PHILIPPE CASSOU-NOGUÈS
JACQUES QUEYRUT

Structure galoisienne des anneaux d'entiers d'extensions sauvagement ramifiées. II

Annales de l'institut Fourier, tome 32, nº 1 (1982), p. 7-27
<http://www.numdam.org/item?id=AIF_1982__32_1_7_0>

Ann. Inst. Fourier, Grenoble
32, 1 (1982), 7-27

STRUCTURE GALOISIENNE DES ANNEAUX D'ENTIERS D'EXTENSIONS SAUVAGEMENT RAMIFIÉES, II

par Ph. CASSOU-NOGUES* et J. QUEYRUT*

1. Introduction.

Soit S un ensemble fini de places de $\mathbf{Q}$ et $\mathfrak{D}$ un ordre de $\mathbf{Z}$ dans la $\mathbf{Q}$-algèbre d'un groupe G fini. On sait classifier ([7]) les $\mathfrak{D}$-modules localement libres pour toute place de $\mathbf{Q}$ n'appartenant pas à S, au moyen du groupe de Grothendieck $\mathcal{K}_0^S(\mathfrak{D})$; on note $\widetilde{\mathcal{K}}_0^S(\mathfrak{D})$ le sous-groupe de torsion de $\mathcal{K}_0^S(\mathfrak{D})$ et on remarque qu'il s'identifie, si S est vide, au groupe des classes usuelles $\mathcal{C}\ell(\mathfrak{D})$ ([14]). On note $\mathfrak{M}$ un ordre maximal de $\mathbf{Z}$ dans $\mathbf{Q}[G]$ contenant $\mathbf{Z}[G]$.

On considère une extension galoisienne finie N, d'un corps de nombres K, de groupe de Galois G ; on note $\mathbf{Z}_N$ l'anneau des entiers de N.

Lorsque N est une extension modérément ramifiée de K, $\mathbf{Z}_N$ définit un élément que l'on note $U_{N/K}$ de $\mathcal{C}\ell(\mathbf{Z}[G])$. Fröhlich ([14]) a démontré que $U_{N/K}$ appartient au noyau de l'homomorphisme d'extension des scalaires de $\mathcal{C}\ell(\mathbf{Z}[G])$ sur $\mathcal{C}\ell(\mathfrak{M})$ (le noyau ne dépend pas du choix de $\mathfrak{M}$). On peut décomposer $U_{N/K}$ en un produit $t(W_{N/K}).V_{N/K}$ où $t(W_{N/K})$ est un élément d'ordre 1 ou 2, défini à partir des constantes de l'équation fonctionnelle des séries L d'Artin associées aux caractères symplectiques de G, qui est égal à 1 lorsque ces constantes valent $+1$. Une forme précise d'une conjecture de Fröhlich est que $V_{N/K}$ est égal à 1. Cette conjecture est démontrée dans [1] et [2] pour une grande famille d'extensions N de K ; les méthodes utilisées consistent à définir un ordre $\mathfrak{A}$ de $\mathbf{Z}$ dans $\mathbf{Q}[G]$ contenant $\mathbf{Z}[G]$, en général strictement contenu dans $\mathfrak{M}$, à démontrer que $V_{N/K}$ appartient au

(*) Laboratoire associé au C.N.R.S. n° 226.

noyau de l'homomorphisme d'extension des scalaires de $\mathcal{C}\ell(\mathbf{Z}[G])$ sur $\mathcal{C}\ell(\mathfrak{A})$ et à majorer l'exposant de ce groupe.

Dans [7] et [8], Queyrut a unifié le cas sauvage et le cas modéré qui avait été traité par Fröhlich. Soit S un ensemble fini de places de $\mathbf{Q}$ contenant les places de K sauvagement ramifiées dans N, c'est-à-dire tel que l'ensemble des idéaux premiers de K au-dessus des nombres premiers p de S contienne les idéaux premiers de K sauvagement ramifiés dans N. Alors $\mathbf{Z}_N$ définit un élément, que l'on note $U^S_{N/K}$, de $\widetilde{\mathcal{K}}^S_0(\mathbf{Z}[G])$. Le principal résultat de [8] est que $U^S_{N/K}$ appartient au noyau de l'homomorphisme d'extension des scalaires de $\widetilde{\mathcal{K}}^S_0(\mathbf{Z}[G])$ sur $\widetilde{\mathcal{K}}^S_0(\mathfrak{M}^S)$ où $\mathfrak{M}^S$ est un ordre de $\mathbf{Z}$ dans $\mathbf{Q}[G]$, localement maximal pour toute place p de $\mathbf{Q}$ n'appartenant pas à S, le résultat de Fröhlich correspondant au cas où S est vide.

Le but de cet article est de démontrer que les résultats de Cassou-Noguès, ([1] et [2]), se généralisent eux-aussi, sans hypothèse sur la ramification de N sur K, à condition de se placer dans des groupes de Grothendieck convenables. L'élément $U^S_{N/K}$ se décompose dans $\widetilde{\mathcal{K}}^S_0(\mathbf{Z}[G])$ en deux éléments $t^S(W_{N/K})$ et $V^S_{N/K}$ où $t^S(W_{N/K})$ est un élément d'ordre 1 ou 2, égal à 1 lorsque les constantes de l'équation fonctionnelle des séries L d'Artin valent $+1$ pour les caractères symplectiques. La conjecture faite par Queyrut dans [8] peut se préciser par l'égalité $V^S_{N/K} = 1$. On définit (§ 4) un ordre $\mathfrak{A}^S$ de $\mathbf{Q}[G]$ contenant $\mathbf{Z}[G]$, en général strictement contenu dans $\mathfrak{M}^S$ et l'on démontre, (théorème 4.1), que l'image de $V^S_{N/K}$ dans $\widetilde{\mathcal{K}}^S_0(\mathfrak{A}^S)$ est triviale. Dans le paragraphe 5, on obtient une majoration de l'exposant du noyau de l'homomorphisme de $\widetilde{\mathcal{K}}^S_0(\mathbf{Z}[G])$ dans $\widetilde{\mathcal{K}}^S_0(\mathfrak{A}^S)$; on en déduit, (théorème 5.3), une majoration de l'ordre de $V^S_{N/K}$ et une grande classe d'extensions N de K et de parties S pour lesquelles $V^S_{N/K}$ est égal à 1. C'est le cas, en particulier, pour les extensions dont le degré est sans facteur cubique, pour les extensions diédrales, (resp. quaternioniennes), de degré $2m$, (resp. $4m$), avec m impair et m quelconque si 2 appartient à S.

On utilise essentiellement les descriptions des groupes $\widetilde{\mathcal{K}}^S_0(\mathfrak{O})$ données dans [7] et du représentant de $U^S_{N/K}$ dans $\widetilde{\mathcal{K}}^S_0(\mathbf{Z}[G])$ donné dans [8]. L'élément $V^S_{N/K}$ est décrit dans le paragraphe 1 ; il appartient à un sous-groupe canonique de $\widetilde{\mathcal{K}}^S_0(\mathbf{Z}[G])$ qui est interprété algébriquement dans ce paragraphe. On montre que les méthodes de [1] se généralisent dans cette situation en démontrant, dans le paragraphe 2, des propriétés de congruences vérifiées par les sommes de Gauss galoisiennes sur certains sous-groupes du groupe des caractères virtuels de G. L'article se termine, (§ 6), par une généralisation dans $\widetilde{\mathcal{K}}_0^S(\mathbf{Z}[G])$ d'un théorème de dualité démontré dans [12] par M.J. Taylor.

Notations. – Pour tout anneau A, on note A^* son groupe d'unités. On choisit une clôture algébrique $\overline{\mathbf{Q}}$ de $\mathbf{Q}$ et on note $G_{\mathbf{Q}}$ le groupe de Galois de $\overline{\mathbf{Q}}$ sur $\mathbf{Q}$. L'ensemble des places de $\mathbf{Q}$, noté $\mathcal{P}(\mathbf{Q})$, s'identifie à l'ensemble formé de la place archimédienne p_∞ de $\mathbf{Q}$ et de l'ensemble $\mathcal{P}(\mathbf{Z})$ des nombres premiers de $\mathbf{Z}$. L'indexation par un élément p appartenant à $\mathcal{P}(\mathbf{Q})$ désignera la complétion en p.

Soit $J(\overline{\mathbf{Q}})$ le groupe des idèles de $\overline{\mathbf{Q}}$. Pour tout $p \in \mathcal{P}(\mathbf{Q})$ le groupe $(\mathbf{Q}_p \otimes_{\mathbf{Q}} \overline{\mathbf{Q}})^*$ peut être considéré comme un sous-groupe de $J(\overline{\mathbf{Q}})$. Un élément x appartenant à $J(\overline{\mathbf{Q}})$ s'écrit ainsi sous la forme $(x_p)_{p\in\mathcal{P}(\mathbf{Q})}$ où x_p appartient à $(\mathbf{Q}_p \otimes_{\mathbf{Q}} \overline{\mathbf{Q}})^*$. On note $U(\overline{\mathbf{Q}})^+$ le groupe des idèles $x = (x_p)_{p\in\mathcal{P}(\mathbf{Q})}$ tels que x_p est une unité pour tout $p \in \mathcal{P}(\mathbf{Z})$ et x_{p_∞} est totalement réel et positif, ce qui signifie la chose suivante : en choisissant un prolongement de la place archimédienne de $\mathbf{Q}$ à $\overline{\mathbf{Q}}$, que l'on note encore p_∞, les autres places de $\overline{\mathbf{Q}}$ sont de la forme p_∞^ω avec ω appartenant à $G_{\mathbf{Q}}$; alors $x_{p_\infty^\omega}$ est réel et positif pour tout ω de $G_{\mathbf{Q}}$. On pose :

$$U_p(\overline{\mathbf{Q}}) = U(\overline{\mathbf{Q}})^+ \cap (\mathbf{Q}_p \otimes_{\mathbf{Q}} \overline{\mathbf{Q}})^* \quad \text{pour tout} \quad p \in \mathcal{P}(\mathbf{Q}).$$

2. Description de $U_{N/K}^S$.

Soit S une partie de l'ensemble $\mathcal{P}(\mathbf{Z})$ des nombres premiers de $\mathbf{Z}$.

