ANNALES DE L'INSTITUT FOURIER

JACQUES QUEYRUT

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

Annales de l'institut Fourier, tome 31, n° 3 (1981), p. 1-35

<http://www.numdam.org/item?id=AIF_1981__31_3_1_0>

Ann. Inst. Fourier, Grenoble
31, 3 (1981), 1-35

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

par Jacques QUEYRUT(*)

Soit $\mathbf{Z}$ l'anneau des entiers et soit $\mathbf{Q}$ son corps des fractions. On fixe une clôture algébrique $\overline{\mathbf{Q}}$ de $\mathbf{Q}$ et l'on note $\overline{\mathbf{Z}}$ la clôture intégrale de $\mathbf{Z}$ dans $\overline{\mathbf{Q}}$. Le groupe de Galois $G_{\mathbf{Q}}$ de $\overline{\mathbf{Q}}$ sur $\mathbf{Q}$ est un groupe profini. Les corps de nombres N, i.e. les extensions de $\mathbf{Q}$ de degré fini incluses dans $\overline{\mathbf{Q}}$, sont en bijections avec les sous-groupes ouverts G_N de $G_{\mathbf{Q}}$.

Tout groupe d'automorphismes Γ de N opère sur la clôture intégrale $\mathbf{Z}_N$ de $\mathbf{Z}$ dans N. On se propose d'étudier la structure de $\mathbf{Z}_N$ en tant que $\mathbf{Z}[\Gamma]$-module.

Soit $\mathcal{P}(\mathbf{Z})$ l'ensemble des nombres premiers de $\mathbf{Z}$. Un automorphisme γ de N est dit ramifié (resp. sauvagement ramifié) en $p \in \mathcal{P}(\mathbf{Z})$ s'il existe un idéal premier $\mathfrak{P}$ de $\mathbf{Z}_N$ au-dessus de p et un entier i supérieur ou égal à 1 (resp. à 2) tel que $\gamma(a) - a \in \mathfrak{P}^i$, $\forall a \in \mathbf{Z}_N$. On note S, ou $S(\Gamma)$, une partie de $\mathcal{P}(\mathbf{Z})$ contenant l'ensemble des nombres premiers p tels que Γ contienne un automorphisme sauvagement ramifié en p.

On généralise, dans cet article, au cas où S est non vide, les résultats de Fröhlich ([10]), Taylor ([22]) et Cougnard ([2] et [3]) obtenus pour les groupes Γ ne contenant pas d'éléments sauvagement ramifiés.

Soit $\mathcal{G}_{\oplus}^{S}(\mathbf{Z}[\Gamma])$ le quotient du groupe abélien libre engendré par les classes d'isomorphismes (M) des $\mathbf{Z}[\Gamma]$-modules M de type

---

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

fini sans $\mathbf{Z}$-torsion par le sous-groupe engendré par les éléments $(M) - (M') - (M'')$ où M, M' et M'' vérifient : il existe une suite exacte

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

telle que pour tout $p \in \mathfrak{P}(\mathbf{Z}) - S$ la suite

$$0 \longrightarrow M'_p \xrightarrow{f_p} M_p \xrightarrow{g_p} M''_p \longrightarrow 0$$

est scindée. On note $[M]$ la classe d'un $\mathbf{Z}[\Gamma]$-module M dans $\mathcal{G}^S_\oplus(\mathbf{Z}[\Gamma])$ (voir [18]).

THEOREME 1. – *Soit* Γ *un groupe d'automorphismes d'un corps de nombres* N. *Soit* S *un ensemble de nombres premiers contenant les nombres premiers* p *tels qu'il existe un automorphisme de* Γ *sauvagement ramifié en* p. *Alors* $[\mathbf{Z}_N] - r[\mathbf{Z}[\Gamma]] = 0$ *dans* $\mathcal{G}^S_\oplus(\mathbf{Z}[\Gamma])$ *où* $r = [N^\Gamma : \mathbf{Q}]$ *est le rang de* $\mathbf{Z}_N$.

