EORIE 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 . C N R S N° 070654
25030 Besançon Cedex

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

ERRATA:

page 7: changer les G en g .
Au bas de la page supprimer la phrase commençantà :" 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:
ε est une unité de O_{N_F} par ε appartient à O_{N_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 3e remplacer $\bigoplus_{i=1}^{t}$ par $\bigoplus_{i=1}^{t-1}$.

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, O_N la clôture intégrale de $\mathbb{Z}$ dans N et O un ordre maximal de $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$. Construisons le O-module OO_N ; dans le cas où $N/\mathbb{Q}$ est modérément ramifiée, A. Fröhlich a démontré que OO_N est O-stablement libre [5], ce qui revient à dire que la classe de OO_N dans le groupe des classes projectives de 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 OO_N ne soit pas stablement libre ([4]).

On peut néanmoins remarquer que dans le cas modérément ramifié OO_N est O-isomorphe à $O \otimes_{\mathbb{Z}[G]} O_N$. On peut donc se proposer d'étudier le O-module $O \otimes_{\mathbb{Z}[G]} O_N$ dans les extensions sauvagement ramifiées. Ce 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 $G_0(O)$ des 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 $O \otimes_{\mathbb{Z}[G]} O_N$ est isomorphe à une somme directe $OO_N \oplus T$ où T est un O-module fini. Dans le cas où G est un groupe non abélien d'ordre pq, on montre que la classe de T dans $G_0(O)$ est l'opposée de celle de OO_N ce qui montre que l'image de $O \otimes_{\mathbb{Z}[G]} O_N$ dans $G_0(O)$ 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 Léopoldt.

§ 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 λ 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

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

comme $G_o(O) \simeq \prod_{i=1}^{r} G_o(O_i)$ 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 $Q \otimes_Z (O_i \otimes_{Z[G]} O_N)$ et $Q \otimes_Z (O_i\, O_N \oplus M_i)$:

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

d'où l'on déduit que $Q \otimes_Z M_i = 0$ 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

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

Or, on peut déduire du théorème I-2 de [8] que la classe de E dans $G_0(O_i)$ est l'élément neutre. On a donc:

$cl(O_i \otimes_{Z[G]} O_N) = -\, cl(E')$ 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 :

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} (O_i \otimes_{\mathbb{Z}[G]} O_N) \simeq (\mathbb{Z}_p \otimes_{\mathbb{Z}} O_i\, O_N) \oplus (\mathbb{Z}_p \otimes_{\mathbb{Z}} T_i)$$

$$\simeq (\mathbb{Z}_p \otimes_{\mathbb{Z}} O_i) \otimes_{\mathbb{Z}_p[G]} (\mathbb{Z}_p \otimes_{\mathbb{Z}} O_N)$$

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 $G_o(O)$ est l'élément neutre .

démonstration :

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

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

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 $O_1 \simeq \mathbb{Z}$, $O_2 \simeq \mathbb{Z}[\omega]$ (ω 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 $G_o(O_3)$ est l'élément neutre.

démonstration :

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

$$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} O_3 \simeq \Lambda_\ell$$

ce qui donne:

$$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} (O_3 O_N \oplus T_3) \simeq \mathbb{Z}_\ell \otimes_{\mathbb{Z}} (O_3 \otimes_{\mathbb{Z}[G]} O_N) \simeq (\mathbb{Z}_\ell \otimes_{\mathbb{Z}} O_3) \otimes_{\mathbb{Z}_\ell[G]} (\mathbb{Z}_\ell \otimes_{\mathbb{Z}} O_N)$$
$$\simeq \mathbb{Z}_\ell \otimes_{\mathbb{Z}} (O_3 O_N)$$

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

Dans le cas des groupes non abéliens d'ordre pq , il reste à étudier $O_2 \otimes_{\mathbb{Z}[G]} O_N$. Le facteur simple O_2 est associé aux caractères χ 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 $\mathbb{Z}[g]$. On considère $N_{/\mathbb{Q}}$ une extension galoisienne de groupe de Galois G telle que N contienne k . On s'intéresse au O'-module $O' \otimes_{\mathbb{Z}[G]} O_N$. Notons $H = \mathrm{Gal}(N_{/k})$.