Soit $\mathfrak{O}$ un ordre de $\mathbf{Z}$ dans $\mathbf{Q}[G]$. On considère la catégorie $\mathcal{C}_{\ell p}^S(\mathfrak{O})$ des $\mathfrak{O}$-modules M de type fini, sans torsion et tels que pour tout p de $\mathcal{P}(\mathbf{Z})$ n'appartenant pas à S, M_p est un $\mathfrak{O}_p$-module projectif. On désigne par $\mathcal{K}_0^S(\mathfrak{O})$ le groupe de Grothendieck de cette catégorie. C'est le quotient du groupe abélien libre engendré par les classes d'isomorphismes (M) des modules M de $\mathcal{C}^{S}_{\mathfrak{L}_p}(\mathfrak{O})$ par le sous-groupe engendré par les éléments de la forme (M) – (M′) – (M″) où M, M′ et M″ sont liés par une suite exacte

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0 .$$

On note [M] la classe d'un module M dans $\mathcal{K}_0^S(\mathfrak{O})$. Le groupe $\mathcal{K}_0^S(\mathfrak{O})$ a été décrit dans [7]. En particulier, ([7], th. 4.1 et 4.2), il existe un isomorphisme $\eta_{\mathfrak{O}}$ du groupe quotient :

$$\mathrm{Hom}_{G_{\mathbf{Q}}}(R(G), J(\overline{\mathbf{Q}}))/\mathrm{Hom}_{G_{\mathbf{Q}}}(R(G), \overline{\mathbf{Q}}^*) . H(\mathcal{K}_0^S(\mathfrak{O})) \qquad (1)$$

sur $\widetilde{\mathcal{K}}_0^S(\mathfrak{O})$, le sous-groupe de torsion de $\mathcal{K}_0^S(\mathfrak{O})$, où R(G) désigne le groupe des caractères virtuels de G dans $\overline{\mathbf{Q}}$ et $H(\mathcal{K}_0^S(\mathfrak{O}))$ est le sous-groupe des éléments f de $\mathrm{Hom}_{G_{\mathbf{Q}}}(R(G), J(\overline{\mathbf{Q}}))$ vérifiant :

- $\forall p \in S$, $f(\chi)_p \in U_p(\overline{\mathbf{Q}})$, pour tout caractère χ nul sur les éléments de G dont l'ordre est divisible par p
- $\forall p \in \mathcal{P}(\mathbf{Z}) - S$, $f(\chi)_p = \mathrm{Det}_\chi(\alpha_p)$ avec $\alpha_p \in \mathfrak{O}_p^*$, pour tout caractère χ de R(G)
- pour p_∞, $f(\chi)_{p_\infty} \in U_{p_\infty}(\overline{\mathbf{Q}})$, pour tout caractère χ symplectique de R(G).

Soit $\mathfrak{O}'$ un ordre de $\mathbf{Z}$ dans $\mathbf{Q}[G]$ contenant $\mathfrak{O}$ et tel que $\mathfrak{O}_p = \mathfrak{O}'_p$ pour $p \in S$. Le foncteur extension des scalaires induit un homomorphisme noté $\mathrm{Ext}_{\mathfrak{O}}^{\mathfrak{O}'}$ de $\mathcal{K}_0^S(\mathfrak{O})$ sur $\mathcal{K}_0^S(\mathfrak{O}')$. On note également $\mathrm{Ext}_{\mathfrak{O}}^{\mathfrak{O}'}$ l'homomorphisme $\eta_{\mathfrak{O}'}^{-1} \circ \mathrm{Ext}_{\mathfrak{O}}^{\mathfrak{O}'} \circ \eta_{\mathfrak{O}}$.

On considère une extension galoisienne finie N d'un corps de nombres K de groupe de Galois G. Pour toute famille S de $\mathcal{P}(\mathbf{Z})$ contenant les places sauvagement ramifiées dans l'extension N de K, on note $U_{N/K}^S$ l'élément du groupe (1) dont l'image dans $\widetilde{\mathcal{K}}_0^S(\mathbf{Z}[G])$ par $\eta_{\mathbf{Z}[G]}$ est $[\mathbf{Z}_N]$-$[\mathbf{Z}[G]^{[K:\mathbf{Q}]}]$.

Il est immédiat que le théorème I de [7] est équivalent au théorème suivant :

THEOREME 2.1. – *Soit* $\mathfrak{M}^S$ *un ordre de* $\mathbf{Z}$ *dans* $\mathbf{Q}[G]$ *contenant* $\mathbf{Z}[G]$ *vérifiant* $\mathfrak{M}_p^S = \mathbf{Z}_p[G]$, $\forall p \in S$ *et* $\mathfrak{M}_p^S$ *est maximal pour tout* $p \notin S$. *Alors* :

$$\mathrm{Ext}_{\mathbf{Z}[G]}^{\mathfrak{M}^S}(U_{N/K}^S) = 1 .$$

Pour tout χ de $R(G)$, on note $W_{N/K}(\chi)$ la constante de l'équation fonctionnelle des séries L d'Artin associées au caractère χ.

On note $W'_{N/K}$ l'élément de $\mathrm{Hom}_{G_{\mathbf{Q}}}(R(G), J(\overline{\mathbf{Q}}))$ construit de la façon suivante :

(3) – pour tout caractère χ irréductible et non symplectique de G, on pose $W'_{N/K}(\chi) = 1$

– pour tout caractère χ irréductible et symplectique de G, on définit les composantes locales de $W'_{N/K}(\chi)$ par :

$$\begin{aligned} W'_{N/K}(\chi)_p &= 1 & \forall p \in \mathcal{P}(\mathbf{Z}) \\ W'_{N/K}(\chi)_{p_\infty^\omega} &= W_{N/K}(\chi^{\omega^{-1}}), & \forall \omega \in G_{\mathbf{Q}} . \end{aligned}$$

(Noter que lorsque N/K est modérément ramifiée, cette définition coïncide avec celle de A. Fröhlich dans [14].)

On désigne par $t^S_{\mathfrak{O}}(W_{N/K})$, et simplement par $t^S(W_{N/K})$ si $\mathfrak{O} = \mathbf{Z}[G]$, la classe de $W_{N/K}$ dans le groupe quotient (1).

Il est clair que si $\mathfrak{O}'$ est un ordre de $\mathbf{Q}[G]$ contenant $\mathfrak{O}$ et tel que $\mathfrak{O}'_p = \mathfrak{O}_p$ pour $p \in S$, on a $t^S_{\mathfrak{O}'}(W_{N/K}) = \mathrm{Ext}^{\mathfrak{O}'}_{\mathfrak{O}}(t^S_{\mathfrak{O}}(W_{N/K}))$.

On définit maintenant l'élément $V^S_{N/K}$ appartenant au groupe quotient (1) par l'égalité :

$$U^S_{N/K} = t^S(W_{N/K})\, V^S_{N/K} . \tag{4}$$

PROPOSITION 2.2. – *Soit* $\overline{S}$ *l'ensemble des nombres premiers n'appartenant pas à* S *et divisant l'ordre de* G. *L'élément* $V^S_{N/K}$ *est la classe de l'homomorphisme* f *de* $\mathrm{Hom}_{G_{\mathbf{Q}}}(R_G, J(\overline{\mathbf{Q}}))$ *défini par : pour tout* $\chi \in R(G)$,

$$(5)\quad \begin{cases} f(\chi)_p = \mathcal{N}_{K/\mathbf{Q}}(a_p \mid \chi) \cdot \tau_K(\chi)_p^{-1} & \textit{pour } p \in \overline{S} \\ f(\chi)_p = 1 & \textit{pour } p \in \mathcal{P}(\mathbf{Q}) - \overline{S} \end{cases}$$

où $\tau_K(\chi)$ *est la somme de Gauss galoisienne associée au caractère* χ, a_p *est une base de* $\mathbf{Z}_{N_p}$ *sur* $\mathbf{Z}_{K_p}[G]$ *pour tout* $p \in \overline{S}$ *et* $\mathcal{N}_{K/\mathbf{Q}}(a_p \mid \chi)$ *est la résolvante de* a_p *(définie dans* ([14]).

Pour la définition de la somme de Gauss galoisienne nous renvoyons le lecteur à [6], chap. II, § 7.

