi$  un caractère de degré 1 de  $g$  , non trivial , à valeurs dans  $\mathbb{C}$  . Soit  $\theta_0$  un élément de  $k$  engendrant avec ses conjugués une base normale de  $k/Q$  ; on considère l'application  $g_{\chi, \theta_0}$  de  $k$  dans  $Q(w)$  définie par :

$$g_{\chi, \theta_0}(\theta) = \frac{\langle \theta, \chi \rangle}{\langle \theta_0, \chi \rangle}$$

où  $\langle \theta, \chi \rangle = \sum_{i=0}^{q-1} \tau^i(\theta) \chi(\tau^{-i})$  est la résolvante de Lagrange de  $\theta$  et de

$\chi$  (cf. [3]) . On sait que  $\text{Ker}(g_{\chi, \theta_0}) = Q$  donc , si on restreint  $g_{\chi, \theta_0}$

à  $T_{N/k}(O_N)$  , on a  $g_{\chi, \theta_0}(T_{N/k}(O_N)) \simeq \frac{T_{N/k}(O_N)}{T_{N/k}(O_N) \cap Z}$  .

Remarque 1 . Lorsque  $p$  n'est pas ramifié dans  $k/Q$  , on a

$$\prod_{p|p} p^t = (p^t) \text{ et } g_{\chi, \theta_0}(T_{N/k}(O_N)) = p^t g_{\chi, \theta_0}(O_k) .$$

de même lorsque  $p=t=3$   $g_{\chi, \theta_0}(T_{N/k}(O_N)) = p g_{\chi, \theta_0}(O_k)$

Remarque 2 . On peut procéder à un choix particulier de l'élément  $\theta_0$  pour simplifier certains calculs . Soit  $f$  le conducteur de l'extension  $k/Q$  ,

$\mathbb{Q}(f)$  le  $f$ -ième corps cyclotomique contient  $k$ . La somme de Gauss associée au caractère  $\chi$  est définie de la façon suivante :

pour tout  $\sigma \in \text{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ , on définit l'entier  $m_\sigma$  modulo  $f$  par

$\sigma(\zeta_f) = \zeta_f^{m_\sigma}$ ,  $\zeta_f$  est une racine primitive  $f$ -ième de l'unité, c'est en fait

la définition de l'isomorphisme de réciprocité :  $\sigma = (m_\sigma, \mathbb{Q}(f)/\mathbb{Q})$  : on

considère le caractère  $\chi$  comme un caractère du groupe de Galois  $\mathbb{Q}(f)/\mathbb{Q}$

(puisque  $k \subset \mathbb{Q}(f)$ ) et, au moyen de l'isomorphisme de réciprocité,

comme un caractère modulo  $f$  par  $\chi(a) = \overline{\chi((a, \mathbb{Q}(f)/\mathbb{Q}))}$  pour  $(a, f) = 1$ .

La somme de Gauss est  $\tau(\chi) = \sum_{\substack{1 \leq a \leq f \\ (a, f) = 1}} \chi(a) \zeta_f^a = \sum_{\sigma \in \text{Gal}(\mathbb{Q}(f)/\mathbb{Q})} \sigma(\zeta_f) \chi(\sigma^{-1})$

$$= \langle T_{\mathbb{Q}(f)/\mathbb{Q}}(\zeta_f), \chi \rangle .$$

On peut alors trouver un élément  $\theta_\chi$  tel que  $\langle \theta_\chi, \chi \rangle = \tau(\chi)$ . Avec ce choix

nous définissons  $g_\chi$  par  $g_\chi(\theta) = \frac{\langle \theta, \chi \rangle}{\tau(\chi)}$ . Les propriétés classiques des

résolvantes de Lagrange montrent que  $\tau(\chi)^q \in \mathbb{Q}(w)$ . Écrivons

