ANNALES DE L'INSTITUT FOURIER

NICOLE MOSER

# Sur les unités d'une extension galoisienne non abélienne de degré *pq* du corps des rationnels *p* et *q* nombres premiers impairs

*Annales de l'institut Fourier*, tome 29, nº 1 (1979), p. 137-158

<http://www.numdam.org/item?id=AIF_1979__29_1_137_0>

Ann. Inst. Fourier, Grenoble
29, 1 (1979), 137-158

# SUR LES UNITÉS D'UNE EXTENSION GALOISIENNE NON ABÉLIENNE DE DEGRÉ *pq* DU CORPS DES RATIONNELS, *p* ET *q* NOMBRES PREMIERS IMPAIRS

par Nicole MOSER

*Dédié à Monsieur Claude Chabauty.*

Le but de cet article est l'étude de la structure, en tant que module sur l'algèbre du groupe de Galois, du groupe des unités $U_K$ d'une extension galoisienne $K/\mathbf{Q}$ non abélienne de degré $pq$. La connaissance de cette structure est en effet précieuse pour déterminer de nombreuses propriétés arithmétiques de K : les indices des groupes de normes d'unités sur les corps intermédiaires, la participation de $p$ au nombre de classes d'idéaux de K, des conditions nécessaires d'existence d'une unité de Minkowski...

Le premier paragraphe sert à dresser une liste de $\mathbf{Z}[G]$-modules de référence, pour G groupe non abélien d'ordre $pq$. Les résultats figurent déjà dans un article de Lena Chang Pu [10] ; mais on reprend une partie des démonstrations d'un point de vue cohomologique, afin de poursuivre plus aisément les calculs.

On étudie ensuite différents invariants arithmétiques qui permettent d'obtenir les propriétés annoncées. Dans le cas particulier où les corps cyclotomiques $\mathbf{Q}^{(p)}$ et $\mathbf{Q}^{(q)}$ sont principaux, et où $q^2$ ne divise pas $p-1$, ces invariants caractérisent les différentes structures de $\mathbf{Z}[G]$-module considérées. De plus, en interprétant les groupes de cohomologie relatifs à $U_K$ comme le fait K. Iwasawa (cf. [7]), en termes d'idéaux ou de classes d'idéaux de K, on obtient quelques renseignements sur les homomorphismes d'extension des idéaux, et sur les idéaux premiers ramifiés. Enfin, on donne une illustration numérique, grâce à la théorie du corps de classes.

## NOTATIONS

Pour tout corps de nombres totalement réel $\Lambda$, nous notons $U_\Lambda$ le groupe des unités, et $E_\Lambda$ le quotient $U_\Lambda/\{\pm 1\}$. Si $\Lambda'$ est une sous-extension de $\Lambda/\mathbf{Q}$, l'application norme $N_{\Lambda/\Lambda'} : U_\Lambda \longrightarrow U_{\Lambda'}$ définit par passage aux quotients une application de $E_\Lambda$ dans $E_{\Lambda'}$, notée encore $N_{\Lambda/\Lambda'}$.

Le lettre G désigne un groupe métacyclique d'ordre $pq$, ($p$ et $q$ sont deux nombres premiers impairs tels que $q$ divise $p-1$), engendré par deux éléments $\sigma$ et $\tau$ liés par les relations :

$$\sigma^p = \tau^q = 1$$

$$\tau\sigma = \sigma^r\tau ,$$

où $r$ est une racine primitive $q$-ième de l'unité modulo $p$. Nous réservons la lettre K pour désigner une extension galoisienne de $\mathbf{Q}$, de groupe G ; nous notons $k$ le sous-corps de K fixe par H, groupe cyclique engendré par $\sigma$, et L le sous-corps qui correspond à $g$, sous-groupe de G engendré par $\tau$.

Enfin, les lettres $p$ et $q$ ayant la signification donnée ci-dessus, nous notons :

$\zeta$ une racine primitive $p$-ième de l'unité ;

$\mathbf{Q}^{(p)}$ le $p$-ième corps cyclotomique ;

$A = \mathbf{Z}[\zeta]$ et $\mathfrak{P} = (1-\zeta)A$ ;

$\psi$ l'élément d'ordre $q$ du groupe cyclique $\mathrm{Gal}(\mathbf{Q}^{(p)}/\mathbf{Q})$, défini par $\zeta \longmapsto \zeta^r$ ;

$\mathbf{Q}_1$ le sous-corps de $\mathbf{Q}^{(p)}$ fixe par $\psi$ ;

$A_1 = \mathbf{Q}_1 \cap A$ et $\mathfrak{P}_1 = A_1 \cap \mathfrak{P}$ ;

$h_1$ le nombre de classes d'idéaux de $A_1$ ;

$\theta$ une racine primitive $q$-ième de l'unité ;

$B = \mathbf{Z}[\theta]$ ;

$h_q$ le nombre de classes d'idéaux de B.

De plus, $\varphi$ désigne la fonction d'Euler.

# 1. STRUCTURE DE G-MODULE DE $E_K$

Si, pour tout sous-groupe $\Delta$ de $G$, on note $\chi_\Delta^*$ le caractère de G induit par le caractère unité $\chi_\Delta$ de $\Delta$, on sait que le groupe $E_K$ est un G-module de caractère $\chi_{\{1\}}^* - \chi_G$. Dans ce paragraphe, on construit une liste de G-modules telle que tout module de caractère $\chi_{\{1\}}^* - \chi_G$ soit isomorphe à un des termes de la liste au moins.

Soit R un G-module de caractère $\chi_{\{1\}}^* - \chi_G$, sans **Z**-torsion ; la méthode utilisée pour étudier sa structure est due à I. Reiner : elle consiste à considérer R comme une extension d'un $\mathbf{Z}[g]$-module $R_0$ par un module $\widetilde{R}$ annulé par $(1 + \sigma + \ldots + \sigma^{p-1})$.

## 1.1. Définition et structure de $\widetilde{R}$.

Supposons R noté additivement, et posons

$$\widetilde{R} = \{x \in R \mid (1 + \sigma + \ldots + \sigma^{p-1})x = 0\}.$$

Puisque R est de caractère $\chi_{\{1\}}^* - \chi_G$, le **Z**-rang de $\widetilde{R}$ est égal à $(p-1)q$. Ainsi, $\widetilde{R}$ est un $\mathbf{Z}[G]/(1 + \sigma + \ldots + \sigma^{p-1})\mathbf{Z}[G]$-module, sans **Z**-torsion, de **Z**-rang $(p-1)q$ : sa structure est connue grâce aux travaux de M. Rosen ([15]), et l'on peut énoncer :

Proposition 1.1. — $\widetilde{R}$ *est* $\mathbf{Z}[G]$-*isomorphe à la somme directe de* $q$ *idéaux invariants de* $A/A_1$ : $\widetilde{R} \simeq \bigoplus_{i=1}^{q} \mathfrak{P}^{e_i}\mathfrak{a}_i$, *les* $\mathfrak{a}_i$ *appartenant à un système de représentants des classes de* $A_1$, *et les* $e_i$ *étant compris entre* 0 *et* $q-1$. *De plus,* $\widetilde{R}$ *est défini, à isomorphisme près, par les* $e_i$ *et la classe de* $\prod_{i=1}^{q} \mathfrak{a}_i$.

Rappelons que $\sigma$ agit sur chaque $\mathfrak{P}^{e_i}\mathfrak{a}_i$ par multiplication par $\zeta$, et que $\tau$ opère comme l'application $\psi$.

## 1.2. Définition et structure de $R_0$.

Notons $R_0$ le quotient $R/\widetilde{R}$ ; c'est un module de **Z**-rang $(q-1)$, et par définition de $\widetilde{R}$, il est invariant par $\sigma$. Sa structure en tant que $\mathbf{Z}[G]$-module est entièrement définie par sa structure en tant que $\mathbf{Z}[g]$-module. D'après les hypothèses sur le caractère de R, aucun élément non trivial de $R_0$ n'est fixe par $\tau$. On utilise alors les résultats de I. Reiner ([14]) sur les représentations entières d'un groupe cyclique d'ordre premier. Pour le module $R_0$, il n'y a qu'une possibilité :

PROPOSITION 1.2. – $R_0$ *est* $\mathbf{Z}[G]$*-isomorphe à un idéal* $\mathfrak{b}$ *de* B. *Sur cet idéal,* $\sigma$ *opère trivialement, tandis que* $\tau$ *agit par multiplication par* $\theta$.