Démonstration. – Soit $a \in \mathrm{N}$ tel que $\mathrm{N} = \mathrm{K}[\mathrm{G}]\,a$; il existe $a_p \in \mathrm{N}_p$ tel que $\mathbf{Z}_{\mathrm{N}_p} = \mathbf{Z}_{\mathrm{K}_p}[\mathrm{G}]\,a_p$ pour $p \notin \mathrm{S}$ et tel que

$$\mathbf{Z}_{\mathrm{N}_p}/\mathbf{Z}_{\mathrm{N}_p} \cap \mathbf{Z}_{\mathrm{K}_p}[\mathrm{G}]\,a_p \quad \text{et} \quad \mathbf{Z}_{\mathrm{K}_p}[\mathrm{G}]\,a_p/\mathbf{Z}_{\mathrm{N}_p} \cap \mathbf{Z}_{\mathrm{K}_p}[\mathrm{G}]\,a_p$$

aient même suite de Jordan Hölder pour $p \in \mathrm{S}$ ([8] proposition 3.3).

L'élément $\mathrm{U}^{\mathrm{S}}_{\mathrm{N/K}}$ est représenté par l'homomorphisme dont la p-composante est donnée par : $\chi \longmapsto \mathcal{N}_{\mathrm{K}/\mathbf{Q}}(a\,|\,\chi)^{-1}\,\mathcal{N}_{\mathrm{K}/\mathbf{Q}}(a_p\,|\,\chi)$. L'application $\chi \longmapsto \tau_{\mathrm{K}}(\chi)\;\mathcal{N}_{\mathrm{K}/\mathbf{Q}}(a\,|\,\chi)^{-1}\;\mathrm{W}'_{\mathrm{N/K}}(\chi)$ appartient à $\mathrm{Hom}_{\mathrm{G}_{\mathbf{Q}}}(\mathrm{R}(\mathrm{G}), \overline{\mathbf{Q}}^*)$ ([4] propositions 2.3 et 2.5).

L'élément $\mathrm{U}^{\mathrm{S}}_{\mathrm{N/K}}$ est donc représenté par l'homomorphisme dont la p-composante est donnée par

$$\chi \longrightarrow \tau_{\mathrm{K}}(\chi)^{-1}\,\mathcal{N}_{\mathrm{K}/\mathbf{Q}}(a_p\,|\,\chi)\;\;\mathrm{W}'_{\mathrm{N/K}}(\chi).$$

L'application f_1 définie par $f_1(\chi)_p = 1$ pour $p \in \overline{\mathrm{S}}$ et

$$f_1(\chi)_p = \tau_{\mathrm{K}}(\chi)^{-1}\;\mathcal{N}_{\mathrm{K}/\mathbf{Q}}(a_p\,|\,\chi)\;\mathrm{W}'_{\mathrm{N/K}}(\chi)$$

pour $p \notin \overline{\mathrm{S}}$ appartient à $\mathrm{H}(\mathcal{K}^{\mathrm{S}}_0(\mathbf{Z}[\mathrm{G}]))$ ([7] théorème 4.1).

Donc l'élément $\mathrm{V}^{\mathrm{S}}_{\mathrm{N/K}}$ est bien représenté par un élément f vérifiant les conditions (5).

Soit ν'_p l'homomorphisme naturel de

$$\mathrm{Hom}_{\mathrm{G}_{\mathbf{Q}}}(\mathrm{R}(\mathrm{G}), \overline{\mathbf{Q}}_p^*)/\mathrm{Det}(\mathbf{Z}_p[\mathrm{G}]^*)$$

dans $\mathrm{Hom}_{\mathrm{G}_{\mathbf{Q}}}(\mathrm{R}(\mathrm{G}), \mathrm{J}(\overline{\mathbf{Q}}))/\mathrm{Hom}_{\mathrm{G}_{\mathbf{Q}}}(\mathrm{R}(\mathrm{G}), \overline{\mathbf{Q}}^*)\,.\,\mathrm{H}(\mathcal{K}^{\mathrm{S}}_0(\mathbf{Z}[\mathrm{G}]))$. La proposition précédente implique immédiatement que l'élément $\mathrm{V}^{\mathrm{S}}_{\mathrm{N/K}}$ appartient à $\prod_{p \in \overline{\mathrm{S}}} \mathrm{Im}\,\nu'_p$. Nous voulons interpréter ce résultat.

THEOREME 2.3. – *Il existe deux* $\mathbf{Z}[\mathrm{G}]$*-modules* M *et* N *localement libres en dehors de* S, *de type fini et sans* $\mathbf{Z}$*-torsion vérifiant :*

i) $\mathrm{M}_p = \mathrm{N}_p$ *si* $p \notin \overline{\mathrm{S}}$, M_p *et* N_p *sont des* $\mathbf{Z}_p[\mathrm{G}]$*-modules isomorphes si* $p \in \overline{\mathrm{S}}$

ii) $\eta_{\mathbf{Z}[\mathrm{G}]}(\mathrm{V}^{\mathrm{S}}_{\mathrm{N/K}}) = [\mathrm{M}] - [\mathrm{N}]$ *dans* $\widetilde{\mathcal{K}}^{\mathrm{S}}_0(\mathbf{Z}[\mathrm{G}])$.

Démonstration. – Ce résultat découle immédiatement des résultats de [7], § 1.

THEOREME 2.4. – *Pour tout idéal premier* $\mathfrak{q}$ *de* $\mathbf{Z}_N$, *on note* $G(\mathfrak{q})$ *le groupe de décomposition de* $\mathfrak{q}$ *dans* G. *Si pour tout idéal* $\mathfrak{q}$ *de* $\mathbf{Z}_N$, $G(\mathfrak{q})$ *est un groupe abélien, alors* $V^S_{N/K} = 1$.

Démonstration. – C'est une formulation plus précise du théorème III de [8].

3. Congruences.

Dans ce paragraphe, nous donnons deux généralisations aux extensions sauvagement ramifiées du théorème 6.1 de [1].

Soit ℓ un nombre premier. On désigne par $\operatorname{Ker} d_\ell$ le sous-groupe de $R(G)$ formé des éléments χ tels que $\chi(g) = 0$ pour les éléments de G dont l'ordre n'est pas divisible par ℓ. On dit que ℓ est modérément ramifié dans N sur K si les idéaux premiers de K au-dessus de ℓ sont modérément ramifiés dans N (i.e. le groupe G ne contient pas d'automorphismes sauvagement ramifiés en ℓ dans la terminologie de [8]).

On note $\mathfrak{L}$ la racine de l'idéal $\ell\overline{\mathbf{Z}}$ où $\overline{\mathbf{Z}}$ est la clôture intégrale de $\mathbf{Z}$ dans $\overline{\mathbf{Q}}$.

Soit μ le groupe des racines de l'unité et μ'_ℓ le groupe des racines de l'unité d'ordre premier à ℓ.

Soit $\mathfrak{p}$ un idéal premier de $\mathbf{Z}_K$ et $\mathfrak{q}$ un idéal premier de $\mathbf{Z}_N$ au-dessus de $\mathfrak{p}$. On note $G(\mathfrak{q})^0$ le groupe d'inertie de $\mathfrak{q}$ dans G. Si χ est le caractère d'un $\overline{\mathbf{Q}}[G]$-module V, on note $\chi^{G(\mathfrak{q})^0}$ le caractère du $\overline{\mathbf{Q}}[G]$-module $V^{G(\mathfrak{q})^0} = \{v \in V\,,\, g(v) = v\,,\ \forall g \in G(\mathfrak{q})^0\}$. On note $\operatorname{Ker}\chi = \{g \in G\,,\, g(v) = v\,,\ \forall v \in V\}$. On définit ainsi $\chi^{G(\mathfrak{q})^0}$ et $\operatorname{Ker}\chi$ pour tout $\chi \in R(G)$.

Pour tout $\chi \in R(G)$, l'élément $\operatorname{Det}_{\chi^{G(\mathfrak{q})^0}}(-F_{K,\mathfrak{p}}) \in \mu$ ne dépend ni du choix de l'idéal $\mathfrak{q}$ au-dessus de $\mathfrak{p}$ ni du relèvement dans $G(\mathfrak{q})$ du Frobenius $F_{K,\mathfrak{p}}$.

THEOREME 3.1. – *Pour tout idéal premier* $\mathfrak{p}$ *de* $\mathbf{Z}_K$ *et pour tout nombre premier* ℓ *modérément ramifié dans* N *sur* K, *ou n'appartenant pas à* $\mathfrak{p}$, *on a :*

$$\forall \chi \in \operatorname{Ker} d_\ell\,,\ \tau_{K,\mathfrak{p}}(\chi) \equiv \operatorname{Det}_{\chi^{G(\mathfrak{q})^0}}(-F_{K,\mathfrak{p}})^{-1} \quad \text{modulo} \quad \mathfrak{L}$$

où $\tau_{K,\mathfrak{p}}$ *est la somme de Gauss galoisienne locale.*

Pour la définition des sommes de Gauss galoisiennes locales le lecteur peut se reporter à [6], chap. II, § 4.

Démonstration. – Si $\mathfrak{p}$ est sauvagement ramifié, $\mathfrak{l}$ n'appartient pas à $\mathfrak{p}$ et le résultat se déduit de la proposition 1.8 de [8].