$(\tau(\chi)^q) = \mathfrak{R}(\chi)^q \prod_{i=1}^{q-1} \rho_i^{-1}(\mathfrak{J})^i$  où  $\mathfrak{J}$  est un produit d'idéaux premiers,

décomposés dans  $\mathbb{Q}(w)/\mathbb{Q}$ , tel que  $N_{\mathbb{Q}(w)/\mathbb{Q}}(\mathfrak{J})$  soit sans facteur carré,

$\rho_i$  a été défini au § 4, 3<sup>ème</sup> cas. On a par ailleurs  $\tau(\chi^{-1}) = \rho_{-1}(\tau(\chi))$

et  $(\tau(\chi) \tau(\chi^{-1})) = (f)$ ; l'étude de  $\mathfrak{J}$  et de la ramification dans  $k/\mathbb{Q}$

montrent que  $\mathfrak{R}(\chi) = \mathbb{Z}[w]$  si  $(f, q) = 1$  et  $\mathfrak{R}(\chi) = q\mathbb{Z}[w]$  sinon. On peut

également déterminer  $g_\chi(\mathcal{O}_k)$ . On sait grâce aux propriétés des résol-

vantes de Lagrange que l'on a la double inclusion

$$q \mathfrak{R}(\chi)^{-1} \subset g_\chi(\mathcal{O}_k) \subset \mathfrak{R}(\chi)^{-1} \quad (\text{cf. [3] prop III 6})$$

On peut montrer par des calculs de discriminants que :



$$g_{\chi}(O_k) = \begin{cases} \mathfrak{R}(\chi)^{-1} & \text{si } k/\mathbb{Q} \text{ est modérément ramifiée} \\ q\mathfrak{R}(\chi)^{-1} & \text{sinon} \end{cases}$$

Avec le choix de  $g_{\chi}$  ici fait on obtient :

$$g_{\chi}(O_k) = Z[w] .$$

On en déduit :

Proposition 9 .    Lorsque  $p$  n'est pas ramifié dans  $k/\mathbb{Q}$  , on a :

$$\frac{T_{N/k}(O_N)}{T_{N/k}(O_N) \cap Z} \simeq g_{\chi}(T_{N/k}(O_N)) = p^t Z[w] \quad (t = 0 \text{ ou } 1) .$$

De même lorsque  $p=t=3$  on a  $g(T_{N/k}(O_N)) = 3Z$

Il nous reste à déterminer  $\frac{T_{N/k}(O_N)}{T_{N/k}(O_N) \cap Z}$  dans le cas

où  $p$  est totalement ramifié dans  $N/\mathbb{Q}$  . Il s'agit , avec des conditions légèrement différentes , d'un calcul effectué par Ullom ([10]) . Nous en redonnons rapidement la démonstration :

Soit  $p$  l'idéal premier de  $O_k$  au-dessus de  $p$  ,  $p''_i$  les idéaux premiers de  $O_{k(w)}$  au-dessus de  $p$  et  $p'_i = p''_i \cap \mathbb{Q}(w)$  . Fixons  $p''$  ,  $p' = p'' \cap \mathbb{Q}(w)$  , de sorte que  $p'$  soit l'idéal au-dessus de  $p$  divisant  $\mathfrak{Z}$  .

Soit  $t$  , tel que  $1 \leq t < q$  et  $x \in p^t$  , on a  $\langle x, \chi \rangle = \sum_{i=1}^{q-1} \tau^i(x) \chi(\tau^{-i})$  qui

appartient à  $\left( \prod_{i=1}^{q-1} \rho_i^{-1}(p'') \right)^t$  donc :

$$\langle x, \chi \rangle^q \in \left( \sum_{i=1}^{q-1} \rho_i^{-1}(p') \right)^t$$