## 1.3. Extensions de $R_0$ par $\widetilde{R}$.

On démontre (voir par exemple [16]) que l'existence d'extensions indécomposables de $R_0$ par $\widetilde{R}$ équivaut à l'existence d'éléments non nuls dans $H^1(G, \mathrm{Hom}_{\mathbf{Z}}(R_0, \widetilde{R}))$, et que les groupes $H^1(G, \mathrm{Hom}_{\mathbf{Z}}(\mathfrak{b}, \mathfrak{P}^e \mathfrak{a}))$ et $H^1(G, \mathrm{Hom}_S(S[\theta], (1-\zeta)^e S))$ sont isomorphes ; (S désigne l'intersection des localisés $\mathbf{Z}_{(p)}$ et $\mathbf{Z}_{(q)}$).

PROPOSITION 1.3. – *Le groupe* $H^1(G, \mathrm{Hom}_S(S[\theta], (1-\zeta)^e S))$ *est trivial si* $e = 1$ ; *sinon il est isomorphe à* $\mathbf{Z}/p\mathbf{Z}$.

*Démonstration.* – Le module $S[\theta]$ est S-libre, de base $\{1, \theta, \ldots, \theta^{q-2}\}$, donc $\mathrm{Hom}_S(S[\theta], (1-\zeta)^e S)$ est isomorphe, en tant que S-module, à $((1-\zeta)^e S)^{q-1}$. Posons $M = ((1-\zeta)^e S)^{q-1}$, et munissons M de la structure de G-module induite par celle de $\mathrm{Hom}_S(S[\theta], (1-\zeta)^e S)$ : $\sigma$ opère sur M par multiplication par $\zeta$, et pour tout $(a_0, a_1, \ldots, a_{q-2})$ de M,

$$\tau(a_0, a_1, \ldots, a_{q-2}) = \Big(-\sum_{i=0}^{q-2} \psi(a_i), \psi(a_0), \ldots, \psi(a_{q-3})\Big).$$

Comme le sous-module de M fixe par $\sigma$ est trivial, l'application restriction est un isomorphisme entre les groupes $H^1(G, M)$ et $H^1(H, M)^{G/H}$. Considérons donc un élément $c$ de $Z^1(H, M)$ ; il est défini par l'image $u \in M$ qu'il donne de $\sigma$, et le transformé de $c$ par $\tau$ associe à l'élément $\sigma$ l'élément $\tau^{-1}[(1 + \zeta + \ldots + \zeta^{r-1})u]$. La condition "$c$ représente une classe fixe par $\tau$" s'exprime par l'existence d'un élément $v \in M$ tel que :

$$\tau^{-1}[(1+\zeta+\ldots+\zeta^{r-1})u]-u=(1-\zeta)v.$$

Si $u=(u_0, u_1, \ldots, u_{q-2})$, chaque $u_i$ s'écrit $(\zeta-1)^e x_i$, $x_i \in \mathrm{S}[\zeta]$. Notons $\overline{x_i}$ la classe de $x_i$ modulo $(\zeta-1)\mathrm{S}[\zeta]$. On obtient le système dans $\mathrm{S}[\zeta]/(\zeta-1)\mathrm{S}[\zeta]$ :

$$\begin{cases} r\overline{x}_0 + r^e \sum_{i=0}^{q-2} \overline{x}_i = 0 \\ r\overline{x}_1 - r^e \overline{x}_0 = 0 \\ \vdots \\ r\overline{x}_{q-2} - r^e \overline{x}_{q-3} = 0. \end{cases}$$

Comme $r$ est inversible modulo $p$, les $q-2$ dernières équations du système donnent, pour $1 \leqslant i \leqslant q-2$ : $\overline{x}_i = r^{i(e-1)}\overline{x}_0$. En reportant ces valeurs dans la première équation, on obtient :

$$\overline{x}_0\left(\sum_{i=0}^{q-1} r^{i(e-1)}\right)=0.$$

Si $e=1$, $\sum_{i=0}^{q-1} r^{i(e-1)}=q$, donc $\overline{x}_0=0$, et le groupe de cohomologie étudié est trivial. Sinon, $\overline{x}_0$ peut être choisi arbitrairement dans $\mathrm{S}[\zeta]/(1-\zeta)\mathrm{S}[\zeta]$, et le groupe de cohomologie est isomorphe à $\mathbf{Z}/p\mathbf{Z}$. ■

PROPOSITION 1.4. – *On note* U* *l'image du groupe des unités de* $\mathrm{A}_1$ *par l'homomorphisme canonique de* A *sur* $\mathrm{A}/\mathfrak{P}$, $\overline{r}$ *l'image de* $r$ *dans* $\mathbf{Z}/p\mathbf{Z}$, *et* V* *l'image du groupe des unités de* $\mathrm{S}[\theta]$ *par le* S-*homomorphisme de* $\mathrm{S}[\theta]$ *dans* $\mathbf{Z}/p\mathbf{Z}$ *défini par* $\theta^i \longmapsto r^{i(e-1)}$. *Si* $\langle \mathrm{U}^*, \mathrm{V}^* \rangle$ *est le sous-groupe de* $(\mathbf{Z}/p\mathbf{Z})^*$ *engendré par* U* *et* V*, *le nombre d'extensions indécomposables deux à deux non* S[G]-*isomorphes de* $\mathrm{S}[\theta]$ *par* $\mathfrak{P}^e$ $(e \neq 1)$ *est égal à l'indice* $[(\mathbf{Z}/p\mathbf{Z})^* : \langle \mathrm{U}^*, \mathrm{V}^* \rangle]$.

*Démonstration.* – Elle utilise le théorème suivant de I. Reiner ([16]).

THEOREME. – *Soit* G *un groupe fini d'ordre* $\ell$, I *l'ensemble des diviseurs premiers de* $\ell$, *et* S *l'intersection des localisés de* $\mathbf{Z}$ *en* $s$ *lorsque* $s$ *parcourt* I. *Soit* $\mathrm{M}_0$ *et* $\mathrm{M}_1$ *deux* S[G]-*modules irréductibles non isomorphes, et* $f$ *et* $g$ *deux éléments de*

$Z^1(G, \mathrm{Hom}_S(M_0, M_1))$. *Les extensions* $(M_1, M_0, f)$ *et* $(M_1, M_0, g)$ *sont* S[G]-*isomorphes si et seulement si l'on peut trouver un* S[G]-*automorphisme* $\alpha$ *de* $M_1$, *un* S[G]-*automorphisme* $\beta$ *de* $M_0$, *et* $c \in \mathrm{Hom}_S(M_0, M_1)$ *tels que pour tout* $m \in M_0$ *et tout* $x \in G$, *on ait :*

$$\alpha f_x(xm) - g_x(x\beta m) = xc(m) - c(xm). \tag{1}$$

On applique ce résultat pour $M_1 = \mathfrak{P}^e$ et $M_0 = S[\theta]$. Si $f$ et $g$ définissent des extensions isomorphes, on pose $f^* = \alpha f$ et $g^* = g\beta$ : les quatre extensions de $S[\theta]$ par $\mathfrak{P}^e$ définies respectivement par $f, f^*$, $g$ et $g^*$ sont S[G]-isomorphes.

D'après les calculs de la proposition 1.3, les cocycles sont caractérisés par la valeur de leur image de $\sigma$ en 1, premier élément de la base canonique de $S[\theta]$. L'élément $\sigma$ agit trivialement sur $S[\theta]$ ; on déduit donc de (1) que $f^*$ et $g^*$ ont même image dans $(\mathbf{Z}/p\mathbf{Z})^*$.

Comme $\mathfrak{P}^e$ est un S-module libre de base

$$\{(1 - \zeta)^e, (1 - \zeta)^e \zeta, \ldots, (1 - \zeta)^e \zeta^{p-2}\},$$

il est clair que tout automorphisme de $\mathfrak{P}^e$ compatible avec l'action de $\sigma$ opère comme la multiplication par une unité de A. Si de plus cet automorphisme commute avec $\tau$, l'unité doit appartenir à $A_1$ ; donc $f$ et $f^*$ ont des images dans $(\mathbf{Z}/p\mathbf{Z})^*$ congrues modulo $U^*$.