Sinon le résultat se déduit de [1] en remarquant que

$$y_{\mathfrak{p}}(\chi) = \operatorname{Det}_{\chi^{G(\mathfrak{q})^0}}(-F_{K,\mathfrak{p}})^{-1} .$$

COROLLAIRE 3.2. – *Il existe un élément* y *de* $\operatorname{Hom}_{G_{\mathbf{Q}}}(R(G), \mu)$ *tel que l'on ait :*

i) $\tau(\chi) \equiv y(\chi)$ *modulo* $\mathfrak{L}$, *pour tout* χ *de* $\operatorname{Ker} d_{\mathfrak{l}}$ *et tout* $\mathfrak{l}$ *modérément ramifié dans* N *sur* K ;

ii) $y(\chi) = 1$ *pour tout caractère* χ *symplectique de* G .

Démonstration. – On prend $y(\chi)$ égal au produit

$$\prod_{\mathfrak{p} \mid \Delta_{N/\mathbf{Q}}} \operatorname{Det}_{\chi^{G(\mathfrak{q})^0}}(-F_{K,\mathfrak{p}})^{-1}$$

où $\Delta_{N/\mathbf{Q}}$ est le discriminant de N sur $\mathbf{Q}$.

On a $\tau_{K,\mathfrak{p}}(\chi) = 1$ pour tout $\chi \in R(G)$ si $\mathfrak{p}$ ne divise pas $\Delta_{N/\mathbf{Q}}$. La deuxième assertion est évidente car si χ est un caractère symplectique, le déterminant de ce caractère est trivial et son degré est congru à 0 modulo 2.

Soit $R^s(G)$ le sous-groupe de R(G) formé des caractères symplectiques et soit $N_{K/\mathbf{Q}}(f_{K,\mathfrak{p}}(\chi))$ le nombre d'éléments de $\mathbf{Z}_K/f_{K,\mathfrak{p}}(\chi)$ où $f_{K,\mathfrak{p}}(\chi)$ est le conducteur d'Artin de χ en $\mathfrak{p}$.

COROLLAIRE 3.3. – *Soit* $W_{K,\mathfrak{p}}$ *la composante locale en* $\mathfrak{p}$ *de la constante* $W_{N/K}$ *de l'équation fonctionnelle des séries* L *d'Artin. Pour tout nombre premier* $\mathfrak{l}$, *modérément ramifié dans* N *sur* K , *on a la congruence suivante :* $W_{K,\mathfrak{p}}(\chi) \equiv N_{K/\mathbf{Q}}(f_{K,\mathfrak{p}}(\chi))^{-1/2}$ *modulo* $\mathfrak{L}$ *pour tout* χ *dans* $R^s(G) \cap \operatorname{Ker} d_{\mathfrak{l}}$.

Démonstration. – D'après le théorème 3.1, on a $\tau_{K,\mathfrak{p}}(\chi) \equiv 1$ modulo $\mathfrak{L}$ pour tout $\mathfrak{l}$ modérément ramifié dans N et pour tout $\chi \in R^s(G) \cap \operatorname{Ker} d_{\mathfrak{l}}$. Par définition on a :

$$W_{K,\mathfrak{p}}(\chi) = \tau_{K,\mathfrak{p}}(\chi)\, N_{K/\mathbf{Q}}(f_{K,\mathfrak{p}}(\chi))^{-1/2} .$$

Pour $\chi \in R^s(G)$, $W_{K,\mathfrak{p}}(\chi)$ est égal à 1 ou -1 ; on en déduit que $f_{K,\mathfrak{p}}(\chi)^{1/2}$ est une unité en $\mathfrak{L}$ et que $W_{K,\mathfrak{p}}(\chi) \equiv N_{K/\mathbf{Q}}(f_{K,\mathfrak{p}}(\chi))^{-1/2}$ modulo $\mathfrak{L}$.

Remarque. – Cette congruence définit la constante locale $W_{K,\mathfrak{p}}(\chi)$ pour tout caractère χ de $\operatorname{Ker} d_\ell \cap R^s(G)$ et ℓ différent de 2 .

COROLLAIRE 3.4. – *Pour tout idéal premier* $\mathfrak{p}$ *de* $\mathbf{Z}_K$ *et pour tout nombre premier* ℓ *modérément ramifié dans* N *sur* K, *on a :* $\forall \chi \in \operatorname{Ker} d_\ell$, $(W_{K,\mathfrak{p}}(\chi))^2 \equiv \operatorname{Det}_{\chi^{G(\mathfrak{q})^0}}(F_{K,\mathfrak{p}})^{-2}$ *modulo* $\mathfrak{L}$.

COROLLAIRE 3.5. – *Il existe une fonction* z *de* $\operatorname{Hom}_{G_{\mathbf{Q}}}(R(G), \mu)$ *telle que l'on ait :*

i) $W_{N/K}(\chi)^2 \equiv z(\chi)$ *modulo* $\mathfrak{L}$, *pour tout* χ *de* $\operatorname{Ker} d_\ell$ *et tout* ℓ *modérément ramifié dans* N *sur* K ;

ii) $z(\chi) = 1$ *pour tout caractère* χ *symplectique de* G .

Démonstration. – Le corollaire 3.5 se déduit du corollaire 3.4, comme le corollaire 3.2 s'est déduit du théorème 3.1. Le corollaire 3.4 se déduit du théorème 3.1 et du lemme suivant :

LEMME 3.7. – *Sous les hypothèses du théorème 3.1, on a la congruence* $N_{K/\mathbf{Q}}(f_{K,\mathfrak{p}}(\chi)) \equiv 1$ *modulo* $\mathfrak{L}$ *pour tout* $\chi \in \operatorname{Ker} d_\ell$.

Démonstration. – On se ramène comme dans le théorème 3.1 au cas où N est une extension abélienne de K et $\chi = \eta\nu - \eta$. Si ν n'est pas ramifié en $\mathfrak{p}$, $f_{K,\mathfrak{p}}(\chi) = 1$. Si ν et η sont tous les deux ramifiés en $\mathfrak{p}$, comme ν est d'ordre une puissance de ℓ et que ℓ est modérément ramifié dans N sur K , ℓ n'appartient pas à $\mathfrak{p}$. L'étude de la valuation de $f_{K,\mathfrak{p}}(\eta\nu)$ et $f_{K,\mathfrak{p}}(\eta)$ montre que $f_{K,\mathfrak{p}}(\eta\nu) = f_{K,\mathfrak{p}}(\eta)$ car ν est modérément ramifié. Si η est non ramifié et ν est ramifié, $f_{K,\mathfrak{p}}(\eta\nu) = f_{K,\mathfrak{p}}(\nu)$. Le caractère ν est modérément ramifié, d'où l'ordre de ν divise le cardinal de $\mathbf{Z}_K/\mathfrak{p}$; donc : $N_{K/\mathbf{Q}}(f_{K,\mathfrak{p}}(\nu)) \equiv 1$ modulo $\mathfrak{L}$.

Remarque. – On peut montrer que $f_{K,\mathfrak{p}}(\chi)$ est un carré pour tout $\chi \in R^s(G) \cap \operatorname{Ker} d_\ell$ et pour tout nombre premier ℓ différent de 2 et modérément ramifié dans N sur K .

4. Description de $\dot{V}^S_{N/K}$.

On déduit de la proposition 1.7 et du théorème I de [8] l'égalité $\mathrm{Ext}^{\mathfrak{M}^S}_{\mathbf{Z}[G]}(V^S_{N/K}) = 1$; on veut maintenant préciser ce résultat.

Soit $\mathfrak{M}^S$ un ordre vérifiant les conditions du théorème 2.1, $\mathfrak{F}$ le conducteur central de $\mathfrak{M}^S$ dans $\mathbf{Z}[G]$ et $\mathrm{Rac}(\mathfrak{F})$ sa racine. On définit l'ordre $\mathfrak{A}^S$ de $\mathbf{Z}$ dans $\mathbf{Q}[G]$ par l'égalité :

$$\mathfrak{A}^S = \mathbf{Z}[G] + \mathrm{Rac}(\mathfrak{F})\mathfrak{M}^S .$$

Cet ordre contient $\mathbf{Z}[G]$; il est en général strictement contenu dans $\mathfrak{M}^S$. De plus pour tout p dans S, $\mathfrak{A}^S_p$ est égal à $\mathbf{Z}_p[G]$.

THEOREME 4.1. – *Soit* S *un ensemble fini de nombres premiers de* $\mathbf{Z}$ *contenant les nombres premiers sauvagement ramifiés dans* N/K ; *alors, on a :*

$$\mathrm{Ext}^{\mathfrak{A}^S}_{\mathbf{Z}[G]}(V^S_{N/K}) = 1 .$$

On a donc l'égalité :

$$\mathrm{Ext}^{\mathfrak{A}^S}_{\mathbf{Z}[G]}(U^S_{N/K}) = t^S\ (W_{N/K}) .$$

L'énoncé du théorème suivant est une traduction du théorème 4.1 ([7], proposition 1.2).

