

ANNALES DE L'INSTITUT FOURIER

PHILIPPE CASSOU-NOGUÈS

JACQUES QUEYRUT

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

Annales de l'institut Fourier, tome 32, n° 1 (1982), p. 7-27

http://www.numdam.org/item?id=AIF_1982__32_1_7_0

© Annales de l'institut Fourier, 1982, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (<http://annalif.ujf-grenoble.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

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

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

1. Introduction.

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

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

Lorsque N est une extension modérément ramifiée de K , $\mathbb{Z}_N$ définit un élément que l'on note $U_{N/K}$ de $\mathcal{C}l(\mathbb{Z}[G])$. Fröhlich ([14]) a démontré que $U_{N/K}$ appartient au noyau de l'homomorphisme d'extension des scalaires de $\mathcal{C}l(\mathbb{Z}[G])$ sur $\mathcal{C}l(\mathfrak{M})$ (le noyau ne dépend pas du choix de $\mathfrak{M}$). On peut décomposer $U_{N/K}$ en un produit $t(W_{N/K}) \cdot V_{N/K}$ 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 $\mathbb{Z}$ dans $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$, 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 $\mathcal{C}\ell(\mathfrak{N})$ 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 $U_{N/K}^S$, de $\tilde{\mathcal{K}}_0^S(\mathbf{Z}[G])$. Le principal résultat de [8] est que $U_{N/K}^S$ appartient au noyau de l'homomorphisme d'extension des scalaires de $\tilde{\mathcal{K}}_0^S(\mathbf{Z}[G])$ sur $\tilde{\mathcal{K}}_0^S(\mathfrak{M}^S)$ 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 $U_{N/K}^S$ se décompose dans $\tilde{\mathcal{K}}_0^S(\mathbf{Z}[G])$ en deux éléments $t^S(W_{N/K})$ et $V_{N/K}^S$ 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 $V_{N/K}^S = 1$. On définit (§ 4) un ordre $\mathfrak{N}^S$ 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 $V_{N/K}^S$ dans $\tilde{\mathcal{K}}_0^S(\mathfrak{N}^S)$ est triviale. Dans le paragraphe 5, on obtient une majoration de l'exposant du noyau de l'homomorphisme de $\tilde{\mathcal{K}}_0^S(\mathbf{Z}[G])$ dans $\tilde{\mathcal{K}}_0^S(\mathfrak{N}^S)$; on en déduit, (théorème 5.3), une majoration de l'ordre de $V_{N/K}^S$ et une grande classe d'extensions N de K et de parties S pour lesquelles $V_{N/K}^S$ 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 $\tilde{\mathcal{K}}_0^S(\mathcal{O})$ données dans [7] et du représentant de $U_{N/K}^S$ dans $\tilde{\mathcal{K}}_0^S(\mathbf{Z}[G])$ donné dans [8]. L'élément $V_{N/K}^S$ est décrit dans le paragraphe 1; il appartient à un sous-groupe canonique de $\tilde{\mathcal{K}}_0^S(\mathbf{Z}[G])$ qui est interprété algé-

briquement 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 $\tilde{\mathcal{K}}_0^S(\mathbf{Z}[G])$ 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 $\mathfrak{R}(\mathbf{Q})$, s'identifie à l'ensemble formé de la place archimédienne p_{∞} de $\mathbf{Q}$ et de l'ensemble $\mathfrak{R}(\mathbf{Z})$ des nombres premiers de $\mathbf{Z}$. L'indexation par un élément p appartenant à $\mathfrak{R}(\mathbf{Q})$ désignera la complétion en p .

