Théorie des Nombres

Besançon

Année 1977-1978

GROUPES DE TORSION ASSOCIES A DES EXTENSIONS QUATERNIONIENNES DE DEGRE 8 DU CORPS DES NOMBRES RATIONNELS

Jean COUGNARD

Laboratoire de Mathématiques

Faculté des Sciences de Besançon

Route de Gray - "La Bouloie"

25030 BESANCON CEDEX

GROUPES DE TORSION ASSOCIES A DES EXTENSIONS QUATERNIONIENNES DE DEGRE 8 DU CORPS DES NOMBRES RATIONNELS

par Jean COUGNARD *

§1. PRELIMINAIRES :

Soit $N/\mathbb{Q}$ une extension galoisienne dont le groupe de Galois G est isomorphe au groupe des quaternions d'ordre 8. Dans tout ce qui suit on suppose que l'extension n'est pas modérément ramifiée.

I. 1. On note σ et τ deux générateurs de G liés par les relations $\sigma^4 = 1$, $\tau^2 = \sigma^2$, $\tau\sigma\tau^{-1} = \sigma^{-1}$; H désigne le sous-groupe de G engendré par σ et $G' = (1, \sigma^2)$ est le centre de G. Soit $\mathbb{Z}'$ (resp $\mathbb{Z}''$) l'anneau quotient de $\mathbb{Z}[G]$ par l'idéal bilatère $(1-\sigma^2)$ (resp $1+\sigma^2$). On identifie $\mathbb{Z}'$ à $\mathbb{Z}[g]$ où g désigne le groupe abélien engendré par deux éléments s et t d'ordre 2 en envoyant σ sur s et τ sur t, et $\mathbb{Z}''$ à l'ordre de base 1, i, j, k du corps des quaternions $\mathbb{H}$ sur $\mathbb{Q}$ où $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$ en envoyant σ sur i et τ sur j.

I. 2. Soient K le sous-corps biquadratique de N, k_i $(1 \leq i \leq 3)$ ses trois sous-corps quadratiques, k_1 étant invariant par H. On suppose σ choisi de façon que

a) Si $K/\mathbb{Q}$ n'est pas totalement ramifiée en 2 alors $k_1/\mathbb{Q}$ n'est pas ramifiée en 2.

b) Si $K/\mathbb{Q}$ est totalement ramifiée en 2, le saut de ramification de $k_1/\mathbb{Q}$ est 1, ceux de k_2 et k_3 étant égaux à 2.

I. 3. Pour tout corps de nombres L, on note Z_L la clôture intégrale de $\mathbb{Z}$ dans L.

I. 4. L'ordre $\mathfrak{S}(N/\mathbb{Q})$ associé à Z_N contient les idempotents $\frac{1+\sigma^2}{2}$ et $\frac{1-\sigma^2}{2}$. On en déduit que Z_N est somme directe de ses deux sous-$\mathbb{Z}[G]$-modules $\mathbb{Z}'_N$ et $\mathbb{Z}''_N$ égaux respectivement à $\frac{1+\sigma^2}{2} Z_N$ et $\frac{1-\sigma^2}{2} Z_N$ et que $\mathfrak{S}(N/\mathbb{Q})$ s'identifie au produit $\mathfrak{S}' \times \mathfrak{S}''$ où $\mathfrak{S}'$ est l'ordre associé à Z_K car $\mathbb{Z}'_N \simeq Z_K$ et $\mathfrak{S}''$ est l'ordre associé à $\mathbb{Z}''_N$ considéré comme module sur $\mathbb{Z}''$. On a le théorème suivant ([3]) :