THEOREME 4.2. – *Il existe des* $\mathfrak{A}^S$*-modules,* M , M′ *et* M″ *de type fini, sans* $\mathbf{Z}$*-torsion, localement libres pour tout nombre premier* p *de* $\mathbf{Z}$ *n'appartenant pas à* S *et deux suites exactes :*

$$0 \longrightarrow M' \longrightarrow M \oplus (\mathfrak{A}^S \otimes_{\mathbf{Z}[G]} \mathbf{Z}_N) \oplus (\mathfrak{A}^S \otimes_{\mathbf{Z}[G]} \mathbf{Z}_N) \longrightarrow M'' \longrightarrow 0$$

$$0 \longrightarrow M' \longrightarrow M \oplus (\mathfrak{A}^S)^r \oplus (\mathfrak{A}^S)^r \longrightarrow M'' \longrightarrow 0$$

où r *est le rang de* $\mathbf{Z}_N$ *sur* $\mathbf{Z}[G]$ $(r = [K : \mathbf{Q}])$.

Remarque. – Si l'extension N/K est modérément ramifiée, on peut prendre S vide, on retrouve ainsi le théorème 6.2 de [1].

Démonstration. – On déduit des paragraphes 2 et 3 que $\mathrm{Ext}^{\mathfrak{M}^S}_{\mathbf{Z}[G]}(V^S_{N/K})$ est représenté par la classe de l'élément

$$f \in \mathrm{Hom}_{G_{\mathbf{Q}}}(R(G), J(\overline{\mathbf{Q}}))$$

vérifiant les conditions (5) de la proposition 3.2.

Soit y l'élément de $\mathrm{Hom}_{G_{\mathbf{Q}}}(R(G), \mu)$ défini dans le corollaire 3.2. Comme $y(\chi) = 1$ pour $\chi \in R^s(G)$, l'élément g égal à fy est un nouveau représentant de $\mathrm{Ext}_{\mathbf{Z}[G]}^{\mathfrak{A}^S}(V_{N/K}^S)$. On a les congruences :

$$g(\chi)_{\mathfrak{L}} \equiv 1 \text{ modulo } \mathfrak{L}\,, \quad \forall \chi \in \mathrm{Ker}\, d_{\mathfrak{L}} \quad \text{et} \quad \forall \mathfrak{L} \in \overline{S}\,.$$

On déduit de [2], qu'il existe $\alpha_{\mathfrak{L}} \in (\mathfrak{A}_{\mathfrak{L}}^S)^*$ tel que l'on ait :

$$g(\chi)_{\mathfrak{L}} = \mathrm{Det}_{\chi}(\alpha_{\mathfrak{L}})\,, \ \forall \chi \in R(G)\,, \ \forall \mathfrak{L} \in \overline{S}.$$

L'homomorphisme g appartient donc à $H(\mathcal{K}_0^S(\mathfrak{A}^S))$.

Remarque. – Notons $\mathfrak{U}^S$ l'ordre de $\mathbf{Z}$ dans $\mathbf{Q}[G]$ défini par

$$\mathfrak{U}_p^S = \mathbf{Z}_p[G] + \mathrm{Rac}(\mathfrak{F})\mathfrak{M}_p \quad \text{pour } p \notin S$$

$$\mathfrak{U}_p^S = \mathfrak{M}_p \quad \text{pour } p \in S\,.$$

Le $\mathfrak{U}^S$-module $\mathfrak{U}^S \mathbf{Z}_N$ est localement libre ; on déduit facilement de la démonstration du théorème 5 que l'élément défini par $\mathfrak{U}^S \mathbf{Z}_N$ dans $\mathcal{CL}(\mathfrak{U}^S)$ appartient au sous-groupe $\prod_{p \in S} \mathrm{Im}\, \nu'_p$. Ce résultat généralise le théorème 1, (ii) de [4].

Pour tout p, on a un homomorphisme, noté $\mathrm{Ext}_{\mathbf{Z}_p[G]}^{\mathfrak{A}_p^S}$ de $\mathcal{K}_{0,\mathrm{rel}}(\mathbf{Z}_p[G])$ sur $\mathcal{K}_{0,\mathrm{rel}}(\mathfrak{A}_p^S)$ (voir [7], § 1, pour la définition de ces groupes de Grothendieck relatifs).

On note $\mathcal{D}^t(\mathbf{Z}_p[G], \mathfrak{A}_p^S)$ son noyau. On a un diagramme commutatif (voir [8], théorème 1.14)

$$\begin{tikzcd}
0 \arrow[r] & \prod_{p \in \overline{S}} \mathcal{D}^t(\mathbf{Z}_p[G], \mathfrak{A}_p^S) \arrow[r] \arrow[d] & \bigoplus_{p \in \overline{S}} \mathcal{K}_{0,\mathrm{rel}}(\mathbf{Z}_p[G]) \arrow[r] \arrow[d, "\bigoplus_{p \in \overline{S}} \nu_{\mathbf{Z}_p[G]}"] & \bigoplus_{p \in \overline{S}} \mathcal{K}_{0,\mathrm{rel}}(\mathfrak{A}_p^S) \arrow[r] \arrow[d, "\bigoplus_{p \in \overline{S}} \nu_{\mathfrak{A}_p^S}"] & 0 \\
0 \arrow[r] & \mathcal{D}(\mathbf{Z}[G], \mathfrak{A}^S) \arrow[r] & \widetilde{\mathcal{K}}_0^S(\mathbf{Z}[G]) \arrow[r] & \widetilde{\mathcal{K}}_0^S(\mathfrak{A}^S) \arrow[r] & 0\,.
\end{tikzcd}$$

On vient donc de démontrer que $V_{N/K}^S$ appartient à l'image de $\bigoplus_{p \in \overline{S}} \nu_{\mathbf{Z}_p[G]}$. On en déduit une décomposition $V_{N/K}^S = \prod_{p \in \overline{S}} V_{N/K,p}^S$ dans laquelle $V_{N/K,p}^S$ appartient à l'image de $\nu_{\mathbf{Z}_p[G]}$. On déduit de la proposition 4.3 de [3] la proposition suivante.

PROPOSITION 4.3. – *L'ordre de* $V_{N/K,p}^S$ *est une puissance de* p.

On a donc décomposé ainsi $V^S_{N/K}$ en ses p-composantes. Pour tout nombre premier p, on note n_p l'exposant de p dans Card G. L'ordre de $V^S_{N/K}$ divise donc $\prod_{p\in\overline{S}} p^{n_p}$. Le paragraphe suivant a pour but de donner une meilleure majoration de l'ordre de $V^S_{N/K}$.

5. Majoration de l'ordre de $V^S_{N/K}$.

Dans ce paragraphe on majore l'ordre de $V^S_{N/K}$ et on donne des exemples d'extension N de K et de familles S de nombres premiers de $\mathbf{Z}$ pour lesquelles $V^S_{N/K}$ est égal à 1.

Si $S \supset S'$, on remarque que $V^S_{N/K}$ est l'image de $V^{S'}_{N/K}$ par l'homomorphisme naturel de $\mathcal{K}^{S'}_0(\mathbf{Z}[G])$ sur $\mathcal{K}^S_0(\mathbf{Z}[G])$. On en déduit que l'égalité $V^{S'}_{N/K} = 1$ implique l'égalité $V^S_{N/K} = 1$. Si S est égal à l'ensemble des diviseurs premiers de l'ordre de G, l'égalité $V^S_{N/K} = 1$ est une conséquence du théorème 2.1.

Soit X_G une famille de sous-groupes de G et soit Ind l'application $\prod_{H\in X_G} R_{\mathbf{Q}}(H) \longrightarrow R_{\mathbf{Q}}(G)$ définie par

$$\mathrm{Ind}((x_H)_{H\in X_G}) = \sum_{H\in X_G} \mathrm{Ind}^G_H\, x_H \quad \text{où } R_{\mathbf{Q}}(G)$$

désigne le sous-groupe de R(G) des caractères rationnels sur $\mathbf{Q}$.

L'exemple le plus important est donné par l'ensemble des groupes $\mathbf{Q}$-élémentaires.

THEOREME 5.1. – *Soit* X_G *une famille de sous-groupes de* G *telle que l'homomorphisme* Ind *soit surjectif. Pour tout* $p \in \overline{S}$, *l'ordre de* $V^S_{N/K,p}$ *divise le plus petit commun multiple des ordres des éléments* $V^S_{N/N^H,p}$ *lorsque* H *parcourt* X_G.

COROLLAIRE 5.2. – *Les deux propositions suivantes sont équivalentes :*

i) $V^S_{N/K,p} = 1$

ii) $V^S_{N/L,p} = 1$ *pour toute sous-extension galoisienne* L *de* N, *contenant* K, *dont le groupe de Galois appartient à* X_G.

Le théorème 5.1 est une conséquence du lemme suivant :

LEMME 5.3.