Soit $J(\overline{\mathbf{Q}})$ le groupe des idèles de $\overline{\mathbf{Q}}$. Pour tout $p \in \mathfrak{R}(\mathbf{Q})$ 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 $(x_p)_{p \in \mathfrak{R}(\mathbf{Q})}$ où x_p appartient à $(\mathbf{Q}_p \otimes_{\mathbf{Q}} \overline{\mathbf{Q}})^*$. On note $U(\overline{\mathbf{Q}})^+$ le groupe des idèles $x = (x_p)_{p \in \mathfrak{R}(\mathbf{Q})}$ tels que x_p est une unité pour tout $p \in \mathfrak{R}(\mathbf{Z})$ et $x_{p_{\infty}}$ 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 :

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

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

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

Soit $\mathfrak{O}$ un ordre de $\mathbf{Z}$ dans $\mathbf{Q}[G]$. On considère la catégorie $\mathfrak{C}_{\mathfrak{p}}^S(\mathfrak{O})$ des $\mathfrak{O}$ -modules M de type fini, sans torsion et tels que pour tout p de $\mathfrak{R}(\mathbf{Z})$ 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 $\mathcal{C}_{\mathbb{Q}_p}^S(\mathcal{D})$ 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 $\mathcal{H}_0^S(\mathcal{D})$. Le groupe $\mathcal{H}_0^S(\mathcal{D})$ a été décrit dans [7]. En particulier, ([7], th. 4.1 et 4.2), il existe un isomorphisme $\eta_{\mathcal{D}}$ du groupe quotient :

$$\text{Hom}_{G_{\mathbb{Q}}}(\mathcal{R}(G), J(\bar{\mathcal{Q}}))/\text{Hom}_{G_{\mathbb{Q}}}(\mathcal{R}(G), \bar{\mathcal{Q}}^*). H(\mathcal{H}_0^S(\mathcal{D})) \quad (1)$$

sur $\mathcal{H}_0^S(\mathcal{D})$, le sous-groupe de torsion de $\mathcal{H}_0^S(\mathcal{D})$, où $\mathcal{R}(G)$ désigne le groupe des caractères virtuels de G dans $\bar{\mathcal{Q}}$ et $H(\mathcal{H}_0^S(\mathcal{D}))$ est le sous-groupe des éléments f de $\text{Hom}_{G_{\mathbb{Q}}}(\mathcal{R}(G), J(\bar{\mathcal{Q}}))$ vérifiant :

$$\left\{ \begin{array}{l} \forall p \in S, f(\chi)_p \in U_p(\bar{\mathcal{Q}}), \text{ pour tout caractère } \chi \text{ nul sur les} \\ \text{éléments de } G \text{ dont l'ordre est divisible par } p \\ \forall p \in \mathcal{P}(\mathcal{Z}) - S, f(\chi)_p = \text{Det}_{\chi}(\alpha_p) \text{ avec } \alpha_p \in \mathcal{D}_p^*, \text{ pour tout} \\ \text{caractère } \chi \text{ de } \mathcal{R}(G) \\ \text{pour } p_{\infty}, f(\chi)_{p_{\infty}} \in U_{p_{\infty}}(\bar{\mathcal{Q}}), \text{ pour tout caractère } \chi \text{ symplec-} \\ \text{tique de } \mathcal{R}(G). \end{array} \right.$$

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

On considère une extension galoisienne finie N d'un corps de nombres K de groupe de Galois G . Pour toute famille S de $\mathcal{P}(\mathcal{Z})$ 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 $\mathcal{H}_0^S(\mathcal{Z}[G])$ par $\eta_{\mathcal{Z}[G]}$ est $[\mathcal{Z}_N] - [\mathcal{Z}[G]^{[K:\mathcal{Q}]}]$.