Or  $(\langle x, \chi \rangle^q) = (g_{\chi}(x) \mathfrak{R}(\chi))^q \sum_{i=1}^{q-1} \rho_i^{-1}(\mathfrak{Z})^i$

on en déduit :

$$(9) \quad \left( \prod_i \rho_i^{-1}(p') \right)^t \supset (g_X(p^t) \mathfrak{R}(X))^q \prod_{i=1}^{q-1} \rho_i^{-1}(\mathfrak{Z})^i$$

$$\begin{aligned} \text{or } [O_k : p^t] &= [g_X(O_k) : g_X(p^t)] \times [(\ker g_X(O_k) : (\ker g_X | p^t))] \\ &= [g_X(O_k) : g_X(p^t)] \times [Z : pZ] \end{aligned}$$

ce qui donne

$$(10) \quad p^{t-1} = [g_X(O_k) : g_X(p^t)] .$$

On voit aisément que  $g_X(O_k)$  et  $g_X(p^t)$  sont des idéaux de  $Z[w]$ , qui sont localement égaux, sauf pour les places au-dessus de  $p$ ; comme  $g_X(O_k) \supset g_X(p^t)$ , on peut écrire

$$(11) \quad g_X(p^t) = g_X(O_k) \prod_{i=1}^{q-1} \rho_i^{-1}(p')^{c_i}$$

$$\text{soit } g_X(p^t) = \mathfrak{R}(X)^{-1} q^\epsilon \prod_{i=1}^{q-1} \rho_i^{-1}(p')^{c_i}$$

où  $\epsilon$  égal 1 (resp. 0) si  $k/\mathbb{Q}$  est (resp. n'est pas) ramifiée en  $q$ .

Donc, d'après (9)

$$\prod_i \rho_i^{-1}(p^t) \mid q^{q\epsilon} \prod_{i=1}^{q-1} \rho_i^{-1}(\mathfrak{Z}^i p'^{qc_i})$$

$$\text{on obtient donc } t \leq i + qc_i \quad \text{soit } c_i \geq \left[ \frac{t-i-1}{q} \right] + 1 .$$

Les relations (10) et (11) ajoutées au fait que  $p$  est décomposé dans  $\mathbb{Q}(w)$

$$\text{montrent que } \sum_{i=1}^{q-1} c_i = t-1 \quad \text{or } \sum_{i=1}^{q-1} \left[ \frac{t-i-1}{q} \right] + 1 = \sum_{i=1}^{t-1} \left[ \frac{t-1-i}{q} \right] + 1 = t-1$$

d'où la proposition .

Proposition 10. Avec les notations précédentes, le  $Z[w]$ -module

$$\frac{T_{N/k}(O_N)}{T_{N/k}(O_N) \cap Z} \text{ est isomorphe à } \prod_{i=1}^{q-1} \rho_i^{-1}(p')^{c_i} \text{ avec } c_i = \left[ \frac{t-i-1}{q} \right] + 1$$

$$\text{soit à } \prod_{i=1}^{q-1} \rho_i^{-1}(p') .$$

Comparons l'idéal  $p'_1$  de la proposition 6 et l'idéal  $p'$  de la proposition 10. Choisissons  $\omega \in \mathbb{Z}_p$  une racine primitive  $q$ -ième de l'unité, fixons  $\tau$  élément de  $\text{Gal}(k/\mathbb{Q}) = \text{Gal}(k_{p/p})$  et choisissons  $\chi$  le caractère de  $g$  tel que  $\chi(\tau) = \omega$ ; l'élément  $\tau(\chi)$  appartient à  $k(\omega)$  et il existe une et une seule place  $p''$  au-dessus de  $p$  telle que  $v_{p''}(\tau(\chi)) = 1$ .