De manière analogue, on vérifie que l'automorphisme $\beta$ est en fait la multiplication par une unité $\epsilon$ de $S[\theta]$. Posons $\epsilon = \sum_{i=0}^{q-2} \lambda_i \theta^i$. Alors $g_\sigma \beta(1_{S[\theta]}) = g_\sigma \left(\sum_{i=0}^{q-2} \lambda_i \theta^i\right) = \sum_{i=0}^{q-2} \lambda_i r^{i(e-1)} g_\sigma(1)$, et $g$ et $g^*$ ont des images congrues modulo $V^*$. Donc $f$ et $g$ ont des images congrues modulo $\langle U^*, V^* \rangle$.

La réciproque s'obtient simplement en remontant les calculs et en utilisant la réciproque du théorème de I. Reiner. ■

LEMME 1.5. – *L'indice* $[(\mathbf{Z}/p\mathbf{Z})^* : \langle U^*, V^* \rangle]$ *vaut* 1 *ou* $q$. *Si* $p$ *n'est pas congru à* 1 *modulo* $q^2$, *il est égal à* 1.

*Démonstration.* – Galovitch, Reiner et Ullom ont calculé dans [4] l'indice $[(\mathbf{Z}/p\mathbf{Z})^* : U^*]$ : il vaut $q$, donc $[(\mathbf{Z}/p\mathbf{Z})^* : \langle U^*, V^* \rangle]$ divise $q$.

Le groupe $V^*$ contient l'image $\overline{r}^{e-1}$ de $\theta$, qui est un élément de $(\mathbf{Z}/p\mathbf{Z})^*$ d'ordre $q$. Comme $\operatorname{Card} U^* = \frac{p-1}{q}$, si $p$ n'est pas congru à 1 modulo $q^2$, $\overline{r}^{e-1}$ n'appartient pas à $U^*$, et $\langle U^*, V^* \rangle = (\mathbf{Z}/p\mathbf{Z})^*$. ■

LEMME 1.6. – *Soit* $\left(\bigoplus_{i=1}^{\ell} \mathfrak{P}^{e_i}, S[\theta]\right)$ *une extension construite à l'aide de cocycles* $f_i$ *non triviaux. S'il existe deux indices* $j$ *et* $k$ *tels que* $e_j = e_k$, *et que* $f_j$ *soit équivalent à* $f_k$ *modulo un cobord, alors* $\left(\bigoplus_{i=1}^{\ell} \mathfrak{P}^{e_i}, S[\theta]\right)$ *est* S[G]-*isomorphe à* $\left(\bigoplus_{\substack{i=1 \\ i\neq j}}^{\ell} \mathfrak{P}^{e_i}, S[\theta]\right) \oplus \mathfrak{P}^{e_j}$.

*Démonstration.* – Pour faciliter la rédaction, choisissons $j = 1$ et $k = 2$. Posons $M = \left(\bigoplus_{i=1}^{\ell} \mathfrak{P}^{e_i}, S[\theta], f_i\right)$ et

$$M' = \mathfrak{P}^{e_1} \oplus \left(\bigoplus_{i=2}^{\ell} \mathfrak{P}^{e_i}, S[\theta], 2f_2, f_3, \ldots, f_\ell\right).$$

Il est clair que l'application $\Phi$ de M dans $M'$ définie par :

$$(a_1, a_2, \ldots, a_\ell, b) \longmapsto (a_1 - a_2, a_1 + a_2, a_3, \ldots, a_\ell, b),$$

avec $a_i \in \mathfrak{P}^{e_i}$ et $b \in S[\theta]$, est une bijection S-linéaire. De plus, on a :

$$\Phi\sigma(a_1, a_2, \ldots, a_\ell, b) = \sigma\Phi(a_1, \ldots, a_\ell, b)$$

et
$$\Phi\tau(a_1, a_2, \ldots, a_\ell, b) = \tau\Phi(a_1, \ldots, a_\ell, b).$$

Donc les S[G]-modules M et $M'$ sont isomorphes. ■

### 1.4. Conclusion.

Tout $\mathbf{Z}$[G]-module de caractère $\chi^*_{\{1\}} - \chi_G$ est isomorphe à l'un au moins des modules de la liste suivante :

- $\bigoplus_{j=1}^{\ell} \mathfrak{P}^{e_j} \mathfrak{a}_j \oplus \mathfrak{b}$
- $\left(\bigoplus_{j=1}^{\ell} \mathfrak{P}^{e_j} \mathfrak{a}_j, \mathfrak{b}\right) \bigoplus_{j=\ell+1}^{\ell} \mathfrak{P}^{e_j} \mathfrak{a}_j$.

Rappelons que $\mathfrak{b}$ désigne un idéal de B, que tous les $e_j$ vérifient la condition $0 \leqslant e_j \leqslant q-1$, et que les $\mathfrak{a}_j$ sont choisis dans un système exact de représentants des classes d'idéaux de $A_1$.

De plus, $\left(\bigoplus_{j=1}^{\ell} \mathfrak{P}^{e_j} \mathfrak{a}_j , \mathfrak{b}\right)$ désigne une extension de $\mathfrak{b}$ par $\bigoplus_{j=1}^{\ell} \mathfrak{P}^{e_j} \mathfrak{a}_j$, construite à l'aide de cocycles non triviaux ; (cela entraîne en particulier que pour $1 \leqslant j \leqslant \ell$, les $e_j$ sont distincts de 1). D'après le lemme 1.6, on peut aussi imposer que si $e_j = e_k$, $j$ et $k$ appartenant à l'intervalle $[1, \ell]$, les cocycles correspondants ne soient pas cohomologues.

## 2. CONSEQUENCES ARITHMETIQUES DE LA STRUCTURE DE G-MODULE DE $E_K$

### 2.1. Etude de l'application $N_{K/L} : E_K \longrightarrow E_L$.

PROPOSITION 2.1. – *Le groupe* $E_L$ *s'identifie au sous-groupe de* $E_K$ *formé des éléments fixes par* $\tau$. *Si* $\widetilde{E}_K$ *est isomorphe à* $\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j$, $E_L$ *est isomorphe à* $\bigoplus_{j=1}^{q} \mathfrak{P}_1^{\widetilde{e}_j} \mathfrak{a}_j$ ; $\widetilde{e}_j$ *est un entier qui vaut* 0 *si* $e_j = 0$, *et* 1 *sinon. De plus, l'application* $N_{K/L} : \widetilde{E}_K \longrightarrow E_L$ *est surjective.*

*Démonstration.* – Il est clair que tout élément de $E_L$ est fixe par $\tau$. Inversement, soit $u$ un élément de $E_K$ fixe par $\tau$ ; il est représenté par un élément $\epsilon$ de $U_K$ ; si $\epsilon^\tau = -\epsilon$, $\epsilon$ serait fixe par $\tau^2$, ce qui conduit à une contradiction ; donc $\epsilon^\tau = \epsilon$, et $u \in E_L$.

D'après le paragraphe 1.1, le sous-module $\widetilde{E}_K$ de $E_K$ annulé par $(1 + \sigma + \ldots + \sigma^{p-1})$ est isomorphe à une somme directe $\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j$. Comme $E_L$ est inclus dans $\widetilde{E}_K$, $E_L$ est isomorphe au sous-groupe de $\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j$ fixe par $\tau$, c'est-à-dire à $\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j \cap A_1 = \bigoplus_{j=1}^{q} \mathfrak{P}_1^{\widetilde{e}_j} \mathfrak{a}_j$.

A l'élément $\xi$ de $\widetilde{E}_K$ est associé l'élément $(\alpha_1, \ldots, \alpha_q)$ de $\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j$, et à $N_{K/L}(\xi)$ correspond $\left(\mathrm{Tr}_{\mathbf{Q}^{(p)}/\mathbf{Q}_1}(\alpha_1), \ldots, \mathrm{Tr}_{\mathbf{Q}^{(p)}/\mathbf{Q}_1}(\alpha_q)\right)$. L'extension $\mathbf{Q}^{(p)}/\mathbf{Q}_1$, de degré $q$, est modérément ramifiée, donc l'application $Tr_{\mathbf{Q}^{(p)}/\mathbf{Q}_1}$ est une surjection de A sur $A_1$. Cela prouve que l'application $N_{K/L}$ est une surjection de $\widetilde{E}_K$ sur $E_L$. ∎

*Remarque.* – Une démonstration de la surjectivité de l'application $N_{K/L} : E_K \longrightarrow E_L$ figure déjà dans un article de C.D. Walter [17].