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

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

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

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 $\text{Hom}_{G_Q}(R(G), J(\bar{Q}))$ construit de la façon suivante :

$$(3) \quad \left\{ \begin{array}{l} - \text{pour tout caractère } \chi \text{ irréductible et non symplectique} \\ \quad \text{de } G, \text{ on pose } W'_{N/K}(\chi) = 1 \\ - \text{pour tout caractère } \chi \text{ irréductible et symplectique de } G, \\ \quad \text{on définit les composantes locales de } W'_{N/K}(\chi) \text{ par :} \\ \quad \quad W'_{N/K}(\chi)_p = 1 \quad \quad \forall p \in \mathcal{P}(Z) \\ \quad \quad W'_{N/K}(\chi)_{p_\infty} = W_{N/K}(\chi^{\omega^{-1}}), \quad \forall \omega \in G_Q. \end{array} \right.$$

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

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

Il est clair que si $\mathcal{D}'$ est un ordre de $Q[G]$ contenant $\mathcal{D}$ et tel que $\mathcal{D}'_p = \mathcal{D}_p$ pour $p \in S$, on a $t_{\mathcal{D}'}^S(W_{N/K}) = \text{Ext}_{\mathcal{D}'}^{\mathcal{D}'}(t_{\mathcal{D}}^S(W_{N/K}))$.

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

$$(4) \quad U_{N/K}^S = t^S(W_{N/K}) V_{N/K}^S.$$

PROPOSITION 2.2. — Soit $\bar{S}$ l'ensemble des nombres premiers n'appartenant pas à S et divisant l'ordre de G . L'élément $V_{N/K}^S$ est la classe de l'homomorphisme f de $\text{Hom}_{G_Q}(R_G, J(\bar{Q}))$ défini par : pour tout $\chi \in R(G)$,

$$(5) \quad \left\{ \begin{array}{ll} f(\chi)_p = \mathfrak{N}_{K/Q}(a_p | \chi) \cdot \tau_K(\chi)_p^{-1} & \text{pour } p \in \bar{S} \\ f(\chi)_p = 1 & \text{pour } p \in \mathcal{P}(Q) - \bar{S} \end{array} \right.$$

où $\tau_K(\chi)$ est la somme de Gauss galoisienne associée au caractère χ , a_p est une base de Z_{N_p} sur $Z_{K_p}[G]$ pour tout $p \in \bar{S}$ et $\mathfrak{N}_{K/Q}(a_p | \chi)$ 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 $a \in N$ tel que $N = K[G]a$; il existe $a_p \in N_p$ tel que $Z_{N_p} = Z_{K_p}[G]a_p$ pour $p \notin S$ et tel que

$$Z_{N_p}/Z_{N_p} \cap Z_{K_p}[G]a_p \quad \text{et} \quad Z_{K_p}[G]a_p/Z_{N_p} \cap Z_{K_p}[G]a_p$$

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

L'élément $U_{N/K}^S$ est représenté par l'homomorphisme dont la p -composante est donnée par : $\chi \mapsto \mathcal{I}_{K/Q}(a|\chi)^{-1} \mathcal{I}_{K/Q}(a_p|\chi)$. L'application $\chi \mapsto \tau_K(\chi) \mathcal{I}_{K/Q}(a|\chi)^{-1} W'_{N/K}(\chi)$ appartient à $\text{Hom}_{G_Q}(R(G), \bar{Q}^*)$ ([4] propositions 2.3 et 2.5).

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

$$\chi \longrightarrow \tau_K(\chi)^{-1} \mathcal{I}_{K/Q}(a_p|\chi) W'_{N/K}(\chi).$$

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

$$f_1(\chi)_p = \tau_K(\chi)^{-1} \mathcal{I}_{K/Q}(a_p|\chi) W'_{N/K}(\chi)$$

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

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

Soit ν'_p l'homomorphisme naturel de

$$\text{Hom}_{G_Q}(R(G), \bar{Q}_p^*)/\text{Det}(Z_p[G]^*)$$

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

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

i) $M_p = N_p$ si $p \notin \bar{S}$, M_p et N_p sont des $Z_p[G]$ -modules isomorphes si $p \in \bar{S}$

ii) $\eta_{Z[G]}(V_{N/K}^S) = [M] - [N]$ dans $\tilde{\mathcal{H}}_0^S(Z[G])$.