1) *Pour tout sous-groupe* H *de* G, *on a :*

$$\mathrm{Res}_{\mathbf{Z}[G]}^{\mathbf{Z}[H]}(\eta_{\mathbf{Z}[G]}(V_{N/K}^{S})) = \eta_{\mathbf{Z}[H]}(V_{N/N^H}^{S}).$$

2) *Pour tout sous-groupe distingué* H *de* G, *on a :*

$${}^t\theta^*(\eta_{\mathbf{Z}[G]}(V_{N/K}^{S})) = \eta_{\mathbf{Z}[G/H]}(V_{N^H/K}^{S})$$

où les applications $\mathrm{Res}_{\mathbf{Z}[G]}^{\mathbf{Z}[H]}$ *(resp.* ${}^t\theta^*$*) de* $\widetilde{\mathcal{K}}_0^S(\mathbf{Z}[G])$ *dans* $\widetilde{\mathcal{K}}_0^S(\mathbf{Z}[H])$ *(resp.* $\widetilde{\mathcal{K}}_0^S(\mathbf{Z}[G/H])$*) sont celles définies dans* [7], § 5, *(voir propositions 5.4 et 5.5).*

Démonstration. – Nous démontrons la première partie et nous laissons au lecteur la démonstration de la deuxième partie. Si $f \in \mathrm{Hom}_{G_{\mathbf{Q}}}(R(G), J(\overline{\mathbf{Q}}))$ représente $V_{N/K}^S$, l'application $\rho(f)$ défini par: $\forall \chi \in R(H)$, $\rho(f)(\chi) = f(\mathrm{Ind}_H^G \chi)$ représente $\mathrm{Res}_{\mathbf{Z}[G]}^{\mathbf{Z}[H]}(\eta_{\mathbf{Z}[G]}(V_{N/K}^S))$ ([7], proposition 5.4). Il est clair que

$$\mathrm{Res}_{\mathbf{Z}[G]}^{\mathbf{Z}[H]}(\eta_{\mathbf{Z}[G]}(U_{N/K}^{S})) = \eta_{\mathbf{Z}[H]}(U_{N/N^H}^{S}).$$

Il suffit donc de montrer l'égalité $\rho(t^S(W_{N/K})) = t^S(W_{N/N^H})$. Or $\rho(t^S(W_{N/K}))$ est représenté par l'homomorphisme

$$\chi \longrightarrow W'_{N/K}(\mathrm{Ind}_H^G(\chi)) \quad \text{pour} \quad \chi \in R(H).$$

On note u l'élément de $H(\mathcal{K}_0^S(\mathbf{Z}[H]))$ défini par

$$u(\chi) = W'_{N/K}(\mathrm{Ind}_H^G(\chi)),$$

(resp. 1) pour tout caractère χ de R(H) irréductible et non symplectique (resp. symplectique). Il suffit de démontrer l'égalité : $\rho(W'_{N/K}) = u\, W'_{N/N^H}$. Ces applications coïncident sur l'ensemble des caractères irréductibles et symplectiques de G). Pour tout χ est irréductible symplectique, $\mathrm{Ind}_H^G(\chi)$ se décompose en une somme $\psi_1 + \psi_2$ où ψ_1 (resp. ψ_2) est orthogonal (resp. somme de caractères irréductibles et symplectiques de G). Pour tout $\omega \in G_{\mathbf{Q}}$, on a :

$$\rho(W'_{N/K})(\chi^\omega) = W'_{N/K}(\mathrm{Ind}_H^G(\chi^\omega)) = W_{N/K}(\psi_2^\omega).$$

Comme $W_{N/K}(\psi_1^\omega) = 1$ ([5]), on a :

$$\rho(W'_{N/K})(\chi^\omega) = W_{N/K}(\mathrm{Ind}_H^G(\chi^\omega)).$$

La formule d'induction pour les constantes $W_{N/K}$ entraîne l'égalité :

$$\rho(W'_{N/K})\,(\chi^{\omega}) = W_{N/N^H}(\chi^{\omega}),$$

c'est-à-dire :

$$\rho(W'_{N/K})\,(\chi)_{p^{\omega}_{\infty}} = W_{N/N^H}(\chi)_{p^{\omega}_{\infty}}\,.$$

Ceci démontre la première partie du lemme.

Démonstration du théorème 5.1. – L'anneau $R_{\mathbf{Q}}(G)$ opère sur le groupe $\mathrm{Hom}_{G_{\mathbf{Q}}}(R(G)\,,\,J(\overline{\mathbf{Q}}))$ de la façon suivante :

$\forall\theta \in R_{\mathbf{Q}}(G)\,,\ \forall\chi \in R(G)\,,\ \forall f \in \mathrm{Hom}_{G_{\mathbf{Q}}}(R(G)\,,\,J(\overline{\mathbf{Q}}))\,,\ (\theta f)\,(\chi) = f(\chi\theta).$

Pour cette opération le groupe (1) a une structure de module de Frobenius ([9], chap. II). Comme l'application Ind est surjective, on a : $1 = \sum_{H\in X_G} \mathrm{Ind}_H^G(\sigma_H)$ où $\sigma_H \in R_{\mathbf{Q}}(H)$. En écrivant les caractères χ de G sous la forme $\chi = \sum_{H\in X_G} \mathrm{Ind}_H^G(\sigma_H\,\mathrm{Res}_G^H(\chi))$, on en déduit que l'ordre de $V^S_{N/K,p}$ divise le p.p.c.m. des ordres de $\rho_{G/H}(V^S_{N/K,p})$ pour H parcourant X_G ; il divise donc le p.p.c.m des ordres de $V^S_{N/N^H,p}$ pour H parcourant X_G.

PROPOSITION 5.4. – *Si G est un groupe $\mathbf{Q}$-ℓ-élémentaire, $V^S_{N/K,p} = 1$ pour tout nombre premier p différent de ℓ.*

Démonstration. – Pour tout sous-groupe abélien H de G, on a $V^S_{N/N^H} = 1$ ([8], théorème III). On en déduit que $V^S_{N/K}$ divise l'exposant d'Artin de G ; or si G est $\mathbf{Q}$-ℓ-élémentaire, on sait que l'exposant d'Artin de G est égal à une puissance de ℓ ; donc pour p différent de ℓ, $V^S_{N/K,p}$ qui est la p-composante de $V^S_{N/K}$ est égal à 1.

On note $|G|$ l'ordre du groupe G et pour tout nombre premier p, n_p l'exposant de p dans $|G|$. On désigne par $|G|_S$ l'entier $\prod_{p\in \overline{S}} p^{n_p}$. On sait que l'ordre de $V^S_{N/K}$ divise $|G|_S$.

On définit $B_0(G)_S$ par l'égalité :

$$B_0(G)_S = |G|_S/\text{p.g.c.d.}\,(\{\chi(1)\,,\,|G|_S\})$$

où χ parcourt l'ensemble des caractères irréductibles non abéliens de G. L'entier $\chi(1)$ divise l'indice du centre de G dans G.

Pour tout entier n, on pose $n' = n\,.\prod_{p|n} p^{-1}$.

THEOREME 5.5. — *L'ordre de* $V^S_{N/K}$ *divise* $B_0(G)'_S$.

Démonstration. — Soit G^{ab} le quotient de G par son sous-groupe des commutateurs. On déduit du lemme 5.3 et du théorème III de [8] que $V^S_{N/K}$ appartient au noyau de l'homomorphisme de $\widetilde{\mathcal{K}}^S_0(\mathbf{Z}[G])$ sur $\widetilde{\mathcal{K}}^S_0(\mathbf{Z}[G^{ab}])$. Plus précisément $V^S_{N/K,p}$ appartient à l'image par ν_p du noyau de l'homomorphisme de $\mathcal{K}_{0,\mathrm{rel}}(\mathbf{Z}_p[G])$ dans $\mathcal{K}_{0,\mathrm{rel}}(\mathbf{Z}[G^{ab}])$. Le théorème découle du lemme 6 de [2].

COROLLAIRE 5.6. — *L'ordre de* $V^S_{N/K,p}$ *divise* $\mathrm{Sup}(1, p^{n_p-2})$.

Démonstration. — D'après le théorème 5.1 et la proposition 5.4, il suffit de démontrer ce corollaire pour les groupes $\mathbf{Q}$-p-élémentaires ; dans ce cas, on sait que la p-composante de $B_0(G)_S$ divise p^{n_p-1}.

THEOREME 5.7. — *Les deux propositions suivantes sont équivalentes :*

1) $(V^S_{N/K,p})^2 = 1$

2) $(V^S_{N/L,p})^2 = 1$ *pour toute sous-extension galoisienne* L *de* N, *contenant* K, *dont le groupe de Galois est* K-*p*-*élémentaire.*

Démonstration. — Soit $\mathrm{Res}^{\mathbf{Z}}_{\mathbf{Z}_K}$ l'homomorphisme de restriction de $\widetilde{\mathcal{K}}^S_0(\mathbf{Z}_K[\Gamma])$ dans $\widetilde{\mathcal{K}}_0(\mathbf{Z}[\Gamma])$; il est clair que $U^S_{N/K}$ appartient à l'image de l'homomorphisme $\mathrm{Res}^{\mathbf{Z}}_{\mathbf{Z}_K}$. Comme $t^S(W^S_{N/K})^2 = 1$, on en déduit que $(V^S_{N/K})^2$ appartient à l'image de l'application $\eta^{-1}_{\mathbf{Z}[G]} \circ \mathrm{Res}^{\mathbf{Z}}_{\mathbf{Z}_K}$. Le groupe $\mathcal{K}^S_0(\mathbf{Z}_K[\Gamma])$ a une structure de $R_K(G)$-module de Frobenius. Si X_G désigne l'ensemble des sous-groupes K-p-élémentaire de G, l'homomorphisme Ind est surjectif. La technique utilisée précédemment montre donc que $(V^S_{N/K})^2 = 1$, si le résultat est vrai pour les groupes K-p-élémentaires.

Exemples. — On a $V^S_{N/K} = 1$, c'est-à-dire $U^S_{N/K} = t^S(W_{N/K})$ dans les cas particuliers suivants :

1) G est diédral (resp. quaternionien) d'ordre $2m$ (resp. $4m$) avec m impair.