* ERA - CNRS - 070654

THEOREME :

a) L'ordre associé à l'extension $N_{/\mathbb{Q}}$ est canoniquement isomorphe au produit $\mathfrak{S}' \times \mathbb{Z}''$ où l'ordre $\mathfrak{S}'$ est ainsi défini :

i) si $k_{/\mathbb{Q}}$ est non ramifiée en 2 $\quad \mathfrak{S}' \simeq \mathbb{Z}[g]$

ii) si $k_{/\mathbb{Q}}$ est ramifiée en 2 et $k_{1/\mathbb{Q}}$ ne l'est pas $\mathfrak{S}'$ est l'ordre de base sur $\mathbb{Z}$:

$$1,\ t,\ \frac{1+s}{2},\ \frac{st+t}{2}$$

iii) si $k_{/\mathbb{Q}}$ est totalement ramifiée en 2, $\mathfrak{S}'$ est l'ordre de base sur $\mathbb{Z}$:

$$1,\ t,\ \frac{1+s}{2},\ \frac{1+s+t+st}{4}$$

b) l'anneau $\mathbb{Z}_N$ des entiers de N est libre sur son ordre associé

Remarque : une erreur s'est glissée dans ([3]) pour le cas (iii).

I. 5. Les idempotents irréductibles de $\mathbb{Q}[G]$ sont les éléments :

$$e_o = \frac{(1+\sigma+\sigma^2+\sigma^3)(1+\tau)}{8}$$ $e_o\,\mathbb{Q}[G] \simeq \mathbb{Q}$ est le facteur simple associé au caractère trivial de G.

$$e_1 = \frac{(1+\sigma+\sigma^2+\sigma^3)(1-\tau)}{8}$$ $e_1\,\mathbb{Q}[G] \simeq \mathbb{Q}$ est le facteur simple associé au caractère de degré 1 dont le noyau est engendré par σ

$$e_2 = \frac{(1-\sigma+\sigma^2-\sigma^3)(1-\tau)}{8}$$ $e_2\,\mathbb{Q}[G] \simeq \mathbb{Q}$ est le facteur simple associé au caractère de degré 1 dont le noyau est engendré par $\sigma\tau$

$$e_3 = \frac{(1-\sigma+\sigma^2-\sigma^3)(1+\tau)}{8}$$ $e_3\,\mathbb{Q}[G] \simeq \mathbb{Q}$ est le facteur simple associé au caractère de degré 1 dont le noyau est engendré par τ

$$\nu = \frac{1-\sigma^2}{2}$$ $\nu\,\mathbb{Q}[G] \simeq \mathbb{H}$ est le facteur simple associé au caractère irréductible de degré 2 deG.

L'ordre maximal de $\mathbb{Q}[G]$ est unique, il est engendré par $\mathbb{Z}[G]$ et les éléments $e_o, e_1, e_2, e_3, \frac{1+\sigma+\tau+\sigma\tau}{4}(1-\sigma^2)$

§2. DEBUT DES CALCULS :

Soit $\mathfrak{M}$ l'ordre maximal de $\mathbb{Q}[G]$, on note $\mathfrak{M}_i = e_i\mathfrak{M} (0 \le i \le 3)$, $\mathfrak{M}' = (1-\nu)\mathfrak{M}$ $\mathfrak{M}'' = \nu\mathfrak{M}$.

Le $\mathfrak{M}$ module $\mathfrak{M} \underset{\mathbb{Z}[G]}{\otimes} \mathbb{Z}_N$ est isomorphe à $\mathfrak{M}\mathbb{Z}_N \oplus T$ où T est fini et $\mathfrak{M}\mathbb{Z}_N$ est $\mathfrak{M}$ libre ; cette décomposition a lieu quelle que soit la ramification de 2 dans $N_{/\mathbb{Q}}$; toutefois $T = (0)$ si 2 n'est pas ramifié dans $N_{/\mathbb{Q}}$. On se propose de déterminer T dans les

cas (i), (ii), (iii) du théorème ci-dessus.