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

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

On est donc conduit à étudier en premier lieu $\mathbb{Z}[g] \otimes_{\mathbb{Z}[G]} O_N$. Il y a une surjection de $\mathbb{Z}[g] \otimes_{\mathbb{Z}} O_N \longrightarrow \mathbb{Z}[g] \otimes_{\mathbb{Z}[g]} O_N$ dont le noyau est le sous-$\mathbb{Z}$-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

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

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

Proposition 3 . Il y a un isomorphisme de $\mathbb{Z}[g]$-modules entre $\mathbb{Z}[g] \otimes_{\mathbb{Z}[G]} O_N$ et $O_N/I_H O_N$ où I_H est l'idéal de $\mathbb{Z}[H]$ 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 $\tau = 1.g$; 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 $p : \mathbb{Z}[G] \times O_N \longrightarrow O_N/I_H O_N$ définie de la façon suivante : pour $\tau \in g$, il existe $g \in G$ tel que $\tau = 1.g$; posons $p(\tau, x) = \overline{gx}$. Si on remplace g par g_1 , on a $gg_1^{-1} \in H$ d'où $g = h g_1$ et $gx - g_1 x = (h-1) g_1 x \in I_H O_N$ 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 $\overline{p}$ de $\mathbb{Z}[g]$-modules de $\mathbb{Z}[g] \otimes_{\mathbb{Z}[G]} O_N$ dans $O_N/I_H O_N$. L'application p étant surjective , il en est de même de $\overline{p}$. Montrons que cet homomorphisme est injectif :

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

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 $O' \otimes_{\mathbb{Z}[g]} O_N/I_H O_N$.

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 $\mathbb{Z}[g]$-module :

(1) $$0 \longrightarrow \frac{\operatorname{Ker} T}{I_H O_N} \longrightarrow \frac{O_N}{I_H O_N} \longrightarrow T_{N/k}(O_N) \longrightarrow 0$$

où Ker T désigne le noyau de la trace dans l'extension N/k restreinte à O_N. De (1) on déduit la suite exacte :

(2) $$\operatorname{Tor}_1^{\mathbb{Z}[G]}(O', T_{N/k}(O_N)) \longrightarrow O' \otimes_{\mathbb{Z}[G]} \frac{\operatorname{Ker} T}{I_H O_N} \longrightarrow \cdots$$

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

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) $$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \operatorname{Tor}_1^{\mathbb{Z}[G]}(O', T_{N/k}(O_N)) \longrightarrow (\mathbb{Z}_\ell \otimes_{\mathbb{Z}} O') \otimes_{\mathbb{Z}_\ell[G]} \left(\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \frac{\operatorname{Ker} T}{I_H O_N}\right) \longrightarrow$$

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

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

Mais $T_{N/k}(O_N)$ est un idéal de O_k, si $\ell \neq q$ $O_\ell \otimes_{\mathbb{Q}} k$ est une algèbre de Galois modérément ramifiée donc $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} T_{N/k} O_N$ 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) $$0 \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \frac{\operatorname{Ker} T}{I_H O_N} \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \frac{O_N}{I_H O_N} \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} T_{N/k}(O_N) \longrightarrow 0$$

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 $(\mathbb{Z}_\ell \otimes_{\mathbb{Z}} O') \otimes_{\mathbb{Z}_\ell[G]}$.

Pour $\ell = q$, $\frac{\operatorname{Ker} T}{I_H O_N}$ a pour ordre une puissance de p, par conséquent on a $\mathbb{Z}_q \otimes_{\mathbb{Z}} \frac{\operatorname{Ker} T}{I_H O_N} = 0$. On en déduit que la ℓ-composante de l'image de

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

Théorème 1. La suite de O-modules :

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

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 $O' \otimes_{\mathbb{Z}[g]} \frac{\mathrm{Ker}\, T}{I_H O_N}$ 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 σ un générateur de $\mathrm{Gal}(K/F)$, π (resp. Π) 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_μ tel que $v_K(x_\mu) = \mu$ et $v((\sigma - 1)x_\mu) = \mu + i(\mu)$ $\left(\text{on choisit } x_\mu = \prod_{i=0}^{\mu-1} \sigma^i(\Pi)\right)$.

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_μ 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 $i_{j-1} \equiv i_j \bmod p^j$ alors les entiers $\mu + i(\mu)$ avec $v_Q(\mu) < s$ sont tous distincts et distincts de i_{s-1} .