### 2.2. Etude de l'application $N_{K/k} : E_K \longrightarrow E_k$.

PROPOSITION 2.2. – *Le groupe* $E_k$ *s'identifie au sous-groupe de* $E_K$ *formé des éléments fixes par* $\sigma$. *Si* $E_K$ *est isomorphe à* $\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j \oplus \mathfrak{b}$, $E_k$ *est isomorphe à* $\mathfrak{b}$. *Si* $E_K$ *est isomorphe à* $\left(\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j, \mathfrak{b}\right) \bigoplus_{j=\ell+1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j$, $E_k$ *est isomorphe à* $\mathfrak{p}_q^{(1)} \dots \mathfrak{p}_q^{(u)} \mathfrak{b}$ ; *les* $\mathfrak{p}_q^{(i)}$ *sont des idéaux premiers de* B *au-dessus de* $p$, *deux à deux distincts, et l'entier* $u$ *est égal au nombre d'exposants* $e_j$ *distincts, pour* $1 \leqslant j \leqslant \ell$.

*Démonstration.* – L'identification de $E_k$ au sous-groupe de $E_K$ formé des éléments fixes par $\sigma$ s'obtient comme celle de $E_L$ à un sous-groupe de $E_K$.

Il est clair que le sous-groupe de $\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j \oplus \mathfrak{b}$, fixe par $\sigma$, est $\mathfrak{b}$. D'autre part, les modules $\left(\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j, \mathfrak{b}\right) \bigoplus_{j=\ell+1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j$ et $M = \left(\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j, \mathfrak{b}\right)$ admettent le même sous-groupe fixe par $\sigma$ ; remarquons que ce sous-groupe s'identifie à $H^0(H, M)$. Si $\mathbf{Z}_{(p)}$ désigne le localisé de $\mathbf{Z}$ en $p$, il est bien connu que les groupes $\mathbf{Z}_{(p)} \otimes_{\mathbf{Z}} H^0(H, M)$ et $H^0(H, \mathbf{Z}_{(p)} \otimes_{\mathbf{Z}} M)$ sont isomorphes. Le module $M_{(p)} = \mathbf{Z}_{(p)} \otimes_{\mathbf{Z}} M$ est une extension de $\mathbf{Z}_{(p)}[\theta]$ par $\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j}$, définie à l'aide de cocycles $f_j \in Z^1(G, \mathrm{Hom}_{\mathbf{Z}_{(p)}}(\mathbf{Z}_{(p)}[\theta], \mathfrak{P}^{e_j}))$ non triviaux. Par des calculs analogues à ceux de la proposition 1.3, on vérifie que chaque $f_j$ est déterminé par $(f_j)_\sigma(1) = (1 - \zeta)^{e_j} \epsilon_j$, $\epsilon_j \notin \mathfrak{P}$.

Désignons par $(a_1, \dots, a_\ell, b)$ un élément de $M_{(p)} : a_i \in \mathfrak{P}^{e_i}$ et $b \in \mathbf{Z}_{(p)}[\theta]$. Cet élément est fixe par $\sigma$ si et seulement si, pour

pour tout indice $j \in [1, \ell]$, on a : $(f_j)_\sigma(b) = (1-\zeta)a_j$. Or $b$ s'écrit $x_0 + x_1\theta + \ldots + x_{q-2}\theta^{q-2}$, $x_i \in \mathbf{Z}_{(p)}$, et

$$(f_j)_\sigma(b) = (1-\zeta)^{e_j}\epsilon_j \times (x_0 + x_1 r^{e_j-1} + \ldots + x_{q-2}(r^{e_j-1})^{q-2}).$$

Pour que $(f_j)_\sigma(b)$ appartienne à $\mathfrak{P}^{e_j+1}$, il faut et il suffit que $x_0 + x_1 r^{e_j-1} + \ldots + x_{q-2}(r^{e_j-1})^{q-2}$ appartienne à $p\mathbf{Z}_{(p)}$.

Considérons alors l'application $\mathbf{Z}_{(p)}$-linéaire $\lambda_j$ de $\mathbf{Z}_{(p)}[\theta]$ dans $\mathbf{F}_p$, définie par $\theta \longmapsto \overline{r}^{e_j-1}$ ; ($\overline{r}$ est la classe de $r$ modulo $p$). Comme $e_j$ est distinct de $1$, $\overline{r}^{e_j-1}$ est un élément d'ordre $q$ de $\mathbf{F}_p^*$, et l'on vérifie facilement que $\lambda_j$ est un homomorphisme d'anneaux surjectif. Son noyau est donc un idéal premier $\mathfrak{p}_q$ de $\mathbf{Z}_{(p)}[\theta]$, au-dessus de $p$.

Comme tout sous-groupe de $\mathbf{F}_p^*$ est cyclique, pour tout $e_k \neq 1$, il existe $x \in \mathbf{Z}$ tel que $\overline{r}^{e_k-1} = \overline{r}^{x(e_j-1)}$ ; l'application $\theta \longmapsto \theta^x$ se prolonge en un automorphisme X de $\mathbf{Z}_{(p)}[\theta]$, et le diagramme suivant est commutatif :

$$\begin{tikzcd}
\mathbf{Z}_{(p)}[\theta] \arrow[rr, "\mathrm{X}"] \arrow[dr, "\lambda_k"'] & & \mathbf{Z}_{(p)}[\theta] \arrow[dl, "\lambda_j"] \\
& \mathbf{F}_p &
\end{tikzcd}$$

Les noyaux de $\lambda_j$ et $\lambda_k$ sont donc conjugés. Comme $p$ est totalement décomposé dans $\mathbf{Z}_{(p)}[\theta]$, les noyaux sont distincts dès que X est non trivial, c'est-à-dire dès que $e_j$ et $e_k$ sont différents.

On obtient ainsi que le sous-groupe $\mathrm{M}_{(p)}^{\langle\sigma\rangle}$ de $\mathrm{M}_{(p)}$ fixe par $\sigma$ est isomorphe à $\mathfrak{p}_q^{(1)} \ldots \mathfrak{p}_q^{(u)}$, les $\mathfrak{p}_q^{(i)}$ étant des idéaux premiers de $\mathbf{Z}_{(p)}[\theta]$ au-dessus de $p$, deux à deux distincts, et $u$ étant égal au nombre d'indices $e_j$ distincts. Pour aboutir au résultat annoncé, il suffit ensuite de remarquer que seule la classe de $\mathfrak{b}$ est déterminée ; donc on peut choisir l'idéal $\mathfrak{b}$ premier à $p$. ■

PROPOSITION 2.3. – *Notons $u$ l'entier qui vaut $0$ si $\mathrm{E}_\mathrm{K}$ est isomorphe à $\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j}\mathfrak{a}_j \oplus \mathfrak{b}$, et qui est égal au nombre d'exposants $e_j$ distincts, pour $1 \leqslant j \leqslant \ell$, si $\mathrm{E}_\mathrm{K}$ est isomorphe à*

$$\left(\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j}\mathfrak{a}_j , \mathfrak{b}\right) \bigoplus_{j=\ell+1}^{q} \mathfrak{P}^{e_j}\mathfrak{a}_j .$$

*Alors l'indice $[\mathrm{E}_k : \mathrm{N}_{\mathrm{K}/k}\mathrm{E}_\mathrm{K}]$ vaut $p^{q-1-u}$.*

*Démonstration.* – Supposons que $E_K$ soit isomorphe à une extension de $\mathfrak{b}$ par $\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j}\mathfrak{a}_j$, définie à l'aide du cocycle $f \in Z^1\left(G, \mathrm{Hom}_Z\left(\mathfrak{b}, \bigoplus_{j=1}^{q} \mathfrak{P}^{e_j}\mathfrak{a}_j\right)\right)$. A l'élément $u$ de $E_K$ est associé le couple $(\alpha, \beta)$, $\alpha \in \bigoplus_{j=1}^{q} \mathfrak{P}^{e_j}$ et $\beta \in \mathfrak{b}$. Donc $N_{K/k}u$ correspond à :

$$(1 + \sigma + \ldots + \sigma^{p-1})(\alpha, \beta) = ((1 + \zeta + \ldots + \zeta^{p-1})\alpha + (f_\sigma + \ldots + f_{\sigma^{p-1}})\beta, p\beta).$$

Or, pour $i > 1$, on a :

$$f_{\sigma^i}(\beta) = (\sigma f_{\sigma^{i-1}} + f_\sigma)(\beta) = (1 + \zeta + \ldots + \zeta^{i-1})f_\sigma(\beta).$$

Donc,

$$(f_\sigma + \ldots + f_{\sigma^{p-1}})(\beta) = f_\sigma(\beta)[1 + (1 + \zeta) + \ldots + (1 + \zeta + \ldots + \zeta^{p-2})] = \frac{f_\sigma(p\beta)}{1 - \zeta}.$$

D'où $(1 + \sigma + \ldots + \sigma^{p-1})(\alpha, \beta) = \left(\frac{f_\sigma(p\beta)}{1 - \zeta}, p\beta\right)$, et les $\mathbf{Z}[G]$-modules $p\,\mathfrak{b}$ et $N_{K/k}E_K$ sont isomorphes.