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

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

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

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

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

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, 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

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

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

i) $\tau(\chi) \equiv y(\chi)$ modulo $\mathfrak{L}$, pour tout χ de $\text{Ker } d_{\mathfrak{L}}$ et tout 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

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

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

On a $\tau_{K,\mathfrak{p}}(\chi) = 1$ pour tout $\chi \in \mathbf{R}(G)$ 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 $\mathbf{R}^s(G)$ le sous-groupe de $\mathbf{R}(G)$ 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 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 $\mathbf{R}^s(G) \cap \text{Ker } d_{\mathfrak{L}}$.*

Démonstration. — D'après le théorème 3.1, on a $\tau_{K,\mathfrak{p}}(\chi) \equiv 1$ modulo $\mathfrak{L}$ pour tout ℓ modérément ramifié dans N et pour tout $\chi \in \mathbf{R}^s(G) \cap \text{Ker } d_{\mathfrak{L}}$. 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 $\chi \in R^s(G)$, $W_{K,p}(\chi)$ est égal à 1 ou -1 ; on en déduit que $f_{K,p}(\chi)^{1/2}$ est une unité en $\mathfrak{O}$ et que $W_{K,p}(\chi) \equiv N_{K/Q}(f_{K,p}(\chi))^{-1/2}$ modulo $\mathfrak{O}$.

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

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

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

i) $W_{N/K}(\chi)^2 \equiv z(\chi)$ modulo $\mathfrak{O}$, pour tout χ de $\text{Ker } d_{\mathfrak{q}}$ 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 $N_{K/Q}(f_{K,p}(\chi)) \equiv 1$ modulo $\mathfrak{O}$ pour tout $\chi \in \text{Ker } d_{\mathfrak{q}}$.*

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 $\mathfrak{p}$, $f_{K,p}(\chi) = 1$. 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 $f_{K,p}(\eta\nu)$ et $f_{K,p}(\eta)$ montre que $f_{K,p}(\eta\nu) = f_{K,p}(\eta)$ car ν est modérément ramifié. Si η est non ramifié et ν est ramifié, $f_{K,p}(\eta\nu) = f_{K,p}(\nu)$. Le caractère ν est modérément ramifié, d'où l'ordre de ν divise le cardinal de $\mathbb{Z}_K/\mathfrak{p}$; donc : $N_{K/Q}(f_{K,p}(\nu)) \equiv 1$ modulo $\mathfrak{O}$.

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

4. Description de $V_{N/K}^S$.

On déduit de la proposition 1.7 et du théorème I de [8] l'égalité $\text{Ext}_{Z[G]}^{\mathfrak{M}^S}(V_{N/K}^S) = 1$; 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 $Z[G]$ et $\text{Rac}(\mathfrak{F})$ sa racine. On définit l'ordre $\mathfrak{A}^S$ de Z dans $Q[G]$ par l'égalité :

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

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

THEOREME 4.1. — Soit S un ensemble fini de nombres premiers de Z contenant les nombres premiers sauvagement ramifiés dans N/K ; alors, on a :

$$\text{Ext}_{Z[G]}^{\mathfrak{A}^S}(V_{N/K}^S) = 1.$$

On a donc l'égalité :

$$\text{Ext}_{Z[G]}^{\mathfrak{A}^S}(U_{N/K}^S) = t^S(W_{N/K}).$$

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 Z -torsion, localement libres pour tout nombre premier p de Z n'appartenant pas à S et deux suites exactes :

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

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

où r est le rang de Z_N sur $Z[G]$ ($r = [K:Q]$).

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 $\text{Ext}_{Z[G]}^{\mathfrak{A}^S}(V_{N/K}^S)$ est représenté par la classe de l'élément

$$f \in \text{Hom}_{G_Q}(R(G), J(\overline{Q}))$$

vérifiant les conditions (5) de la proposition 3.2.