2) G est diédral ou quaternionien et 2 appartient à S.

3) L'ordre de G est sans facteur cubique.

4) G est produit semi-direct d'un sous-groupe distingué cyclique A d'ordre m par un sous-groupe abélien dont l'ordre est premier à m et qui opère fidèlement sur A.

Dans les cas 1 et 4, $B_0(G)_S$ est un diviseur de m ou de $2m$; donc l'ordre de $V^S_{N/K}$ divise m'. Dans le cas 2, si l'ordre de G est de la forme $2^{n_2}n$ (avec $(n, 2) = 1$), alors $B_0(G)_S$ divise n, donc l'ordre de $V^S_{N/K}$ divise n'. Dans ces trois cas, l'ordre de $V^S_{N/K}$ est impair. Or on déduit du théorème III de [8] que l'ordre de $V^S_{N/K}$ divise l'exposant d'Artin de G. Or cet exposant est pair dans les cas 1 et 2 et premier à m dans le cas 4. L'exemple 3 est une conséquence du corollaire 5.4.

6. Dualité.

Le but de ce paragraphe est de généraliser les résultats de M.J. Taylor ([12]).

Le groupe $\widetilde{\mathcal{K}}_0^S(\mathbf{Z}[G])$ est muni d'une involution, notée $x \longmapsto \overline{x}$. Si $f \in \mathrm{Hom}_{G_{\mathbf{Q}}}(R(G), J(\overline{\mathbf{Q}}))$ représente x, $\overline{x}$ est représenté par l'homomorphisme $\chi \longrightarrow f(\overline{\chi})$ où $\overline{\chi}$ désigne le conjugué complexe de χ.

THEOREME 6.1. — *Pour tout ensemble* S *de nombres premiers contenant les idéaux premiers sauvagement ramifiés dans* N *sur* K, *on a :* $U^S_{N/K} \cdot \overline{U^S_{N/K}} = 1$.

Dans [8], on a construit à partir de l'application de trace de N sur K une forme hermitienne, noté $\mathrm{Tr}_{N/K}$. Puis on a défini le discriminant de $\mathbf{Z}_N$ par rapport à cette forme hermitienne, comme étant un élément du groupe de Grothendieck $\mathcal{K}_{0,\mathrm{rel}}(\mathbf{Z}_K[G])$ de la catégorie des $\mathbf{Z}_K[G]$-modules de type fini, de $\mathbf{Z}$-torsion, quotients de deux modules localement libres en dehors de S. Soit ν l'homomorphisme de $\mathcal{K}_{0,\mathrm{rel}}(\mathbf{Z}[G])$ dans $\widetilde{\mathcal{K}}_0^S(\mathbf{Z}[G])$, ([7], § 1). Il est immédiat à partir des définitions des paragraphes 2 et 3 de [8] que l'on a la proposition suivante :

PROPOSITION 6.2. — *On a les égalités :*

$$\eta_{\mathbf{Z}[G]}(U^S_{N/K} \cdot \overline{U^S_{N/K}}) = \nu(\mathrm{Res}^{\mathbf{Z}}_{\mathbf{Z}_K}(\Delta_{\mathrm{Tr}_{N/K}}(\mathbf{Z}_N))) = \nu(\Delta_{\mathrm{Tr}_{N/\mathbf{Q}}}(\mathbf{Z}_N)).$$

Remarque. – La proposition 2.11 de [8], montre que :

$$\forall \chi \in R(G) \quad \mathrm{Res}^{\mathbf{Z}}_{\mathbf{Z}_K}(\Delta_{\mathrm{Tr}_{N/K}}(\mathbf{Z}_N))\,(\chi)\;\Delta_{K/\mathbf{Q}}^{\chi(1)} = \Delta_{\mathrm{Tr}_{N/\mathbf{Q}}}(\mathbf{Z}_N)\,(\chi)$$

où $\Delta_{K/\mathbf{Q}}$ est le discriminant de K sur $\mathbf{Q}$ (par rapport à l'application de trace de K sur $\mathbf{Q}$).

Comme l'application $\chi \longrightarrow \Delta_{K/\mathbf{Q}}^{\chi(1)}$ appartient à $\mathrm{Hom}_{G_{\mathbf{Q}}}(R(G), \overline{\mathbf{Q}}^*)$ on a la deuxième égalité.

COROLLAIRE 6.3. – *Soit* $\mathcal{D}_{N/K}^{-1}$ *la codifférente de* N *sur* K ; *on a* $[\mathbf{Z}_N] = [\mathcal{D}_{N/K}^{-1}]$ *dans* $\mathcal{K}_0^S(\mathbf{Z}[G])$.

Démonstration. – On vérifie $\Delta_{\mathrm{Tr}_{N/K}}(\mathbf{Z}_N) = \chi_{\mathbf{Z}_K[G]}(\mathbf{Z}_N, \mathcal{D}_{N/K}^{-1})$. Pour cela on se ramène au cas local et on utilise le fait que $\mathcal{D}_{N/K}^{-1}$ est isomorphe à $\mathrm{Hom}_{\mathbf{Z}_K}(\mathbf{Z}_N, \mathbf{Z}_K)$.

Le théorème 6.1 est une conséquence immédiate de la proposition 6.2 et du théorème suivant :

Soit $\mathfrak{F}_{K,\mathfrak{p}}$ l'homomorphisme de R(G) dans $\mathbf{Q}^*$ défini dans [8], $(\mathfrak{F}_{K,\mathfrak{p}}(\chi) = N_{K/\mathbf{Q}}(f_{K,\mathfrak{p}}(\chi)))$. En plongeant $\overline{\mathbf{Q}}^*$ dans $J(\overline{\mathbf{Q}})$, on obtient à partir de $\mathfrak{F}_{K,\mathfrak{p}}$ un élément de $\mathrm{Hom}_{G_{\mathbf{Q}}}(R(G), J(\overline{\mathbf{Q}}))$. On pose $\mathcal{F}_K = \prod_{\mathfrak{p}} \mathfrak{F}_{K,\mathfrak{p}}$.

THEOREME 6.4. – *L'élément* $\mathrm{Res}^{\mathbf{Z}}_{\mathbf{Z}_K}(\Delta_{\mathrm{Tr}_{N/K}}(\mathbf{Z}_N))$ *est représenté par* $\mathcal{F}_K$.

La démonstration de ce théorème se fait en deux étapes données par les deux propositions suivantes :

PROPOSITION 6.5. – *Soit* $\mathfrak{p}$ *un idéal premier de* $\mathbf{Z}_K$, *et* p *tel que* $p\mathbf{Z} = \mathfrak{p} \cap \mathbf{Z}$ *l'élément* $\mathrm{Res}^{\mathbf{Z}_p}_{\mathbf{Z}_{K_\mathfrak{p}}}(\Delta_{\mathrm{Tr}_{N_\mathfrak{p}/K_\mathfrak{p}}}(\mathbf{Z}_{N_\mathfrak{p}}))$ *est représenté par la* p*-composante de* $\mathfrak{F}_{K,\mathfrak{p}}$.

Démonstration. – On suppose que K est un corps local. Si $\mathfrak{p}$ est modérément ramifié, on utilise le fait que

$$\Delta_{\mathrm{Tr}_{N/K}}(\mathbf{Z}_N) = \chi_{\mathbf{Z}_K[G]}(\mathbf{Z}_N, \mathcal{D}_{N/K}^{-1})^{-1}$$

et on démontre que

$$\chi_{\mathbf{Z}_K[G]}(\mathbf{Z}_N, \mathcal{D}_{N/K}^{-1})^{-1} = \chi_{\mathbf{Z}_K[G]}(\mathbf{Z}_K[G], T)$$

où T est le module de Swan défini par M.J. Taylor ([12], § 4). Si $\mathfrak{p}$ est sauvagement ramifié le résultat se démontre comme la proposition 4.5 de [8] en utilisant le théorème de Brauer ; on se ramène ainsi à une extension abélienne modérément ramifiée.

PROPOSITION 6.6. — *Pour tout nombre premier* ℓ *et tout idéal premier* $\mathfrak{p}$ *de* $\mathbf{Z}_K$ *tels que* $\ell \notin \mathfrak{p}$, *la* ℓ*-composante de* $\mathfrak{F}_{K,\mathfrak{p}}$ *appartient à* $\mathrm{Det}(\mathbf{Z}_\ell[G]^*)$.

La démonstration découle des lemmes suivants établis sous les hypothèses de la proposition 6.6.

LEMME 6.7. — *Si* G *est abélien, la* ℓ *composante de* $\mathfrak{F}_{K,\mathfrak{p}}$ *appartient à* $\mathrm{Det}(\mathbf{Z}_\ell[G]^*)$.