La proposition 2.2 donne l'image de $E_k$ par ce même isomorphisme. Comme $p$ est totalement décomposé dans l'extension $\mathbf{Q}(\theta)/\mathbf{Q}$, le calcul de l'indice $[E_k : N_{K/k}E_K]$ est alors immédiat. ∎

*Remarque.* – On a vérifié dans [11] que pour qu'une extension galoisienne totalement réelle $\Lambda/\mathbf{Q}$ admette une unité de Minkowski, il faut que pour toute extension intermédiaire $\Lambda'$, l'application $N_{\Lambda/\Lambda'} : E_\Lambda \longrightarrow E_{\Lambda'}$ soit surjective. Donc si une extension métacyclique $K/\mathbf{Q}$ de degré $pq$ admet une unité de Minkowski, $E_K$ est $\mathbf{Z}[G]$-isomorphe à l'un des modules suivants :

$$\left(\bigoplus_{\substack{j=0\\ j\neq 1}}^{q-1} \mathfrak{P}^j\mathfrak{a}_j, \mathfrak{b}\right) \oplus \mathfrak{P}^e\mathfrak{a}, \quad \text{ou} \quad \left(\bigoplus_{\substack{j=0\\ j\neq 1}}^{q-1} \mathfrak{P}^j\mathfrak{a}_j \oplus \mathfrak{P}^e\mathfrak{a}, \mathfrak{b}\right), \quad \text{avec } e \neq 1.$$

### 2.3. Calcul de l'indice $a = [E_K : E_L E_{L^\sigma} \ldots E_{L^{\sigma^{q-1}}} E_k]$.

PROPOSITION 2.4. – *L'entier $u$ étant défini à la proposition 2.3, et les $\widetilde{e}_i$ à la proposition 2.1, si $E_K$ est isomorphe à une extension de $\mathfrak{b}$ par $\bigoplus_{i=1}^{q} \mathfrak{P}^{e_i}\mathfrak{a}_i$, on a :* $a = p^{\sum_{i=1}^{q}(q\widetilde{e}_i - e_i) + u}$.

*Démonstration.* – L'isomorphisme $\Phi$, qui associe à $E_K$ une extension de $\mathfrak{b}$ par $\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j$, transforme $E_L E_{L^\sigma} \dots E_{L^{\sigma^{q-1}}}$ en $\bigoplus_{j=1}^{q} \mathfrak{P}_1^{\tilde{e}_j} \mathfrak{a}_j A$ ; (on le démontre en utilisant la proposition 2.1, et le fait que $\{1, \zeta, \dots, \zeta^{q-1}\}$ est une $A_1$-base de A). Comme $\Phi$ transforme $E_k$ en un sous-groupe de $\mathfrak{b}$ déterminé à la proposition 2.2, on a :

$$a = \left[ \bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \mathfrak{a}_j : \bigoplus_{j=1}^{q} \mathfrak{P}_1^{\tilde{e}_j} \mathfrak{a}_j A \right] \times [\mathfrak{b} : \Phi(E_k)]$$
$$= \prod_{j=1}^{q} N_{\mathbf{Q}(p)/\mathbf{Q}} (\mathfrak{P}_1^{\tilde{e}_j} A \times \mathfrak{P}^{-e_j}) \times p^u . \blacksquare$$

Remarquons que l'indice $a$ ne peut être égal à 1 que lorsque $E_K$ est $\mathbf{Z}[G]$-isomorphe à un module de la forme $\bigoplus_{i=1}^{q} \mathfrak{a}_i A \oplus \mathfrak{b}$. D'autre part, on retrouve dans ce cas particulier la valeur maximum obtenue par F. Halter-Koch dans [6], c'est-à-dire $p^{q(q-1)}$ ; cette valeur correspond au cas où $E_K$ est isomorphe à $\bigoplus_{i=1}^{q} \mathfrak{P} \mathfrak{a}_i \oplus \mathfrak{b}$, ou à $(\mathfrak{P}^2 \mathfrak{a}_1, \mathfrak{b}) \bigoplus_{i=2}^{q} \mathfrak{P} \mathfrak{a}_i$ ; si l'on modifie l'un des $e_i$, l'exposant de $p$ diminue d'au moins une unité dans $\left[ \bigoplus_{i=1}^{q} \mathfrak{P}^{e_i} \mathfrak{a}_i : \bigoplus_{i=1}^{q} \mathfrak{P}_1^{\tilde{e}_i} \mathfrak{a}_i A \right]$, et augmente d'au plus une unité dans $[\mathfrak{b} : \Phi(E_k)]$.

Pour tout corps de nombres $\Lambda$, désignons par $h_\Lambda$ son nombre de classes d'idéaux. L'indice $a$ est apparu dans le calcul du rapport $\frac{h_K}{h_k . h_L^q}$, effectué dans [6] ; on démontre en effet que $\frac{h_K}{h_k . h_L^q} = \frac{a}{p^{\frac{(q-1)(q+2)}{2}}}$. A l'aide des notations des propositions 2.1 et 2.3, on obtient :

$$\frac{h_K}{h_k . h_L^q} = p^{\sum_{i=1}^{q} (q\tilde{e}_i - e_i) + u - \frac{(q-1)(q+2)}{2}} .$$

## 2.4. Invariant de Brauer-Walter.

Soit $\Gamma$ un groupe fini, et $\Delta$ un sous-groupe de $\Gamma$. Si M est un $\Gamma$-module, désignons par $M^\Delta$ le sous-groupe de M fixe par $\Delta$. C.D. Walter étudie dans [17] les $\Gamma$-modules de caractère donné ; il démontre en particulier que si l'on a une relation de dépendance linéaire, à coefficients dans $\mathbf{Z}$, de caractères induits, $\sum_{\Delta} a_{\Delta} \chi_{\Delta}^{*} = 0$, et si les modules M et N sont $\mathbf{Z}[\Gamma]$-isomorphes, alors $\prod_{\Delta} [M^{\Delta} : N^{\Delta}]^{a_{\Delta}} = 1$.

DEFINITION. – *Soit* $\Gamma$ *un groupe fini,* M *et* N *deux* $\mathbf{Z}[\Gamma]$-*modules de même caractère, et* $\mathcal{R} : \sum_{\Delta} a_{\Delta} \chi_{\Delta}^{*} = 0$ *une relation de dépendance linéaire non triviale, à coefficients dans* $\mathbf{Z}$, *de caractères induits. On appelle invariant de Brauer-Walter associé à la relation* $\mathcal{R}$ *et aux modules* M *et* N *le produit* $J_{\mathcal{R}}(M,N) = \prod_{\Delta} [M^{\Delta} : N^{\Delta}]^{a_{\Delta}}$.

On pourra trouver dans un exposé de J.J. Payan [12] quelques propriétés et quelques exemples d'utilisation de cet invariant. En particulier J.J. Payan démontre que si pour tout nombre premier $\ell$, les localisés $\mathbf{Z}_{(\ell)} \otimes M$ et $\mathbf{Z}_{(\ell)} \otimes N$ sont $\mathbf{Z}_{(\ell)}[\Gamma]$-isomorphes, $J_{\mathcal{R}}(M,N) = 1$.