Soit γ l'élément de $\text{Hom}_{G_Q}(R(G), \mu)$ défini dans le corollaire 3.2. Comme $\gamma(\chi) = 1$ pour $\chi \in R^S(G)$, l'élément g égal

à fy est un nouveau représentant de $\text{Ext}_{\mathbf{Z}[G]}^{\mathfrak{A}^S}(\mathbf{V}_{N/K}^S)$. On a les congruences :

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

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

$$g(\chi)_\ell = \text{Det}_\chi(\alpha_\ell), \quad \forall \chi \in R(G), \quad \forall \ell \in \overline{S}.$$

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

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

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

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

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

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

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

$$\begin{array}{ccccccc} 0 \longrightarrow & \prod_{p \in \overline{S}} \mathcal{O}^t(\mathbf{Z}_p[G], \mathfrak{A}_p^S) & \longrightarrow & \bigoplus_{p \in \overline{S}} \mathcal{K}_{0,\text{rel}}(\mathbf{Z}_p[G]) & \longrightarrow & \bigoplus_{p \in \overline{S}} \mathcal{K}_{0,\text{rel}}(\mathfrak{A}_p^S) & \longrightarrow 0 \\ & \downarrow & & \downarrow \bigoplus_{p \in \overline{S}} \nu_{\mathbf{Z}_p[G]} & & \downarrow \bigoplus_{p \in \overline{S}} \nu_{\mathfrak{A}_p^S} & \\ 0 \longrightarrow & \mathcal{O}(\mathbf{Z}[G], \mathfrak{A}^S) & \longrightarrow & \tilde{\mathcal{K}}_0^S(\mathbf{Z}[G]) & \longrightarrow & \tilde{\mathcal{K}}_0^S(\mathfrak{A}^S) & \longrightarrow 0. \end{array}$$

On vient donc de démontrer que $\mathbf{V}_{N/K}^S$ appartient à l'image de $\bigoplus_{p \in \overline{S}} \nu_{\mathbf{Z}_p[G]}$. On en déduit une décomposition $\mathbf{V}_{N/K}^S = \prod_{p \in \overline{S}} \mathbf{V}_{N/K,p}^S$ dans laquelle $\mathbf{V}_{N/K,p}^S$ 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 $\mathbf{V}_{N/K,p}^S$ est une puissance de p .*

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

5. Majoration de l'ordre de $V_{N/K}^S$.

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

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

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

$$\text{Ind}((x_H)_{H \in X_G}) = \sum_{H \in X_G} \text{Ind}_H^G x_H \quad \text{où } R_Q(G)$$

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

L'exemple le plus important est donné par l'ensemble des groupes Q -élémentaires.

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

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

- i) $V_{N/K,p}^S = 1$
- ii) $V_{N/L,p}^S = 1$ 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 :

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

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 $\text{Res}_{\mathbf{Z}[G]}^{\mathbf{Z}[H]}$ (resp. ${}^t\theta^*$) de $\tilde{\mathcal{K}}_0^S(\mathbf{Z}[G])$ dans $\tilde{\mathcal{K}}_0^S(\mathbf{Z}[H])$ (resp. $\tilde{\mathcal{K}}_0^S(\mathbf{Z}[G/H])$) 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 $f \in \text{Hom}_{G_{\mathbf{Q}}}(\mathbf{R}(G), \mathbf{J}(\bar{\mathbf{Q}}))$ représente $V_{N/K}^S$, l'application $\rho(f)$ défini par: $\forall \chi \in \mathbf{R}(H)$, $\rho(f)(\chi) = f(\text{Ind}_H^G \chi)$ représente $\text{Res}_{\mathbf{Z}[G]}^{\mathbf{Z}[H]}(\eta_{\mathbf{Z}[G]}(V_{N/K}^S))$ ([7], proposition 5.4). Il est clair que

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

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

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

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

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

(resp. 1) pour tout caractère χ de $\mathbf{R}(H)$ 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, $\text{Ind}_H^G(\chi)$ 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 :

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

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

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

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 :

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

Ceci démontre la première partie du lemme.