On déduit de ces lemmes :

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

Ces résultats permettent de déterminer la structure du groupe $\operatorname{Ker} T_{K/F} \big/ (1-\sigma) A$ de la façon suivante . Pour μ tel que $1 \le \mu \le p^n - 1$ choisissons des x_μ dans K vérifiant les conditions du lemme 1 . Les x_μ et 1 forment une B-base de A ; posons $y_\mu = (\sigma - 1) x_\mu$, du théorème et du lemme 3 on déduit que les y_μ ont des valuations distinctes et même que les entiers $v_K(y_\mu)$ sont distincts modulo p^n ([6] p. 38) donc les y_μ forment une B-base de $(1-\sigma)A$. Il en résulte que les y_μ 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 $v_K(z) \ge 0$, $v_K(b_\mu) \equiv 0 \ (p^n)$; 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 μ on a $p^n v_F(b_\mu) + \mu + i(\mu) \ge 0$ ce qui équivaut à $v_F(b_\mu) \ge -\left[\frac{\mu + i(\mu)}{p^n}\right]$.

Une B-base de $\operatorname{Ker} T_{K/F}$ 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 σ et τ 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 σ , k le sous-corps de N formé des éléments invariants par H et $g = G/H$. Nous voulons étudier $O' \otimes_{\mathbb{Z}[g]} \frac{\operatorname{Ker} T}{I_H O_N} = O' \otimes_{\mathbb{Z}[g]} \frac{\operatorname{Ker} T}{(\sigma-1)O_N}$ où O' est isomorphe à $\mathbb{Z}[\omega]$ (ω racine primitive q-ieme de l'unité) .

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

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

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

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

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

$$(5) \qquad 0 \longrightarrow (\sigma-1)\mathbb{Z}_p \otimes_{\mathbb{Z}} O_N \longrightarrow \operatorname{Ker} T_{\mathbb{Z}_p \otimes_{\mathbb{Z}} O_N} \Big/ \mathbb{Z}_p \otimes_{\mathbb{Z}} O_k \longrightarrow \frac{\operatorname{Ker} T}{(\sigma-1)O_N} \longrightarrow 0 .$$

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

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 :

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

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

L'extension N/k étant ramifiée en p , on a $\mathrm{Gal}\left(N_{\mathfrak{P}_i}/k_{p_i}\right) = H$ ce qui justifie l'écriture au second membre de (6) . Déterminons les groupes $\dfrac{\mathrm{Ker}\ T_i}{(\sigma-1)\,O_{N_{\mathfrak{P}_i}}}$. D'après la discussion de la fin du § 3 , on a :

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

Il faut calculer (μ) et pour cela connaître $i(\mu)$. Mais , par définition des groupes de ramification , $\sigma^{\mu} \in H_u \Leftrightarrow i(\mu) \geq u$; 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 $1 \leq t \leq \left[\dfrac{pe}{p-1}\right]$ 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 (μ) est égal à $\left[\dfrac{\mu+1}{p}\right]$, il est donc nul sauf pour $\mu = p-1$ où il vaut 1 . Pour $e = q$, on a $1 \leq t \leq \left[\dfrac{pq}{p-1}\right]$.

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 :

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

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

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

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

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

$$(8) \qquad O \otimes_{\mathbb{Z}[g]} \frac{\operatorname{Ker} T}{(\sigma-1)O_N} \simeq \frac{\mathbb{Z}[\omega]}{(p)}$$

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

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

Soit un relèvement de g dans $\mathrm{Gal}(N/\mathbb{Q})$ (ce groupe est en effet produit semi-direct de H par g) et K son corps des invariants . On note Π 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 $\mathbb{Q}_p$ l'élément $N_{K_\mathfrak{p}/\mathbb{Q}_p}(\Pi) = a$. Construisons les x_μ ($1 \le \mu \le p-1$) comme dans le lemme 1 , on a donc $x_{p-1} = \frac{a}{\sigma^{-1}(\Pi)}$,

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

Soit f l'application de $O_{N_\mathfrak{P}/\mathfrak{P}}$ dans $O_{N_\mathfrak{P}}$ qui donne le système de représentants multiplicatifs de $O_{N_\mathfrak{P}/\mathfrak{P}}$; ce système est également le système de représentants multiplicatifs de $O_{k_p/p}$. 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 Ker T admet pour O_{k_p}-base les éléments $y_i = (\sigma-1)x_i$ $(1 \le i \le p-2)$ et $v = \frac{y_{p-1}}{a}$, d'autre part $(\sigma-1)O_{N_\mathfrak{P}}$ admet pour O_{k_p}-base les y_i $(1 \le i \le p-1)$. 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 $bv = f(\beta_o)\, v + \left(\sum_{n=1}^{\infty} f(\beta_n)\, a^{n-1} \right) y_{p-1}$. On peut donc choisir dans $O_{N_\mathfrak{P}}$ 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 $\sigma^{-1}(\Pi) = \Pi + f(\alpha)\Pi^2 + \ldots$ 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 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 valuation 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 φ est un homomorphisme de $\mathbb{Z}[g]$-modules.