D'après un théorème classique de R. Brauer [1], pour un groupe métacyclique d'ordre $pq$, toutes les relations non triviales entre caractères induits sont des conséquences de la relation $\mathcal{R}$ :

$$q\chi_G - \chi_H^* + \chi_{\{1\}}^* - q\chi_g^* = 0 .$$

Comme représentants des $\mathbf{Z}[G]$-modules de caractère $\chi_{\{1\}}^* - \chi_G$, modulo l'isomorphisme des localisés en $\ell$ pour tout nombre premier $\ell$, choisissons les modules de la forme $\left(\bigoplus_{j=1}^{s} \mathfrak{P}^{e_j}, B\right) \bigoplus_{j=s+1}^{q} \mathfrak{P}^{e_j}$ ou $\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \oplus B$. Toutes les valeurs de $J_{\mathcal{R}}(M,N)$ s'obtiennent à l'aide du résultat suivant :

PROPOSITION 2.5. – *Posons* $T = A^q \oplus B$. *Pour chacun des* $\mathbf{Z}[G]$-*modules ci-dessus,* $J_{\mathcal{R}}(M,T) = a$, *où* $a$ *est l'indice associé à* M *calculé dans la proposition 2.4.*

*Démonstration.* – Si M est de la forme $\bigoplus_{j=1}^{q} \mathfrak{P}^{e_j} \oplus B$, M est contenu dans T, et le calcul de $J_{\mathcal{R}}(M,T)$ est immédiat.

Si M s'écrit $\left(\bigoplus_{j=1}^{s} \mathfrak{P}^{e_j}, B\right) \bigoplus_{j=s+1}^{q} \mathfrak{P}^{e_j}$, notons $M_1$ le sous-groupe de $\left(\bigoplus_{j=1}^{s} \mathfrak{P}^{e_j}, B\right)$ fixe par $\sigma$. On vérifie facilement que $(pA)^q \oplus M_1$ est un sous-$\mathbf{Z}[G]$-module de M isomorphe à T ; d'où le calcul de $J_{\mathcal{R}}(M,T)$. ■

Lorsque K admet une unité de Minkowski, $E_K$ est $\mathbf{Z}[G]$-isomorphe au module $M = \mathbf{Z}[G]/\mathbf{Z}\widetilde{G}$, où $\widetilde{G}$ désigne l'élément $\sum_{\sigma \in G} \sigma$ de $\mathbf{Z}[G]$. En utilisant la remarque du paragraphe 2.2, on obtient : $J_{\mathfrak{K}}(M, T) = 2^{\frac{1}{2}q(q-1)+q\tilde{e}-e}$. La connaissance de cet invariant équivaut à celle de l'indice $e$. Si $e = 1$, ou bien si le groupe $\langle U^*, V^* \rangle$ défini dans la proposition 1.4 est identique à $(\mathbf{Z}/p\mathbf{Z})^*$, on connait la structure de M modulo les $\mathbf{Z}_{(\ell)}[G]$-isomorphismes, pour tout nombre premier $\ell$. Nous effectuerons le calcul de $J_{\mathfrak{K}}(M, T)$ dans un cas particulier, au paragraphe 4.

## 3. CONTRAINTES GALOISIENNES SUR LE GROUPE DES CLASSES D'IDEAUX DE K

Lorsqu'on connaît la structure de G-module de $E_K$, on détermine assez facilement les groupes $H^n(H, U_K)$ et $H^n(g, U_K)$. Or d'après K. Iwasawa [7], ces groupes s'interprètent en termes d'idéaux ou de classes d'idéaux. En particulier, K. Iwasawa démontre :

PROPOSITION 3.1. – *Soit $\Lambda'/\Lambda$ une extension galoisienne finie de corps de nombres, de groupe de Galois $\Gamma$. Le groupe $H^1(\Gamma, U_{\Lambda'})$ est canoniquement isomorphe au quotient du groupe des idéaux principaux invariants de $\Lambda'$ modulo le groupe des idéaux principaux de $\Lambda$.*

L'interprétation du deuxième groupe de cohomologie est moins simple. Dans l'article de K. Iwasawa, on trouve encore :

PROPOSITION 3.2. – *Si $\Lambda'/\Lambda$ est non ramifiée, $H^2(\Gamma, U_{\Lambda'})$ est isomorphe au quotient du groupe des classes invariantes de $\Lambda'/\Lambda$ par le groupe des classes représentées par des idéaux de $\Lambda$.*

Reprenons les calculs dans le cas où il y a ramification. Si l'on désigne par :

$I_K$ le groupe des idéaux de K,

$H_K$ le groupe des classes d'idéaux de K,

$J_K$ le groupe des idèles de K,

$C_K$ le groupe des classes d'idèles de K,

$P_K$ le groupe des idèles principaux de K,

$W_K$ le noyau de l'homomorphisme canonique de $J_K$ sur $I_K$,

on a des isomorphismes bien connus entre les groupes suivants : $P_K \cap W_K$ et $I_K$, $J_K/P_K W_K$ et $H_K$, $P_K/U_K$ et $P_K W_K/W_K$, et $P_K W_K/P_K$ et $W_K/U_K$. Donc la suite exacte :

$$1 \longrightarrow P_K W_K/W_K \longrightarrow J_K/P_K \longrightarrow J_K/P_K W_K \longrightarrow 1$$

s'écrit aussi :

$$1 \longrightarrow W_K/U_K \longrightarrow C_K \longrightarrow H_K \longrightarrow 1 .$$

Comme $K/\mathbf{Q}$ est une extension galoisienne de groupe G, la suite exacte ci-dessus est une suite de $\Delta$-modules, pour tout sous-groupe $\Delta$ de G, et l'on peut écrire la suite de cohomologie associée au groupe $\Delta$. Or, d'après un théorème de J. Tate (qui figure par exemple dans [2], p. 197), le groupe $\hat{H}^i(\Delta, C_K)$ est isomorphe à $\hat{H}^{i-2}(\Delta, \mathbf{Z})$, où $\Delta$ agit trivialement sur $\mathbf{Z}$. Si $\Delta$ est cyclique d'ordre $\alpha$, pour $i$ impair, $\hat{H}^i(\Delta, C_K)$ est trivial, et pour $i$ pair, $\hat{H}^i(\Delta, C_K)$ est isomorphe à $\mathbf{Z}/\alpha\mathbf{Z}$. Dans ce cas, on a la suite exacte (1) :

$$0 \longrightarrow H^1(\Delta, H_K) \longrightarrow H^2(\Delta, W_K/U_K) \longrightarrow \mathbf{Z}/\alpha\mathbf{Z} \longrightarrow H^2(\Delta, H_K)$$
$$\longrightarrow H^3(\Delta, W_K/U_K) \longrightarrow 0 .$$

La détermination des groupes $H^i(\Delta, W_K/U_K)$ s'effectue à partir des groupes de cohomologie de $U_K$ et $W_K$.

PROPOSITION 3.3. – *Soit* $K/\mathbf{Q}$ *une extension métacyclique de degré* $pq$. *L'entier* $u$ *étant défini dans la proposition 2.3, on a :*

$$H^1(H, U_K) \simeq \mathbf{F}_p^{q-u} \quad , \quad H^2(H, U_K) \simeq \mathbf{F}_p^{q-1-u}$$

$$H^1(g, U_K) \simeq \mathbf{F}_q \quad \text{et} \quad H^2(g, U_K) = (0) .$$

*Démonstration.* – Remarquons que $U_K$ et $E_K$ admettent mêmes groupes de cohomologie relativement à H et à $g$. En effet, on a la suite exacte :

$$1 \longrightarrow \{\pm 1\} \longrightarrow U_K \longrightarrow E_K \longrightarrow 1 ;$$

comme les groupes H et $g$ sont d'ordre impair, les groupes de cohomologie de $\{\pm 1\}$ sont triviaux.

Le calcul des groupes $H^2(g, E_K)$ et $H^2(H, E_K)$ est immédiat grâce aux propositions 2.1 et 2.3. Comme on connaît les quotients de Herbrand (voir H. Yokoi [19], lemme 3), on en déduit les groupes $H^1(g, E_K)$ et $H^1(H, E_K)$. ∎

*Remarque.* – D'après C.D. Walter [18], l'homomorphisme "d'extension" est une injection du groupe des classes de L dans le groupe des classes de K. Comme $H^1(g, U_K)$ n'est jamais trivial, d'après la proposition 3.1, K possède un idéal principal produit de puissances d'idéaux premiers ramifiés dans K/L.