L'énoncé du théorème suivant est une traduction du théorème 1 ([18], proposition 1.3) :

THEOREME 2. – *Sous les hypothèses du théorème 1, il existe trois* $\mathbf{Z}[\Gamma]$*-modules* U, V, W *de type fini, sans* $\mathbf{Z}$*-torsion et deux suites exactes :*

$$0 \longrightarrow U \longrightarrow V \oplus \mathbf{Z}_N \longrightarrow W \longrightarrow 0$$

$$0 \longrightarrow U \longrightarrow V \oplus \mathbf{Z}[\Gamma]^r \longrightarrow W \longrightarrow 0$$

localement scindées pour tout p *n'appartenant pas à* S.

Si Γ ne contient pas d'automorphisme sauvagement ramifié, on peut prendre S vide et l'on retrouve le résultat suivant, dû à Fröhlich ([10], théorème 11) :

COROLLAIRE 1. – *Soit* $\mathfrak{M}$ *un ordre maximal de* $\mathbf{Z}$ *dans* $\mathbf{Q}[\Gamma]$ *contenant* $\mathbf{Z}[\Gamma]$. *On suppose que* Γ *ne contient pas d'automorphisme sauvagement ramifié ; alors* $\mathfrak{M} \otimes_{\mathbf{Z}[\Gamma]} \mathbf{Z}_N$ *et* $\mathfrak{M}\,\mathbf{Z}_N$ *sont des* $\mathfrak{M}$*-modules stablement libres.*

Cela se déduit du résultat bien connu suivant (voir [18], proposition 1.7) : soient deux $\mathbf{Z}[\Gamma]$-modules M et M' localement libres ; M et M' deviennent par extension des scalaires des $\mathfrak{M}$-modules stablement isomorphes si et seulement s'il existe un $\mathbf{Z}[\Gamma]$-module

X de type fini sans $\mathbf{Z}$-torsion et un isomorphisme de $M \oplus X$ sur $M' \oplus X$.

Quelques résultats ont été démontrés par Fröhlich et Cougnard dans le cas où Γ contient des automorphismes sauvagement ramifiés. En utilisant les exemples de [18], corollaire 6.4, on retrouve le résultat suivant, dû à Cougnard dans le cas où $N^\Gamma = \mathbf{Q}$ ([2]) et à Fröhlich dans le cas général ([11]) :

COROLLAIRE 2. – *Soit* $\mathfrak{M}$ *un ordre maximal de* $\mathbf{Z}$ *dans* $\mathbf{Q}[\Gamma]$ *contenant* $\mathbf{Z}[\Gamma]$. *Si* Γ *est un p-groupe,* $\mathfrak{M}\,\mathbf{Z}_N$ *est un* $\mathfrak{M}$*-module stablement libre.*

J. Cougnard ([3]) a montré que $\mathfrak{M} \otimes_{\mathbf{Z}[\Gamma]} \mathbf{Z}_N$ est isomorphe à $\mathfrak{M}\,\mathbf{Z}_N \oplus T$ où T est un groupe fini dont les facteurs premiers de l'ordre sont les nombres premiers p tels que Γ contienne un automorphisme sauvagement ramifié en p et $\mathfrak{M}$ est toujours un ordre maximal de $\mathbf{Z}$ dans $\mathbf{Q}[\Gamma]$ contenant $\mathbf{Z}[\Gamma]$. On écrit T comme quotient d'un module libre ; on a donc une suite exacte

$$0 \longrightarrow M \longrightarrow \mathfrak{M}^n \longrightarrow T \longrightarrow 0.$$

En utilisant les exemples de [18], on retrouve les résultats suivants, dus à Cougnard ([3]) :