démonstration :

Montrons tout d'abord que φ est un homomorphisme de groupes. Soient β_1 et β_2 deux éléments de $O_{k_p}/\mathfrak{p}$, calculons $\varphi(\overline{f(\beta_1)v} + \overline{f(\beta_2)v})$ $= \varphi(\overline{(f(\beta_1)+f(\beta_2))v})$ or $f(\beta_1) + f(\beta_2) = f(\beta_1+\beta_2) + u a$ où u est une unité de O_{k_p} donc $(f(\beta_1) + f(\beta_2))\, v = f(\beta_1+\beta_2)\, v + u\, y_{p-1}$ par conséquent

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

Montrons maintenant que φ commute avec l'action de g :

$$\varphi(\tau(\overline{f(\beta)v}) = \varphi(\overline{f(\tau(\beta))\,\tau(v)}) = \varphi(\overline{f(\tau(\beta))\, f(\frac{\tau(\alpha)}{\alpha})v}) = \varphi(\overline{f(\frac{\tau(\beta\alpha)}{\alpha})v})$$

$$= \tau(\beta)\,\tau(\alpha) = \tau\,\varphi(\overline{f(\beta)v}) \; ;$$ ce qui démontre la proposition .

On constate immédiatement que φ est un isomorphisme d'où

$$O' \otimes_{\mathbb{Z}[g]} \frac{\operatorname{Ker} T}{(\sigma-1)O_N} \simeq \frac{\mathbb{Z}[g]}{1+\tau+\ldots+\tau^{q-1}} \otimes_{\mathbb{Z}[G]} \frac{O_{k_p}}{p} \simeq \frac{\mathbb{Z}[g]}{1+\tau+\ldots+\tau^{q-1}} \otimes_{\mathbb{Z}[g]} \mathbb{F}_p[g]$$

$$\simeq \frac{\mathbb{Z}[\omega]}{(p)}$$

3ème 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 p et par $\mathfrak{p}_i'$ les idéaux premiers de $\mathbb{Z}[\omega]$ au-dessus de (p) . On localise en p et on choisit des uniformisantes de la façon suivante : dans k_p on choisit π tel que $\pi^q \in \mathbb{Q}_p$; on choisit ensuite une uniformisante Π_K dans $K.\mathbb{Q}_p$, l'élément $\Pi = \Pi_K^{-\frac{p-1}{q}}\,\pi$ est une uniformisante de $\mathfrak{P}$. Pour le générateur τ 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 $\mathbb{Q}_p$.

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 $\mu \not\equiv 0 \;(p)$ on a $i(\mu) = t$, d'où :

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

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 $O_{N_{\mathfrak{P}}/\mathfrak{P}}$ dans $O_{N_{\mathfrak{P}}}$ qui donne le système de représentants multiplicatifs de $O_{N_{\mathfrak{P}}/\mathfrak{P}}$; ce système est le même que celui de $\mathbb{Z}_{p/(p)}$, 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 :

$y_{\mu} = \mu f(\alpha)\Pi^{\mu+t} + \varepsilon \Pi^{\mu+t+1}$ où ε est une unité de $O_{N_{\mathfrak{P}}}$ et $1 \le \mu \le p-1$

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

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

démonstration :

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

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

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

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

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

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

$$x_\mu \equiv \Pi^\mu + f(\alpha)\frac{\mu.(\mu-1)}{2}\Pi^{\mu+t} \qquad (\Pi^{\mu+t+1})$$

démonstration :

Remarquons que $(p) = \left(\Pi^{pq}\right)$ 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 :

$$x_\mu = \prod_{i=0}^{\mu-1} (\Pi + \sigma^i(\Pi) - \Pi) \equiv \prod_{i=0}^{\mu-1} (\Pi + i\, f(\alpha)\, \Pi^{t+1}) \qquad (\Pi^{\mu+t+1})$$

$$\equiv \Pi^\mu + f(\alpha)\left(\sum_{i=0}^{\mu-1} i\right)\Pi^{\mu+t} \quad (\Pi^{\mu+t+1})$$

ce qui démontre la congruence

Démonstration de la proposition :