Choisissons pour $\Delta$ le sous-groupe $g$, et notons $t$ le nombre d'idéaux premiers ramifiés dans K/L. D'après la théorie du corps de classes local, on a : $H^1(g, W_K) \simeq H^2(g, W_K) \simeq \mathbf{F}_q^t$. Donc, en utilisant la proposition 3.3, on obtient que $H^2(g, W_K/U_K)$ est un $\mathbf{F}_q$-espace-vectoriel de dimension $t$ ou $t+1$. Et grâce à la suite exacte (1), on vérifie que les deux $\mathbf{F}_q$-espaces vectoriels $H^1(g, H_K)$ et $H^2(g, H_K)$ sont isomorphes de dimension $t-1$, $t$ ou $t+1$. Rappelons que $H^2(g, H_K)$ s'interprète comme quotient du groupe des classes invariantes relatives à K/L par le groupe $N_{K/L} H_K$ ; quant à $H^1(g, H_K)$, il est isomorphe au quotient du groupe des classes de norme triviale sur L par le sous-groupe des classes quotients d'une classe de K par sa conjuguée par $\tau$. Ces résultats fournissent en particulier une minoration du $q$-rang du groupe des classes de K invariantes par $g$, à rapprocher de celle donnée par J. Martinet [10 bis].

Si l'on remplace $g$ par H, et si l'on note $t'$ le nombre d'idéaux premiers ramifiés dans $K/k$, on a encore :

$$H^1(H, W_K) \simeq H^2(H, W_K) \simeq \mathbf{F}_p^{t'}.$$

Comme les groupes $H^i(H, U_K)$ sont moins simples que les groupes $H^i(g, U_K)$, nous ne ferons pas d'étude générale de ce cas.

## 4. EXEMPLES NUMERIQUES

Citons d'abord quelques résultats de la théorie du corps de classes global, qui assurent l'existence de telles extensions.

THEOREME 4.1. – *Soit* $k/\mathbf{Q}$ *une extension cyclique de degré* $q$ *premier, et soit* $p$ *un nombre premier congru à* 1 *modulo* $q$. *Si* $p$ *divise le nombre de classes d'idéaux de* $k$, *il existe des extensions* K *cycliques non ramifiées de* $k$, *de degré* $p$ *sur* $k$, *et galoisiennes non abéliennes sur* $\mathbf{Q}$.

Ce théorème figure par exemple dans [3]. D'autre part, H. Kisilevsky a démontré dans [8] le résultat suivant :

THEOREME 4.2. – *Si* $\Lambda$ *est un corps de nombres dont le* $p$-*groupe des classes est cyclique d'ordre* $p$, *la* $p$-*tour des corps de classes est de longueur* 1.

Enfin l'on a (cf. [19]) :

THEOREME 4.3. – *Soit* $\Lambda'$ *une extension cyclique non ramifiée d'un corps de nombres* $\Lambda$. *Si le nombre de classes d'idéaux de* $\Lambda$ *qui deviennent principales dans* $\Lambda'$ *est égal à* $[\Lambda' : \Lambda]$, *alors* : $U_\Lambda = N_{\Lambda'/\Lambda} U_{\Lambda'}$.

Lorsqu'on parcourt la table figurant dans l'article [5], on remarque des corps cubiques cycliques à nombre de classes premier congru à 1 modulo 3. Le premier rencontré est le corps $k$ de discriminant $313^2$, de nombre de classes 7 ; il existe donc une extension $K/k$ non ramifiée, telle que $K/\mathbf{Q}$ soit métacyclique de degré 21. D'après les théorèmes 4.2 et 4.3 le nombre de classes de K n'est pas divisible par 7, et l'application $N_{K/k} : U_K \longrightarrow U_k$ est surjective.

Compte-tenu des résultats des paragraphes 1.4 et 2.2, et du fait que les corps cyclotomiques $\mathbf{Q}^{(7)}$ et $\mathbf{Q}^{(3)}$ sont principaux, $E_K$ est $\mathbf{Z}[G]$-isomorphe à un module du type : $(A \oplus \mathfrak{P}^2, B) \oplus \mathfrak{P}^e$. (Pour $p = 7$ et $q = 3$, on peut en effet utiliser les lemmes 1.5 et 1.6). D'après la proposition 2.4, l'indice $a = [E_K : E_L E_{L^\sigma} E_{L^{\sigma^2}} E_k]$ vaut $7^{3+3\widetilde{e}-e}$, l'entier $\widetilde{e}$ étant égal à 0 pour $e = 0$, et à 1 sinon. La formule du nombre de classes, rappelée au paragraphe 2.3, conduit à l'égalité : $h_K = 7^{3\widetilde{e}-e-1} \times h_L^3$. Comme 7 ne doit pas diviser $h_K$, nécessairement $h_L$ est premier à 7, et $e$ vaut 2 ; ainsi la structure de $\mathbf{Z}[G]$-module de $E_K$ est parfaitement déterminée : $E_K$ est $\mathbf{Z}[G]$-isomorphe à $(A \oplus \mathfrak{P}^2, B) \oplus \mathfrak{P}^2$.

Comme l'application $N_{K/k} : E_K \longrightarrow E_k$ est surjective, on peut se poser la question de savoir si K admet une unité de Minkowski. Le lemme suivant prouve qu'il n'en est rien.

LEMME 4.4. – *Soit* K *une extension métacyclique de* $\mathbf{Q}$, *de degré* 21. *Si* K *admet une unité de Minkowski,* $E_K$ *est* $\mathbf{Z}[G]$-*isomorphe au module* $(A \oplus \mathfrak{P}^2, B) \oplus \mathfrak{P}$.

*Démonstration.* – Posons encore $M = \mathbf{Z}[G]/\mathbf{Z}\widetilde{G}$, avec $\widetilde{G} = \sum_{\sigma \in G} \sigma$. D'après la dernière remarque du paragraphe 2, la structure de $\mathbf{Z}[G]$-module de M est connue sans ambiguïté si l'on sait calculer l'invariant $J_{\mathfrak{R}}(M, T) = a$ associé.

Tout élément de M s'écrit de manière unique :

$$\alpha = \sum_{i=0}^{6} (\lambda_i + \mu_i \tau + \nu_i \tau^2)\, \sigma^i, \quad \text{avec} \quad \sum_{i=0}^{6} (\lambda_i + \mu_i + \nu_i) = 0 .$$

On vérifie facilement que pour que $\alpha$ soit fixe par $\tau$ (resp. $\tau\sigma$, resp. $\tau\sigma^2$, resp. $\sigma$), il doit s'écrire :

$$\begin{aligned}
&\alpha = (1 + \tau + \tau^2)\, \Sigma\, a_i \sigma^i && \text{avec } \Sigma\, a_i = 0 ,\\
\text{resp. } &\alpha = (1 + \tau\sigma + (\tau\sigma)^2)\, \Sigma\, b_i \sigma^i && \text{avec } \Sigma\, b_i = 0 ,\\
\text{resp. } &\alpha = (1 + \tau\sigma^2 + (\tau\sigma^2)^2)\, \Sigma\, c_i \sigma^i && \text{avec } \Sigma\, c_i = 0 ,\\
\text{resp. } &\alpha = (\lambda + \mu\tau + \nu\tau^2)\, \Sigma\, \sigma^i \quad \text{avec} && \lambda + \mu + \nu = 0 .
\end{aligned}$$

Etant donné $\lambda_i, \mu_i, \nu_i$, cherchons à quelles conditions l'on peut trouver $\lambda, \mu, \nu, a_i, b_i$ et $c_i$ tels que :

$$\begin{aligned}
\Sigma\, (\lambda_i + \mu_i \tau + \nu_i \tau^2)\, \sigma^i &= (1 + \tau + \tau^2)\, \Sigma\, a_i \sigma^i \\
&\quad + (1 + \tau\sigma + (\tau\sigma)^2)\, \Sigma\, b_i \sigma^i + (1 + \tau\sigma^2 + (\tau\sigma^2)^2)\, \Sigma\, c_i \sigma^i \\
&\quad + (\lambda + \mu\tau + \nu\tau^2)\, \Sigma\, \sigma^i .
\end{aligned}$$

Il est clair qu'il faut d'abord que $\Sigma \lambda_i \equiv \Sigma\, \mu_i \equiv 0 (7)$. Ces conditions étant réalisées, les valeurs de $\lambda, \mu, \nu$ sont déterminées ; posons alors $\lambda_i' = \lambda_i - \lambda$, $\mu_i' = \mu_i - \mu$ et $\nu_i' = \nu_i - \nu$. Comme $\tau\sigma = \sigma^2\tau$, $\sigma\tau = \tau\sigma^4$, et l'on obtient le système suivant, où les indices sont définis modulo 7 :

$$\left\{ \begin{aligned} \lambda_i' &= a_i + b_i + c_i \\ \mu_i' &= a_i + b_{i-1} + c_{i-2} \\ \nu_i' &= a_i + b_{i-5} + c_{i-3} . \end{aligned} \right. \tag{1}$$