Démonstration. — On se ramène comme dans la proposition 4.6 de [8] au cas où N est un corps de classes de rayon $\mathfrak{p}^n$. Soit $t_\mathfrak{p}(N/K) = \sum_{i=1}^{\ell} t^i_\mathfrak{p}(N/K)$ où $t^i_\mathfrak{p}(N/K)$ est l'élément de $\overline{\mathbf{Q}}[G]$ défini dans [8], § 1. On a $\mathfrak{F}_{K,\mathfrak{p}} = \mathrm{Det}(t_\mathfrak{p}(N/K) . \overline{t_\mathfrak{p}(N/K)})$ (si $\lambda = \sum_g \lambda_g g$, on note $\overline{\lambda}$ l'élément $\sum_g \lambda_g g^{-1}$). Comme $\ell \notin \mathfrak{p}$, $\mathfrak{F}_{K,\mathfrak{p}}(\chi)$ est une unité pour tout $\chi \in R(G)$. On montre que $t_\mathfrak{p}(N/K)\, \overline{t_\mathfrak{p}(N/K)}$ appartient à $\mathbf{Z}_\ell[G]$. Donc $t_\mathfrak{p}(N/K)\, \overline{t_\mathfrak{p}(N/K)}$ appartient à $\mathbf{Z}_\ell[G]^*$.

LEMME 6.8. — *Si* $\mathfrak{p}$ *est modérément ramifié, la* ℓ*-composante de* $\mathfrak{F}_{K,\mathfrak{p}}$ *appartient à* $\mathrm{Det}(\mathbf{Z}_\ell[G]^*)$.

Démonstration. — On utilise le fait que

$$\mathfrak{F}_{K,\mathfrak{p}}(\chi) = \tau_{K,\mathfrak{p}}(\chi) \cdot \tau_{K,\mathfrak{p}}(\overline{\chi}) \det_\chi(-1)$$

et les résultats de M.J. Taylor, [13], théorème 2 (b) et théorème 6.

LEMME 6.9. — *Si* $\mathfrak{p}$ *est sauvagement ramifié, la* ℓ*-composante de* $\mathfrak{F}_{K,\mathfrak{p}}$ *appartient à* $\mathrm{Det}(\mathbf{Z}_\ell[G]^*)$.

Démonstration. — On déduit tout d'abord du lemme 3.7 et de la remarque 1 suivant ce lemme que l'ordre de $\mathfrak{F}_{K,\mathfrak{p}}$ est une puissance de ℓ. On déduit du lemme 6.7 que l'ordre de $\mathfrak{F}_{K,\mathfrak{p}}$ divise l'exposant d'Artin de G. En utilisant le fait que $\mathcal{K}_{0,\mathrm{rel}}(\mathbf{Z}_\ell[G])$ est un module de Frobenius et que l'application qui à $\chi \in R(G)$

associe $N_{K/\mathbf{Q}}(\Delta_{\mathfrak{p}}(F/K))^{\chi(1)}$ où $\Delta_{\mathfrak{p}}(F/K)$ est la $\mathfrak{p}$ -composante du discriminant de F sur K, pour F extension de K contenue dans N, appartient à $\mathrm{Det}(\mathbf{Z}_{\ell}[G]^*)$, on se ramène au cas où G est $\mathbf{Q}$-élémentaire. Les conditions sur l'ordre de $\mathfrak{F}_{K,\mathfrak{p}}$ entraînent qu'il suffit de traiter le cas où G est $\mathbf{Q}$-ℓ-élémentaire ; la définition de $\mathfrak{F}_{K,\mathfrak{p}}$ permet de se ramener au cas où G est le groupe de décomposition d'un relèvement premier de $\mathfrak{p}$ dans N.

Pour achever la démonstration de ce lemme nous utilisons les techniques de ([13], § 7) ou ([3]).

Le groupe G est le produit semi-direct d'un sous-groupe cyclique et distingué H d'ordre m premier à ℓ par un sous-groupe L d'ordre une puissance de ℓ. Les caractères irréductibles de G sont de la forme $\mathrm{Ind}_{HL_\chi}^{G}(\chi\varphi)$ où χ (resp. φ) est un caractère de H (resp. irréductible de L_χ) où L_χ est le sous-groupe d'isotropie de χ. Compte tenu de [13], il nous suffit de démontrer l'existence d'un élément α de $(\mathbf{Z}_{\ell}\otimes_{\mathbf{Z}}\mathbf{Z}(\chi)\,[L_\chi])^*$ tel qu'on ait :

$$\mathrm{Det}_{\varphi}(\alpha) = \mathfrak{F}_{K,\mathfrak{p}}(\mathrm{Ind}_{HL_\chi}^{G}(\chi\varphi))$$

pour tout caractère irréductible φ de L_χ, où χ est un caractère fidèle de H, $\mathbf{Z}(\chi)$ l'anneau des entiers de l'extension de $\mathbf{Q}$ obtenue par adjonction des valeurs de χ et $\mathbf{Z}(\chi)\,[L_\chi]$ l'algèbre du groupe L_χ à coefficients dans $\mathbf{Z}(\chi)$. Si χ est trivial, G est d'ordre premier à p donc ne contient pas d'automorphismes sauvagement ramifiés et le résultat se déduit du lemme 6.8.

Soient $N(\mathfrak{p})$ le cardinal de $\mathbf{Z}_K/\mathfrak{p}$ et $n_\chi(\varphi,\mathfrak{p})$ l'entier défini par l'égalité :

$$n_\chi(\varphi,\mathfrak{p}) = \langle \mathrm{Ind}_{HL_\chi}^{G}(\chi\varphi)\,,\,a_G\rangle\,,$$

où a_G désigne le caractère d'Artin de G et $\langle\ ,\ \rangle$ le produit scalaire de caractères. Nous en déduisons :

$$\mathfrak{F}_{K,\mathfrak{p}}(\mathrm{Ind}_{HL_\chi}^{G}(\chi\varphi)) = N(\mathfrak{p})^{n_\chi(\varphi,\mathfrak{p})}\,.$$

Nous déduisons de ([10], chap. VI, proposition 2), et de la formule de réciprocité de Frobenius l'égalité :

$$n_\chi(\varphi,\mathfrak{p}) = \sum_{i=0}^{\infty}\,[G_0 : G_i]^{-1}\,\langle \mathrm{Res}_{G}^{G_i}(\mathrm{Ind}_{HL_\chi}^{G}(\chi\varphi))\,,\,u_{G_i}\rangle$$

où G_i désigne le $i^{\text{ème}}$ groupe de ramification et u_{G_i} le caractère d'augmentation de G_i. Le caractère χ est fidèle sur H et pour tout entier $i \geqslant 1$ le groupe G_i est un sous-groupe de H ; nous en déduisons :

$$\langle \mathrm{Res}_G^{G_i}(\mathrm{Ind}_{HL_\chi}^G(\chi\varphi)), u_{G_i}\rangle = [G : HL_\chi]\ \varphi(1)$$

(resp. 0) si $G_i \neq \{1\}$ (resp. $= \{1\}$), d'où :

$$n_\chi(\varphi, \mathfrak{p}) = n_\chi(\epsilon_\chi, \mathfrak{p}) \,.\, \varphi(1),$$

où ϵ_χ désigne le caractère trivial de L_χ.

L'élément $d = \mathrm{N}(\mathfrak{p})^{n_\chi(\epsilon_\chi,\mathfrak{p})}$ de $(\mathbf{Z}_\ell \otimes_{\mathbf{Z}} \mathbf{Z}(\chi))^*$ répond à la question.

BIBLIOGRAPHIE

[1] Ph. Cassou-Nogues, Structure galoisienne des anneaux d'entiers, *Proc. London Math. Soc.*, 38, 3 (1979), 545-576.

[2] Ph. Cassou-Nogues, Module de Frobenius et structure galoisienne des anneaux d'entiers, *J. of Alg.*,, 71 (1981), 268-289.

[3] Ph. Cassou-Nogues, Quelques théorèmes de base normale d'entiers, *Ann. Inst. Fourier*, 28, 3 (1978), 1-33.

[4] A. Fröhlich, Some problems of Galois module structure for wild extensions, *Proc. London Math. Soc.*, 37 (1978), 193-212.

[5] A. Fröhlich and J. Queyrut, On the functional equation of the Artin L function for characters of real representations, *Invent. Math.*, 20 (1973), 125-138.

[6] J. Martinet, Algebraic number fields : L Functions and Galois properties, *Proc. Sympos. Univ. Durham*, Academic Press, London 1977.

[7] J. Queyrut, S-groupes des classes d'un ordre arithmétique (à paraître).

[8] J. Queyrut, Structure galoisienne des anneaux d'entiers d'extensions sauvagement ramifiées (I), *Ann. Inst. Fourier*, 31, 3 (1981), 1-35.

[9] R.G. SWAN and E.G. EVANS, K-theory of finite groups and orders, *Lecture notes in Mathematics* 149, Springer, Berlin - New York, 1970.

[10] J.-P. SERRE, *Corps locaux*, 2e édition, Hermann, Paris, 1968.

[11] J.-P. SERRE, *Représentations linéaires de groupes finis*, 2e édition, Hermann, Paris, 1971.

[12] M.J. TAYLOR, On the self-duality of a ring of integers as a Galois module, *Invent. Math.*, 46 (1978), 173-177.

[13] M.J. TAYLOR, On Fröhlich's conjecture for rings of integers of tame extensions, *Invent. Math.*, 63 (1981), 41-79.

[14] A. FROHLICH, Arithmetic and Galois module structure for tame extensions, *J. Reine angew. Math.*, 286-287 (1976), 380-440.

Manuscrit reçu le 9 juillet 1981
révisé le 14 septembre 1981.

Ph. CASSOU-NOGUES & J. QUEYRUT,
Université de Bordeaux I
U.E.R. de Mathématiques
et d'Informatique
351 cours de la Libération
33405 Talence.