Localisons en  $p''$ . On a  $k(\omega)_{p''} = k_p$  et on prend  $\tau(\chi)$  comme uniformisante. On a alors  $\tau(\tau(\chi)) = \chi(\tau) \tau(\chi) = \omega \tau(\chi)$ , ce qui identifie  $\tau(\chi)$  avec  $\pi$  et montre que l'image de  $\omega$  dans  $\frac{\mathcal{O}_{k(\omega)}}{p''} = \frac{\mathbb{Z}[\omega]}{p'}$  est la même que

dans  $\frac{\mathcal{O}_{k_p}}{p} = \frac{\mathbb{Z}_p}{p}$ . On a donc  $p' = p'_1$ . D'où en regroupant les différents résultats :

Proposition 11. En désignant par  $e$  l'indice de ramification de  $p$  dans l'extension  $N/\mathbb{Q}$ , on a avec les notations précédentes :

$$\mathcal{O} \otimes_{\mathbb{Z}[g]} \mathcal{O}_N \text{ isomorphe à } \begin{cases} \frac{\mathbb{Z}[\omega]}{(1-\omega)^e} & \text{si } e = 1 \text{ ou } e=q \\ \frac{\mathbb{Z}[\omega]}{(p)} \oplus \frac{\mathbb{Z}[\omega]}{(1-\omega)^e} \oplus p\mathbb{Z}[\omega] & \text{si } e = p \\ \bigoplus_{i=1}^t \frac{\mathbb{Z}[\omega]}{\rho_i^{-1}(p')} \oplus \frac{\mathbb{Z}[\omega]}{(1-\omega)^e} \oplus \prod_{i=1}^{t-1} \rho_i^{-1}(p') & \text{si } e = pq \text{ en} \end{cases}$$

excluant le cas  $p=t=3$ . Si  $p=t=3$ , on trouve :  $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2^e\mathbb{Z} \oplus 3\mathbb{Z}$

On en déduit immédiatement le théorème :

Théorème 3. Lorsque  $N/\mathbb{Q}$  est une extension non abélienne de degré  $pq$  ( $p$  et  $q$  premiers  $q \mid p-1$ ) du corps des rationnels, l'image de  $\mathcal{O} \otimes_{\mathbb{Z}[G]} \mathcal{O}_N$  dans le groupe de Grothendieck des  $\mathcal{O}$ -modules de type fini est l'élément neutre de ce groupe.

- [1] D. CHATELAIN : Etude du  $O$ -module  $O \otimes_{\mathbb{Z}[G]} O_N$  pour une extension  $N/Q$  abélienne de groupe  $G$  avec  $O$  ordre maximal de  $\mathbb{Q}[G]$ ,  $O_N$  anneau des entiers de  $N$ . Séminaire de Théorie des nombres de Besançon 1976-77.
- [2] J. COUGNARD : Propriétés galoisiennes des anneaux d'entiers .  
Thèse ( Bordeaux 1975 ) .
- [3] J. COUGNARD : Propriétés galoisiennes des anneaux d'entiers des  $p$ -extensions dans Compositio math. ) .
- [4] J. COUGNARD : Un contre exemple à une conjecture de J. Martinet .  
Proc. Durham Symposium 1975 .
- [5] A. FRÖHLICH : Galois Module Structure .  
Proc. Durham Symposium 1975 .
- [6] J. MARTINET : Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre  $2p$  .  
Ann. Inst. Fourier 19 ( 1969 ) p. 1-80 .
- [7] S. SEN : On automorphisms of local fields .  
Annals of Math. Vol. 90 n° 1 Juillet 69 p. 33-46 .
- [8] SWAN-EVANS : K-Theory of finite groups and maximal Orders. Lecture note n° 143 Springer Verlag - 1976-
- [9] S. ULLOM : Integral normal bases in Galois extensions of local fields.  
Nagoya Math. J. Vol 39 ( 1970 ), 141-148 .
- [10] S. ULLOM : Integral representations afforded by ambiguous ideals in some abelian extensions .  
J. Number Theory 6 ( 1974 ) 32-49 .

Jean COUGNARD  
Faculté des Sciences. Mathématiques  
E. R. A. CNRS n° 070654  
25030 BESANCON CEDEX