On a la décomposition suivante de $\mathfrak{M} \underset{\mathbb{Z}[G]}{\otimes} Z_N$:

$\mathfrak{M} \underset{\mathbb{Z}[G]}{\otimes} Z_N \simeq (\mathfrak{M}' \oplus \mathfrak{M}'') \underset{\mathbb{Z}[G]}{\otimes} (Z_K \oplus Z''_N)$ ceci nous donne une décomposition de T en quatre facteurs qui sont les groupes de torsion de

$$\mathfrak{M}' \underset{\mathbb{Z}[G]}{\otimes} Z_K \,,\ \mathfrak{M}' \underset{\mathbb{Z}[G]}{\otimes} Z''_N \,,\ \mathfrak{M}'' \underset{\mathbb{Z}[G]}{\otimes} Z''_N \,,\ \mathfrak{M}'' \underset{\mathbb{Z}[G]}{\otimes} Z_K .$$

1) Le premier produit tensoriel se ramène au cas abélien : en effet $\mathfrak{M}'$ et Z_K sont annulés par $1-\sigma^2$, on obtient donc :

$\mathfrak{M}' \underset{\mathbb{Z}[G]}{\otimes} Z_K \simeq \mathfrak{M}' \underset{\mathbb{Z}[g]}{\otimes} Z_K \simeq \mathfrak{M}' \underset{\mathbb{Z}[g]}{\otimes} \mathfrak{S}'$, le dernier isomorphisme se déduisant du Hauptsatz de (2). Le calcul de ce produit tensoriel a été éffectué dans (3). On obtient ici :

cas (i) $\quad \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$

cas (ii) $\quad (\mathbb{Z} \times \mathbb{Z}_{/2\mathbb{Z}}) \times (\mathbb{Z} \times \mathbb{Z}_{/2\mathbb{Z}}) \times (\mathbb{Z} \times \mathbb{Z}_{/2\mathbb{Z}}) \times (\mathbb{Z} \times \mathbb{Z}_{/2\mathbb{Z}})$

Chacun des facteurs entre parenthèse étant isomorphe à un des $\mathfrak{M}_i \underset{\mathbb{Z}[g]}{\otimes} \mathfrak{S}'$.

cas (iii) $\quad (\mathbb{Z} \times \mathbb{Z}_{/2\mathbb{Z}} \times \mathbb{Z}_{/2\mathbb{Z}}) \times (\mathbb{Z} \times \mathbb{Z}_{/2\mathbb{Z}} \times \mathbb{Z}_{/2\mathbb{Z}}) \times (\mathbb{Z} \times \mathbb{Z}_{/2\mathbb{Z}} \times \mathbb{Z}_{/2\mathbb{Z}}) \times \ldots$

$\ldots (\mathbb{Z} \times \mathbb{Z}_{/2\mathbb{Z}} \times \mathbb{Z}_{/2\mathbb{Z}})$

Avec la même signification pour les parenthèses que dans le cas (ii)

2) Regardons maintenant $\mathfrak{M}' \underset{\mathbb{Z}[G]}{\otimes} Z''_N \simeq \mathfrak{M}' \underset{\mathbb{Z}[G]}{\otimes} \mathbb{Z}'' \simeq \mathfrak{M}' \underset{\mathbb{Z}[G]}{\otimes} \frac{\mathbb{Z}[G]}{1+\sigma^2}$ ce qui donne

$$\frac{\mathfrak{M}'}{(1+\sigma^2)\mathfrak{M}'} \simeq \frac{\mathfrak{M}'}{2\mathfrak{M}'} \simeq (\mathbb{Z}_{/2\mathbb{Z}})^4$$

3) Le troisième facteur se calcule tout aussi aisément :

$$\mathfrak{M}'' \underset{\mathbb{Z}[G]}{\otimes} \mathbb{Z}''_N \simeq \mathfrak{M}'' \underset{\mathbb{Z}[G]}{\otimes} \frac{\mathbb{Z}[G]}{(1+\sigma^2)} \simeq \frac{\mathfrak{M}''}{(1+\sigma^2)\mathfrak{M}''} \simeq \mathfrak{M}''$$

Il reste un terme à calculer, ce sera l'objet du paragraphe suivant.