D'où :

$$\begin{cases} \ell_i = \mu_i' - \lambda_i' = b_{i-1} - b_i + c_{i-2} - c_i \\ m_i = \nu_i' - \lambda_i' = b_{i-5} - b_i + c_{i-3} - c_i . \end{cases} \tag{2}$$

En éliminant les $b_i$, il vient :

$$\ell_{i+1} + \ell_{i+2} + m_i = c_{i+4} + c_{i-1} - c_{i+1} - c_{i+2} . \tag{3}$$

Posons $d_i = c_{i+2} - c_i$. Le système (3) se transforme en :

$$\ell_{i+1} + \ell_{i+2} + m_i = d_{i+2} - d_{i-1} . \tag{4}$$

Comme $\Sigma \ell_i = \Sigma m_i = 0$, la septième équation du système est une conséquence des autres ; les six premières équations permettent de calculer tous les $d_i$ en fonction de $d_0$. Le choix de $d_0$ est imposé par la condition $\Sigma d_i = 0$, qui s'exprime encore : $7d_0 + F_1(\lambda_i , \mu_i , \nu_i) = 0$, où $F_1$ est une forme linéaire à coefficients dans $\mathbf{Z}$. Le calcul de $d_0$ n'est possible que si $F_1(\lambda_i , \mu_i , \nu_i) \equiv 0$ modulo 7 ; remarquons que cette condition n'est pas triviale, puisque $\nu_i$ n'y intervient que par l'intermédiaire de l'expression : $6m_1 + 5m_4 + 4m_0 + 3m_3 + 2m_6 + m_2$.

Les $d_i$ étant ainsi obtenus, six des formules de définition des $d_i$ donnent les $c_i$ en fonction de $c_0$, tandis que la septième est une conséquence des autres. Comme on doit avoir $\Sigma c_i = 0$, $c_0$ vérifie l'égalité : $7c_0 + 7 \times 3d_0 + F_2(\lambda_i , \mu_i , \nu_i) = 0$, $F_2$ étant une forme linéaire à coefficients dans $\mathbf{Z}$. D'où une nouvelle condition : $F_2(\lambda_i , \mu_i , \nu_i) \equiv 0 \mod 7$, indépendante de la précédente, puisque les $\nu_i$ figurent uniquement dans l'expression : $m_1 + 4m_0 + 6m_3 + 6m_6 + 4m_2$.

On utilise alors les six premières équations du système (2), qui définissent tous les $b_i$ en fonction de $b_0$ ; exprimer que $\Sigma b_i = 0$ conduit à imposer une nouvelle condition, $F_3(\lambda_i , \mu_i , \nu_i) \equiv 0 \mod 7$, où les $\nu_i$ interviennent par : $2m_1 + m_0 + 5m_3 + 5m_6 + m_2$. On obtient sans problème les $a_i$ à partir de (1). L'indice $a$ cherché vaut donc $7^5$, et $e = 1$. ■

Pour terminer l'étude de ce cas particulier, voyons ce que l'on peut obtenir du calcul des groupes de cohomologie de $U_K$ et $H_K$. Les résultats relatifs au sous-groupe H sont déjà exploités : ils se retrouvent dans la théorie du corps de classes.

Pour le sous-groupe $g$, la proposition 3.3 donne :

$$H^1(g, U_K) \simeq \mathbf{F}_3 \quad \text{et} \quad H^2(g, U_K) = (0).$$

D'après [12], il existe dans $K/L$ un unique idéal premier ramifié, qui est au-dessus de 313 ; comme C.D. Walter a montré dans [18] l'injectivité de l'homomorphisme d'extension des idéaux, $j_{K/L} : H_L \longrightarrow H_K$, on déduit de la proposition 3.1 que tout idéal premier de K au-dessus de 313 est équivalent à l'étendu d'un idéal de L ou d'un de ses conjugués. Remarquons de plus que le groupe des classes invariantes par $g$ est isomorphe à $H_L$ ; donc le 3-rang du groupe $H_L$ est supérieur ou égal à la dimension du $\mathbf{F}_3$-espace vectoriel $H^2(g, H_K)$. En particulier, si 3 ne divise pas $h_L$, toute classe de K de norme triviale sur L est quotient d'une classe de K par sa conjugée par $\tau$.

Comme la table [5] fournit aussi des corps cubiques cycliques de nombre de classes 13 ou 19, on pourrait construire de manière analogue des extensions métacycliques de degré $3 \times 13$ ou $3 \times 19$, non ramifiées dans la branche $K/k$. Remarquons enfin qu'il serait possible de préciser numériquement les corps ainsi définis : J. Cougnard indique en effet dans [3] une méthode pour déterminer le polynôme irréductible d'un élément primitif de K.

## BIBLIOGRAPHIE

[1] R. BRAUER, Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoischen Körpers, *Math. Nachr.*, 4 (1951), 158-174.

[2] J. CASSELS et A. FRÖHLICH, Algebraic Number Theory. Academic Press, New-York, 1967.

[3] J. COUGNARD, Sur les extensions galoisiennes non abéliennes de degré $pq$ du corps des rationnels ($p$ et $q$ premiers), thèse de 3^e^ cycle, Bordeaux, 1972.

[4] S. GALOVITCH, I. REINER et S. ULLOM, Class groups for integral representations of metacyclic groups, *Mathematika,* 19 (1972), 105-111.

[5] M.N. GRAS, N. MOSER et J.J. PAYAN, Approximation algorithmique du groupe des classes de certains corps cubiques cycliques, *Acta Arithmetica,* 23 (1973), 295-300.

[6] F. HALTER-KOCH et N. MOSER, Sur le nombre de classes de certaines extensions métacycliques sur $\mathbf{Q}$ ou sur un corps quadratique imaginaire, *J. Math. Soc. Japan,* 30 (1978), 237-248.

[7] K. IWASAWA, A note on the group of units of an algebraic number field, *J. Math. pures et appliquées,* 35 (1956), 189-192.

[8] H. KISILEVSKY, Some results related to Hilbert's theorem 94, *J. Number Theory,* 2 (1970), 198-206.

[9] S.N. KURODA, Über die Klassenzahl eines relativ zyklischen Zahlkörpers von Primzahlgrade, *Proc. Japan Academy,* 40 (1964), 623-626.

[10] LENA CHANG PU, Integral representations of non abelian groups of order *pq*, *Mich. Math. J.,* 12 (1965), 231-246.

[10bis] J. MARTINET, Tours de corps de classes et estimations de discriminants, *Inventiones math.,* 44 (1978), 65-73.

[11] N. MOSER, Unités et nombre de classes d'une extension galoisienne diédrale de $\mathbf{Q}$, *Abh. Math. Sem. Hamburg* (à paraître).

[12] J.J. PAYAN, Sur le théorème des indices de Brauer-Walter. Application à l'existence d'unités de Minkowski, *Sém. Th. Nb.,* Grenoble, 1975-1977.

[13] J. PORUSCH, Die Arithmetik in Zahlkörpern, deren zugehörige Galoische Körper spezielle metabelsche gruppen besitzen, auf klassenkörpertheoretischer Grundläge, *Math. Z.,* 37 (1933), 134-160.

[14] I. REINER et C. CURTIS, Representation theory of finite groups and associative algebras, Interscience New-York, 1962.

[15] M. ROSEN, Representations of twisted group rings, Ph. D. Thesis, Princeton, 1963.

[16] Représentations entières de certains groupes finis, *Sém. Th. Nb.,* Grenoble, 1973-1974.

[17] C.D. WALTER, Brauer class number relation. (à paraître dans *Acta Arithmetica*).

[18] C.D. WALTER, A class number relation in Frobenius extensions of number fields, *Mathematika,* 24 (1977), 216-225.

[19] H. YOKOI, On the class number of a relatively cyclic number field, *Nagoya Math. J.,* 29 (1967), 31-44.

Manuscrit reçu le 28 avril 1978.

Nicole MOSER,
Université de Grenoble I
Laboratoire de Mathématiques Pures
Associé au CNRS
Institut Fourier
B.P. 116
38402 St Martin d'Hères.