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

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

Pour cette opération le groupe (1) a une structure de module de Frobenius ([9], chap. II). Comme l'application Ind est surjective,

on a : $1 = \sum_{H \in X_G} \text{Ind}_H^G(\sigma_H)$ où $\sigma_H \in R_{\mathbf{Q}}(H)$. En écrivant les caractères χ de G sous la forme $\chi = \sum_{H \in X_G} \text{Ind}_H^G(\sigma_H \text{Res}_G^H(\chi))$, on en

déduit que l'ordre de $V_{N/K,p}^S$ divise le p.p.c.m. des ordres de $\rho_{G/H}(V_{N/K,p}^S)$ pour H parcourant X_G ; il divise donc le p.p.c.m. des ordres de $V_{N/N^H,p}^S$ pour H parcourant X_G .

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

Démonstration. — Pour tout sous-groupe abélien H de G , on a $V_{N/N^H}^S = 1$ ([8], théorème III). On en déduit que $V_{N/K}^S$ 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 , $V_{N/K,p}^S$ qui est la p -composante de $V_{N/K}^S$ 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 $\prod_{p \in S} p^{n_p}$. On sait que l'ordre de $V_{N/K}^S$ 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 $n' = n \cdot \prod_{p|n} p^{-1}$.

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

Démonstration. — Soit $\hat{G}^{ab}$ le quotient de G par son sous-groupe des commutateurs. On déduit du lemme 5.3 et du théorème III de [8] que $V_{N/K}^S$ appartient au noyau de l'homomorphisme de $\tilde{\mathcal{K}}_0^S(\mathbb{Z}[G])$ sur $\tilde{\mathcal{K}}_0^S(\mathbb{Z}[G^{ab}])$. Plus précisément $V_{N/K,p}^S$ appartient à l'image par ν_p du noyau de l'homomorphisme de $\mathcal{K}_{0,rel}^S(\mathbb{Z}_p[G])$ dans $\mathcal{K}_{0,rel}^S(\mathbb{Z}_p[G^{ab}])$. Le théorème découle du lemme 6 de [2].

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

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

Démonstration. — Soit $\text{Res}_{\mathbb{Z}_K}^{\mathbb{Z}}$ l'homomorphisme de restriction de $\tilde{\mathcal{K}}_0^S(\mathbb{Z}_K[\Gamma])$ dans $\tilde{\mathcal{K}}_0^S(\mathbb{Z}[\Gamma])$; il est clair que $U_{N/K}^S$ appartient à l'image de l'homomorphisme $\text{Res}_{\mathbb{Z}_K}^{\mathbb{Z}}$. Comme $t^S(W_{N/K}^S)^2 = 1$, on en déduit que $(V_{N/K}^S)^2$ appartient à l'image de l'application $\eta_{\mathbb{Z}[G]}^{-1} \circ \text{Res}_{\mathbb{Z}_K}^{\mathbb{Z}}$. Le groupe $\mathcal{K}_0^S(\mathbb{Z}_K[\Gamma])$ 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 $(V_{N/K}^S)^2 = 1$, si le résultat est vrai pour les groupes K - p -élémentaires.