§3. CALCUL DE $\mathfrak{M}'' \underset{\mathbb{Z}[G]}{\otimes} \mathfrak{S}'$

Nous allons effectuer ce calcul en séparant les cas (i), (ii), (iii).

Cas (i) :

On a $\mathcal{O}' \simeq \mathbb{Z}[g] \simeq \dfrac{\mathbb{Z}[g]}{(1-\sigma^2)}$ ce qui donne $\mathfrak{M}'' \underset{\mathbb{Z}[g]}{\otimes} \mathcal{O}' \simeq \dfrac{\mathfrak{M}''}{1-\sigma^2} \simeq \dfrac{\mathfrak{M}''}{2}$

Cas (ii)

On a $\mathcal{O}' \simeq \dfrac{(\mathbb{Z}[G], e_o, e_1)}{(1-\sigma^2)}$ et donc $\mathfrak{M}'' \underset{\mathbb{Z}[G]}{\otimes} \mathcal{O}' \simeq \mathfrak{M}'' \underset{\mathbb{Z}[G]}{\otimes} \dfrac{\mathbb{Z}[G]}{1-\sigma^2} \underset{\frac{\mathbb{Z}[G]}{1-\sigma^2}}{\otimes} \mathcal{O}'$

$$\simeq \frac{\mathfrak{M}''}{(1-\sigma^2)\mathfrak{M}''} \underset{\mathbb{Z}[g]}{\otimes} \mathcal{O}' \simeq \frac{\mathfrak{M}''}{2\mathfrak{M}''} \underset{\mathbb{Z}[g]}{\otimes} \mathcal{O}' \simeq \frac{\mathfrak{M}''}{2\mathfrak{M}''} \underset{\mathbb{F}_2[g]}{\otimes} \mathcal{O}'/2\mathcal{O}'$$

or $\dfrac{\mathfrak{M}''}{2\mathfrak{M}''}$ est engendré, comme $\mathbb{F}_2$ - espace vectoriel, par les classes $\bar{1}, \bar{i}, \bar{j}, \overline{\dfrac{1+i+j+k}{2}} = \theta$

On a les relations : $\theta^2 + \theta + 1 = 0$, $\theta\bar{i} + \theta + \bar{1} + \overline{ij} = 0$,

$$\theta j + \theta + \bar{1} + \bar{i} = 0 \ , \quad \theta k + \theta + \bar{1} + \bar{j} = 0$$

Pour $m \in \dfrac{\mathfrak{M}''}{2\mathfrak{M}''}$ l'action de $\mathbb{F}_2[g]$ est donnée par $m.s = m.\bar{i}$, $m.t = m.\bar{j}$. Par ailleurs $\mathcal{O}'$ admet une base sur $\mathbb{Z}$ formée des éléments $1, t, \dfrac{1+s}{2}, \dfrac{s+st}{2}$ donc $\dfrac{\mathcal{O}'}{2\mathcal{O}'}$ admet pour base sur $\mathbb{F}_2$: $\bar{1}, \bar{t}, \alpha, \beta$ où α (resp β) est la classe de $\dfrac{1+s}{2}$ (resp $\dfrac{st+t}{2}$).

On remarque que 1 et s (resp t et st) ont même image dans $\mathcal{O}/2\mathcal{O}'$. On en déduit que s opère trivialement sur $\mathcal{O}'/2\mathcal{O}'$ et que $\mathcal{O}'/2\mathcal{O}$ est somme directe de deux $\mathbb{F}_2[g]$ modules, l'un V_1 ayant pour base $\underline{1}, \underline{t}$ sur $\mathbb{F}_2$, l'autre V_2 ayant pour base α et β. Le produit tensoriel est donc isomorphe à la somme directe $\dfrac{\mathfrak{M}''}{2\mathfrak{M}''} \underset{\mathbb{F}_2[g]}{\otimes} (V_1 \oplus V_2)$ or V_1 et V_2 sont tous les deux isomorphes à $\dfrac{\mathbb{F}_2[g]}{(1+s)}$.