Nous pouvons écrire d'une part :

$$y_\mu = (\sigma-1)x_\mu = x_\mu \frac{(\sigma^\mu-1)\Pi}{\Pi} = x_\mu\,(\mu\, f(\alpha)\,\Pi^t + \epsilon_1\,\Pi^{t+1}) \text{ où } \epsilon_1 \in O_{N_\mathfrak{P}}.$$

$$= (\Pi^\mu + f(\alpha)\frac{\mu(\mu-1)}{2}\Pi^{\mu+t} + \epsilon_2\,\Pi^{\mu+t+1})(\mu\, f(\alpha)\,\Pi^t + \epsilon_1\,\Pi^{t+1})$$

$$= \mu\, f(\alpha)\,\Pi^{\mu+t} + \epsilon\,\Pi^{\mu+t+1}$$

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

la proposition 5 est donc démontrée.

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

$\frac{\operatorname{Ker} T_{\mathfrak{P}}}{(\sigma-1)O_{N_{\mathfrak{P}}}}$ est un $\mathbb{F}_p[g]$-module ; on peut le décomposer de la façon suivante : $\frac{\operatorname{Ker} T_{\mathfrak{P}}}{(\sigma-1)O_{N_{\mathfrak{P}}}} = V_o \oplus V$ où V_o est le sous-espace invariant par g . On aura $O \otimes_{\mathbb{Z}[g]} \frac{\operatorname{Ker} T_{\mathfrak{P}}}{(\sigma-1)O_{N_{\mathfrak{P}}}} \simeq V$.

Pour connaître cette décomposition , déterminons le caractère ψ de la représentation de g sur $\mathbb{F}_p$ fournie par $\frac{\operatorname{Ker} T_{\mathfrak{P}}}{(\sigma-1)O_{N_{\mathfrak{P}}}}$. Pour ce faire reprenons un raisonnement utilisé dans le deuxième cas .

On a une O_{k_p}-base de $\operatorname{Ker} T_{\mathfrak{P}}$ formée par les $\frac{y_\mu}{\pi^{(\mu)}}$ $(1 \le \mu \le p-1)$ et une O_{k_p}-base de $(\sigma-1)O_{N_{\mathfrak{P}}}$ formée par les y_μ $(1 \le \mu \le p-1)$. Un élément de O_{k_p} s'écrit $\sum_{n=0}^{\infty} f(\beta_n)\pi^n$, étant données les valeurs de (μ) , tout élément de $\frac{\operatorname{Ker} T_{\mathfrak{P}}}{(\sigma-1)O_{N_{\mathfrak{P}}}}$ 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 ψ associé à cette représentation de g , il suffit, si on écrit

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

(sauf si p=t=3 où l'on écrit $\tau^j(\frac{y_\mu}{\pi}) = \sum_{i=1}^{2} b^j_{\mu i} \frac{y_i}{\pi}$)

de déterminer $b^j_{\mu,\mu}$ et on a $\psi(\tau^j) = \sum_{\mu} b^j_{\mu,\mu}$. Mais on connaît $\tau^j(\pi^{(\mu)}) = \omega^{j(\mu)}\pi$ et on sait que l'on peut écrire $\tau^j(y_\mu) = \Sigma\, C^j_{\mu,i}\, y_i$ avec les coefficients $C^j_{\mu,i}$ dans O_{k_p} on peut également écrire d'après la proposition 5 $\tau^j(y_\mu) = f(\alpha)\ \mu\, \omega^{j(\mu+t)}\Pi^{\mu+t} + \varepsilon\Pi^{\mu+t+1}$. On sait que les valuations des y_i sont deux à deux distinctes modulo p et que les coefficients $C^j_{\mu,i}$ ont des valuations congrues à 0 modulo p . Le représentant $f(b^j_{\mu,\mu})$ est donc tel que $v\left(\tau^j\left(\frac{y_\mu}{\pi}\right) - f(b^j_{\mu,\mu})\frac{y_\mu}{\pi}\right) \neq v\left(\frac{y_\mu}{\pi}\right)$. En comparant les développements de y_μ et $\tau^j(y_\mu)$ donnés dans la proposition 5 , on voit que $b^j_{\mu,\mu}$ est la classe de $(\omega^{\mu-1+t})^j$. On trouve donc que $b^j_{\mu,\mu} = \bar{\omega}^{(\mu+t-1)j}$ où $\bar{\omega}$ est la classe de ω dans $\mathbb{Z}_{p/(p)} = \mathbb{F}_p$, ce qui nous donne :