Exemples. — On a $V_{N/K}^S = 1$, c'est-à-dire $U_{N/K}^S = t^S(W_{N/K})$ 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 $V_{N/K}^S$ 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 $V_{N/K}^S$ divise n' . Dans ces trois cas, l'ordre de $V_{N/K}^S$ est impair. Or on déduit du théorème III de [8] que l'ordre de $V_{N/K}^S$ 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 $\tilde{\mathcal{K}}_0^S(\mathbb{Z}[G])$ est muni d'une involution, notée $x \mapsto \bar{x}$. Si $f \in \text{Hom}_{G_Q}(\mathbb{R}(G), J(\bar{\mathbb{Q}}))$ représente x , $\bar{x}$ est représenté par l'homomorphisme $\chi \mapsto f(\bar{\chi})$ où $\bar{\chi}$ 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 : $U_{N/K}^S \cdot \bar{U}_{N/K}^S = 1$.*

Dans [8], on a construit à partir de l'application de trace de N sur K une forme hermitienne, noté $\text{Tr}_{N/K}$. Puis on a défini le discriminant de $\mathbb{Z}_N$ par rapport à cette forme hermitienne, comme étant un élément du groupe de Grothendieck $\mathcal{K}_{0,\text{rel}}(\mathbb{Z}_K[G])$ de la catégorie des $\mathbb{Z}_K[G]$ -modules de type fini, de $\mathbb{Z}$ -torsion, quotients de deux modules localement libres en dehors de S . Soit ν l'homomorphisme de $\mathcal{K}_{0,\text{rel}}(\mathbb{Z}[G])$ dans $\tilde{\mathcal{K}}_0^S(\mathbb{Z}[G])$, ([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 :*

$$\eta_{\mathbb{Z}[G]}(U_{N/K}^S \cdot \bar{U}_{N/K}^S) = \nu(\text{Res}_{\mathbb{Z}_K}^{\mathbb{Z}}(\Delta_{\text{Tr}_{N/K}}(\mathbb{Z}_N))) = \nu(\Delta_{\text{Tr}_{N/Q}}(\mathbb{Z}_N)).$$

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

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

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

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

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

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

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

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

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

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

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

Démonstration. — On suppose que K est un corps local. Si p est modérément ramifié, on utilise le fait que

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

et on démontre que

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

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 $\text{Det}(\mathbf{Z}_\ell[G]^*)$.*

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 $\text{Det}(\mathbf{Z}_\ell[G]^*)$.*

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 $t_{\mathfrak{p}}(N/K) = \sum_{i=1}^{\ell} t_{\mathfrak{p}}^i(N/K)$ où $t_{\mathfrak{p}}^i(N/K)$ est l'élément de $\overline{\mathbf{Q}}[G]$ défini dans [8], § 1. On a $\mathfrak{F}_{K,\mathfrak{p}} = \text{Det}(t_{\mathfrak{p}}(N/K) \cdot \overline{t_{\mathfrak{p}}(N/K)})$ (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 $\text{Det}(\mathbf{Z}_\ell[G]^*)$.*

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 $\text{Det}(\mathbf{Z}_\ell[G]^*)$.*

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 $\mathcal{H}_{0,\text{rel}}(\mathbf{Z}_\ell[G])$ est un module de Frobenius et que l'application qui à $\chi \in R(G)$

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

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

pour tout caractère irréductible φ de L_χ , où χ est un caractère fidèle de H , $\mathbb{Z}(\chi)$ l'anneau des entiers de l'extension de $\mathbb{Q}$ obtenue par adjonction des valeurs de χ et $\mathbb{Z}(\chi)[L_\chi]$ l'algèbre du groupe L_χ à coefficients dans $\mathbb{Z}(\chi)$. 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 $N(p)$ le cardinal de $\mathbb{Z}_K/p$ et $n_\chi(\varphi, p)$ l'entier défini par l'égalité :

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

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

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

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

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

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 $i \geq 1$ le groupe G_i est un sous-groupe de H ; nous en déduisons :

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

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

$$n_X(\varphi, p) = n_X(\epsilon_X, p) \cdot \varphi(1),$$

où ϵ_X désigne le caractère trivial de L_X .

L'élément $d = N(p)^{n_X(\epsilon_X, p)}$ de $(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}(\chi))^*$ 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*, 2^e édition, Hermann, Paris, 1968.
- [11] J.-P. SERRE, *Représentations linéaires de groupes finis*, 2^e 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.