On est donc ramené à la somme directe de deux modules isomorphes à $\dfrac{\dfrac{\mathfrak{M}''}{2}}{\dfrac{\mathfrak{M}''}{2}(1+s)}$.

Mais on a $\underline{1}(1+s) = \underline{i}(1+s) = j(1+s) = \underline{1+i}$ et $\theta(1+s) = \theta + \theta\underline{i} = \underline{1+ij} = \underline{i+j}$. Comme les éléments $\underline{1}, \underline{1+i}, \underline{i+j}, \theta$ forment une base de $\dfrac{\mathfrak{M}''}{2\mathfrak{M}''}$, le quotient est un $\mathbb{F}_2$ espace vectoriel ayant pour base les classes de $\underline{1}$ et θ. Or tout $\mathfrak{M}''$ module ayant quatre éléments est isomorphe au quotient de $\mathfrak{M}''$ par l'unique idéal premier $\mathfrak{p}$ au-dessus de 2 dans $\mathfrak{M}''$.

De ceci il résulte que $\mathfrak{M}'' \underset{\mathbb{Z}[G]}{\otimes} \mathcal{O}' \simeq \dfrac{\mathfrak{M}''}{\mathfrak{p}} \times \dfrac{\mathfrak{M}''}{\mathfrak{p}}$

Cas (iii) :

$\mathfrak{S}'$ est le sous-anneau de $\mathbb{Q}[g]$ engendré par $\mathbb{Z}[g]$, $\frac{1+s}{2}$, $\frac{1+s+t+st}{4}$ il est donc isomorphe à $\frac{(\mathbb{Z}[G], e_0, e_0+e_1)}{(1-\sigma^2)}$. Dans ces conditions :

$$\mathfrak{M}'' \underset{\mathbb{Z}[G]}{\otimes} \mathfrak{S}' \simeq \mathfrak{M}'' \underset{\mathbb{Z}[G]}{\otimes} \frac{\mathbb{Z}[G]}{1-\sigma^2} \underset{\frac{\mathbb{Z}[G]}{1-\sigma^2}}{\otimes} \mathfrak{S}' \simeq \frac{\mathfrak{M}''}{2\mathfrak{M}''} \underset{\mathbf{F}_2[g]}{\otimes} \mathfrak{S}'/2\mathfrak{S}'.$$

L'ordre $\mathfrak{S}'$ ayant pour base sur $\mathbb{Z}$: $1, t, \frac{1+s}{2}, \frac{1+s+t+st}{4}$, son quotient $\mathfrak{S}'/2\mathfrak{S}'$ a pour base $\underline{1}, \underline{t}, \alpha, \beta$ où α (resp β) est la classe de $\frac{1+s}{2}$ (resp $\frac{1+s+t+st}{4}$).

On a alors $\underline{1} = \underline{s}$ et donc s opère trivialement sur $\mathfrak{S}'/2\mathfrak{S}'$. De plus la classe de $\frac{1+s}{2} + \frac{t+st}{2}$ est égale à deux fois celle de β donc est nulle.

On en déduit que $\frac{\mathfrak{S}'}{2\mathfrak{S}'}$ est somme directe de trois $\mathbf{F}_2[g]$ modules l'un V_1 de base $\underline{1}, \underline{t}$ isomorphe à $\frac{\mathbf{F}_2[g]}{1+a}$ les deux autres étant isomorphes à $\mathbf{F}_2$, g y opérant trivialement. On est ramené à :

$$\mathfrak{M}'' \underset{\mathbb{Z}[G]}{\otimes} \mathfrak{S}' \simeq \frac{\frac{\mathfrak{M}''}{2\mathfrak{M}''}}{\frac{\mathfrak{M}''}{2\mathfrak{M}''}(1+s)} \oplus \left(\frac{\mathfrak{M}''}{2\mathfrak{M}''} \underset{\mathbf{F}_2[g]}{\otimes} \mathbf{F}_2\right) \oplus \left(\frac{\mathfrak{M}''}{2\mathfrak{M}''} \underset{\mathbf{F}_2[g]}{\otimes} \mathbf{F}_2\right)$$