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

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

soit en tenant compte de la congruence $p \equiv 1\ (q)$

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

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

$$\psi = \sum_{s=0}^{t-1} \psi_s \qquad \text{sauf si p=t=3 où } \Psi = \Psi_0 + \Psi_1$$

D'après ce qui a été dit plus haut , le caractère de g fourni par le $\mathbb{F}_p[g]$-module $V = O \otimes_{Z[g]} \frac{\text{Ker } T}{(\sigma-1)O_N}$ est $\sum_{\ell=1}^{t-1} \psi_\ell$ sauf si p=t=3 où il est égal à Ψ_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 $\frac{Z[\omega]}{p'_i}$. Définissons p'_1 comme

étant l'idéal premier de $\mathbb{Z}[\omega]$ au-dessus de p associé au caractère ψ_1 , ce qui revient à dire que $\psi_1(\tau)$ est l'image de ω dans $\frac{\mathbb{Z}[\omega]}{\mathfrak{p}'_1}$; soit ρ_ℓ le $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\omega)$ défini par $\rho_\ell(\omega) = \omega^\ell$ $(1 \le \ell \le q-1)$ on a $\psi_\ell(\tau) = \psi_1(\tau)^\ell$ c'est donc l'image de $\rho_\ell(\omega)$ dans $\frac{\mathbb{Z}[\omega]}{\mathfrak{p}'_1}$ c'est-à-dire l'image de ω dans $\frac{\mathbb{Z}[\omega]}{\rho_\ell^{-1}(\mathfrak{p}'_1)}$. Avec ces notations on peut donc énoncer :

Proposition 6 . Lorsque $N/\mathbb{Q}$ est totalement ramifiée en p , le $\mathbb{Z}[\omega]$- module

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

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

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

Comme $O = \frac{\mathbb{Z}[g]}{1+\tau+\ldots+\tau^{q-1}}$, le O-module $O \otimes_{\mathbb{Z}[g]} T_{N/k}(O_N)$ est isomorphe à $\frac{T_{N/k}(O_N)}{(1+\tau+\ldots+\tau^{q-1})\,T_{N/k}(O_N)}$ c'est-à-dire à $\frac{T_{N/k}(O_N)}{T_{N/\mathbb{Q}}(O_N)}$

Le $\mathbb{Z}[g]$-module $\frac{T_{N/k}(O_N)}{T_{N/k}(O_N) \cap \mathbb{Z}}$ est annulé par $1+\tau+\ldots+\tau^{q-1}$ c'est donc en fait un O-module , il est sans torsion , donc projectif . L'application canonique de $\frac{T_{N/k}(O_N)}{T_{N/\mathbb{Q}}(O_N)} \longrightarrow \frac{T_{N/k}(O_N)}{T_{N/k}(O_N) \cap \mathbb{Z}}$ est donc scindée . On en déduit :

Proposition 7 . Le O-module $\dfrac{T_{N/k}(O_N)}{T_{N/\mathbb{Q}}(O_N)}$ est O-isomorphe à la somme directe des O-modules $\dfrac{T_{N/k}(O_N)}{T_{N/k}(O_N)\cap\mathbb{Z}}$ et $\dfrac{T_{N/k}(O_N)\cap\mathbb{Z}}{T_{N/\mathbb{Q}}(O_N)}$, ce dernier étant son groupe de torsion .

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

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

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

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

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

où $\varepsilon = 0$ sauf lorsque q est ramifié dans $k/\mathbb{Q}$ auquel cas $\varepsilon = 1$.

Q est le produit des idéaux premiers de O_k au-dessus de q .

$\mathfrak{L}$ parcourt les idéaux premiers de O_k , premiers avec q .

$e_{\mathfrak{L}}$ est l'indice de ramification de $\mathfrak{L}$.