Le premier terme a déjà été determiné, il est isomorphe à $\frac{\mathfrak{M}''}{\mathfrak{p}}$, les deux autres sont isomorphes à $\frac{\frac{\mathfrak{M}''}{2\mathfrak{M}''}}{\frac{\mathfrak{M}''}{2\mathfrak{M}''}(1+s) + \frac{\mathfrak{M}''}{2\mathfrak{M}''}(1+t)}$

Or $\underline{1}(1+t) = \underline{1}+\underline{j}$, $\underline{i}(1+t) = \underline{i}+\underline{ij} = \underline{1}+\underline{i}$, $\underline{j}(1+t) = \underline{1}+\underline{j}$

$\theta(1+t) = \theta+\theta\underline{j} = \underline{1}+\underline{i}$

Le quotient admet encore pour base sur $\mathbf{F}_2$ les classes de 1 et θ. On aura avec le même raisonnement que précedemment :

$$\mathfrak{M}'' \underset{\mathbb{Z}[G]}{\otimes} \mathfrak{S}' \simeq \frac{\mathfrak{M}''}{\mathfrak{p}} \times \frac{\mathfrak{M}''}{\mathfrak{p}} \times \frac{\mathfrak{M}''}{\mathfrak{p}}.$$

En résumé nous avons :

Théorème Le produit tensoriel $\mathfrak{M} \underset{\mathbb{Z}[G]}{\otimes} \mathbb{Z}_N$ est isomorphe à $\mathfrak{M} \oplus T$ où $T = (\bigoplus_{i=0}^{3} T_i) \oplus T''$ avec T_i (resp T'') groupe de torsion de $\mathfrak{M}_i \underset{\mathbb{Z}[G]}{\otimes} \mathbb{Z}''_N$ (resp $\mathfrak{M}'' \underset{\mathbb{Z}[G]}{\otimes} \mathbb{Z}''_N$) et valant dans :

- le cas (i) $T_i = \mathbb{Z}/2\mathbb{Z}$, $T'' = \frac{\mathfrak{M}''}{2\mathfrak{M}''}$

- le cas (ii) $T_i = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\frac{\mathfrak{M}''}{\mathfrak{p}} \times \frac{\mathfrak{M}''}{\mathfrak{p}} = T''$

- le cas (iii) $T_i = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $T'' = \frac{\mathfrak{M}''}{\mathfrak{p}} \times \frac{\mathfrak{M}''}{\mathfrak{p}} \times \frac{\mathfrak{M}''}{\mathfrak{p}}$

où $\mathfrak{p}$ est l'unique idéal premier au-dessus de (2) dans $\mathfrak{M}''$.

[1] D. CHATELAIN : Etude du O-module $O \underset{\mathbb{Z}[G]}{\otimes}$ où N est une extension abélienne de $\mathbb{Q}$ et O l'ordre maximal de $\mathbb{Q}[G]$.
Séminaire de Théorie des nombres - Besançon - 1976-77.

[2] H. W. LEOPOLDT : Uber die Hauptordnung der ganzen elementen eines abelschen Zahlkörpern.
J. für reine Ang. Math. (1959).

[3] J. MARTINET : Sur les extensions à groupe de Galois quaternionien.
Note aux C. R. A. S. t. 274 Série A p. 933-935 (20 mars 1972).

Jean COUGNARD
Laboratoire de Mathématiques
Faculté des Sciences de Besançon
Route de Gray - "La Bouloie"
25030 BESANCON CEDEX