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

$$\mathfrak{U} = \begin{cases} q^{\varepsilon} & \text{si } t = 0 \\ pq^{\varepsilon} & \text{si } 1 \leq t < q \end{cases}$$

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

$T_{N/\mathbb{Q}}(O_N) = T_{k/\mathbb{Q}}(\mathfrak{p}O_k) = (q^{\varepsilon}P)$

Proposition 8 . Le O-module $\dfrac{T_{N/k}(O_N) \cap \mathbb{Z}}{T_{N/\mathbb{Q}}(O_N)}$ est isomorphe à $\dfrac{\mathbb{Z}[\omega]}{(1-\omega)^{\varepsilon}\mathbb{Z}[\omega]}$

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

Soit χ un caractère de degré 1 de $\mathfrak{g}$, non trivial , à valeurs dans $\mathbb{C}$. Soit θ_o un élément de k engendrant avec ses conjugués une base normale de $k/\mathbb{Q}$; on considère l'application g_{χ,θ_o} de k dans $\mathbb{Q}(\omega)$ définie par : $g_{\chi,\theta_o}(\theta) = \dfrac{\langle \theta, \chi \rangle}{\langle \theta_o, \chi \rangle}$

où $\langle \theta, \chi \rangle = \sum_{i=0}^{q-1} \tau^i(\theta)\chi(\tau^{-i})$ est la résolvante de Lagrange de θ et de χ (cf. [3]) . On sait que $\mathrm{Ker}(g_{\chi,\theta_o}) = \mathbb{Q}$ donc , si on restreint g_{χ,θ_o} à $T_{N/k}(O_N)$, on a $g_{\chi,\theta_o}(T_{N/k}(O_N)) \simeq \dfrac{T_{N/k}(O_N)}{T_{N/k}(O_N) \cap \mathbb{Z}}$.

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

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

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

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

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

pour tout $\sigma \in \mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$, on définit l'entier m_σ modulo f par $\sigma(\zeta_f) = \zeta_f^{m_\sigma}$, ζ_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 χ 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 $\tau(\chi) = \sum_{\substack{1 \le a \le f \\ (a,f)=1}} \chi(a)\, \zeta_f^a = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})} \sigma(\zeta_f)\, \chi(\sigma^{-1})$

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

On peut alors trouver un élément θ_o tel que $\langle \theta_o, \chi \rangle = \tau(\chi)$. Avec ce choix nous définissons g_χ par $g_\chi(\theta) = \dfrac{\langle \theta, \chi \rangle}{\tau(\chi)}$. Les propriétés classiques des résolvantes de Lagrange montrent que $\tau(\chi)^q \in \mathbb{Q}(\omega)$. Ecrivons $(\tau(\chi)^q) = \mathfrak{R}(\chi)^q \prod_{i=1}^{q-1} \rho_i^{-1}(\mathfrak{J})^i$ où $\mathfrak{J}$ est un produit d'idéaux premiers , décomposés dans $\mathbb{Q}(\omega)/\mathbb{Q}$, tel que $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\mathfrak{J})$ soit sans facteur carré , ρ_i a été défini au § 4 , 3$^{\text{eme}}$ 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 $\mathfrak{R}(\chi) = \mathbb{Z}[\omega]$ si $(f,q) = 1$ et $\mathfrak{R}(\chi) = q\mathbb{Z}[\omega]$ sinon . On peut également déterminer $g_\chi(O_k)$. On sait grâce aux propriétés des résol - vantes de Lagrange que l'on a la double inclusion

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

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_χ ici fait on obtient :

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

On en déduit :

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

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

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

Il nous reste à déterminer $\dfrac{T_{N/k}(O_N)}{T_{N/k}(O_N) \cap \mathbb{Z}}$ 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 $\mathfrak{p}$ l'idéal premier de O_k au-dessus de p , $\mathfrak{p}''_i$ les idéaux premiers de $O_{k(\omega)}$ au-dessus de $\mathfrak{p}$ et $\mathfrak{p}'_i = \mathfrak{p}''_i \cap \mathbb{Q}(\omega)$. Fixons $\mathfrak{p}''$, $\mathfrak{p}' = \mathfrak{p}'' \cap \mathbb{Q}(\omega)$, de sorte que $\mathfrak{p}'$ soit l'idéal au-dessus de p divisant $\mathfrak{J}$.

Soit t , tel que $1 \leq t < q$ et $x \in \mathfrak{p}^t$, on a $\langle x,\chi \rangle = \sum_{i=1}^{q-1} \tau^i(x)\,\chi(\tau^{-i})$ qui appartient à $\left(\prod_{i=1}^{q-1} \rho_i^{-1}(\mathfrak{p}'')\right)^t$ donc :

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

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

on en déduit :

$$(9) \qquad (\prod_i \rho_i^{-1}(\mathfrak{p}'))^t \supset (g_\chi(\mathfrak{p}^t)\,\mathfrak{R}(\chi))^q \prod_{i=1}^{q-1} \rho_i^{-1}(\mathfrak{I})^i$$

or $[O_k : \mathfrak{p}^t] = [g_\chi(O_k) : g_\chi(\mathfrak{p}^t)] \times [(\ker g_\chi(O_k) : (\ker g_\chi \mid \mathfrak{p}^t)]$

$$= [g_\chi(O_k) : g_\chi(\mathfrak{p}^t)] \times [\mathbb{Z} : p\mathbb{Z}]$$

ce qui donne

$$(10) \qquad p^{t-1} = [g_\chi(O_k) : g_\chi(\mathfrak{p}^t)] \quad .$$

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

$$(11) \qquad g_\chi(\mathfrak{p}^t) = g_\chi(O_k) \prod_{i=1}^{q-1} \rho_i^{-1}(\mathfrak{p}')^{c_i}$$

soit $$g_\chi(\mathfrak{p}^t) = \mathfrak{R}(\chi)^{-1}\, q^{\varepsilon} \prod_{i=1}^{q-1} \rho_i^{-1}(\mathfrak{p}')^{c_i}$$

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

Donc , d'après (9)

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

on obtient donc $\quad t \le i + qc_i \quad$ soit $\quad c_i \ge \left[\dfrac{t-i-1}{q}\right] + 1 \quad .$

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

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

d'où la proposition .

Proposition 10 . Avec les notations précédentes , le $\mathbb{Z}[\omega]$- module $\dfrac{T_{N/k}(O_N)}{T_{N/k}(O_N) \cap \mathbb{Z}}$ est isomorphe à $\prod_{i=1}^{q-1} \rho_i^{-1}(\mathfrak{p}')^{c_i}$ avec $c_i = \left[\dfrac{t-i-1}{q}\right] + 1$

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

Comparons l'idéal $\mathfrak{p}'_1$ de la proposition 6 et l'idéal $\mathfrak{p}'$ de la proposition 10 . Choisissons $\omega \in \mathbb{Z}_p$ une racine primitive q-ième de l'unité, fixons τ élément de $\mathrm{Gal}(k_{/\mathbb{Q}}) = \mathrm{Gal}(k_{\mathfrak{p}/p})$ et choisissons χ 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 $\mathfrak{p}''$ au-dessus de p telle que $v_{\mathfrak{p}''}(\tau(\chi)) = 1$. Localisons en $\mathfrak{p}''$. On a $k(\omega)_{\mathfrak{p}''} = k_p$ 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 π et montre que l'image de ω dans $\dfrac{O_{k(\omega)}}{\mathfrak{p}''} = \dfrac{\mathbb{Z}[\omega]}{\mathfrak{p}'}$ est la même que dans $\dfrac{O_{k_{\mathfrak{p}/p}}}{\mathfrak{p}} = \dfrac{\mathbb{Z}_p}{p}$. On a donc $\mathfrak{p}' = \mathfrak{p}'_1$. D'où en regroupant les différents résultats :

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

$$O \otimes_{\mathbb{Z}[g]} O_N \text{ isomorphe à } \begin{cases} 1^\circ\ \mathbb{Z}[\omega] \oplus \dfrac{\mathbb{Z}[\omega]}{(1-\omega)^\epsilon} & \text{si } e = 1 \text{ ou } e=q \\ \quad \text{(cas où p est modérément ramifié dans N/Q)} & \\ 2^\circ\ \dfrac{\mathbb{Z}[\omega]}{(p)} \oplus \dfrac{\mathbb{Z}[\omega]}{(1-\omega)^\epsilon} \oplus p\,\mathbb{Z}[\omega] & \text{si } e = p \\ 3^\circ\ \bigoplus_{i=1}^{t} \dfrac{\mathbb{Z}[\omega]}{\rho_i^{-1}(\mathfrak{p}')} \oplus \dfrac{\mathbb{Z}[\omega]}{(1-\omega)^\epsilon} \oplus \prod_{i=1}^{t-1} \rho_i^{-1}(\mathfrak{p}') & \text{si } e = pq \text{ en} \end{cases}$$

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

On en déduit immédiatement le théorème :

héorème 3 . Lorsque $N_{/\mathbb{Q}}$ est une extension non abélienne de degré pq (p et q premiers q | p-1) du corps des rationnels , l'image de $O \otimes_{\mathbb{Z}[G]} O_N$ dans le groupe de Grothendieck des 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-ex - tensions dans Compositio math.) .

[4] J. COUGNARD : Un contre exemple à une conjecture de J. Martinet . Proc. Durham Symposium 1975 .

[5] A. FROHLICH : 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°149 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