COROLLAIRE 3. – *Si* Γ *est un groupe métacyclique d'ordre* pq ($q/p-1$, p *et* q *premiers*) *ou un groupe quaternionien d'ordre* $4p^m$ *ou diédral* $2p^m$ (p *premier*) *alors* $[\mathfrak{M}\,\mathbf{Z}_N] - [\mathfrak{M}^r] = [\mathfrak{M}^r] - [M]$ *dans le groupe* $\mathcal{C}\ell(\mathfrak{M})$ *des classes des* $\mathfrak{M}$*-modules de type fini sans torsion.*

Le choix de S fait dans le théorème 1 entraîne que $\mathbf{Z}_N$ est un $\mathbf{Z}[\Gamma]$-module localement projectif pour tout p n'appartenant pas à S. On peut donc considérer la classe de $\mathbf{Z}_N$ dans le groupe de Grothendieck $\mathcal{K}_0^S(\mathbf{Z}[\Gamma])$ de la catégorie $\mathcal{C}_{\ell p}^S(\mathbf{Z}[\Gamma])$ des $\mathbf{Z}[\Gamma]$-modules de type fini sans $\mathbf{Z}$-torsion, localement projectif pour tout p n'appartenant pas à S (voir [18]).

CONJECTURE. – *L'élément* $[\mathbf{Z}_N] - r[\mathbf{Z}[\Gamma]]$ *est d'ordre 2 dans* $\mathcal{K}_0^S(\mathbf{Z}[\Gamma])$. *Il est même trivial si les constantes de l'équation fonctionnelle des fonctions* L *d'Artin valent* $+1$ *pour les caractères symplectiques de* Γ.

Cette conjecture généralise celle donnée par A. Fröhlich dans [10]. On trouvera une formulation plus précise dans [6]. Le théorème suivant et plus précisément son corollaire 1 montrent que cette conjecture est vérifiée pour un groupe Γ abélien. Ce résultat permet de démontrer la conjecture précédente pour une large classe de groupes (voir [6]).

Pour tout idéal premier $\mathfrak{q}$ de N, on note $\Gamma(\mathfrak{q})$ le groupe de décomposition de $\mathfrak{q}$ dans Γ (i.e. le sous-groupe de Γ formé des automorphismes γ tels que $\gamma(\mathfrak{q}) = \mathfrak{q}$).

THEOREME 3. — *Si* Γ *ne possède pas de caractère symplectique irréductible et si pour tout idéal premier* $\mathfrak{q}$ *de* $\mathbf{Z}_N$, $\Gamma(\mathfrak{q})$ *est abélien, alors* $[\mathbf{Z}_N] - r[\mathbf{Z}[\Gamma]] = 0$ *dans* $\mathcal{K}_0^S(\mathbf{Z}[\Gamma])$.

COROLLAIRE. — *Si* Γ *est abélien, alors* $[\mathbf{Z}_N]$ *est égal à* $r[\mathbf{Z}[\Gamma]]$ *dans* $\mathcal{K}_0^S(\mathbf{Z}[\Gamma])$.

Ce résultat a été démontré par M.J. Taylor ([23]) dans le cas où Γ ne contient pas d'automorphisme sauvagement ramifié.

Les démonstrations utilisent les notions algébriques introduites dans [18] et font appel à la $\mathcal{K}$-théorie algébrique.

La première partie de cet article traite des sommes de Gauss. On y rappelle la définition des sommes de Gauss non abéliennes. On les décompose en produit de sommes de Gauss locales.

Les sommes de Gauss abéliennes locales s'expriment simplement comme des images par l'application Det, définie dans [10] et [18], d'éléments de l'algèbre de groupe $\overline{\mathbf{Q}}[\Gamma]$. Une nouvelle propriété de congruence du conducteur d'Artin des caractères réels permet de préciser le signe de la constante de l'équation fonctionnelle des séries L d'Artin pour les caractères symplectiques.

La deuxième partie traite des résolvantes. On y rappelle tout d'abord la notion d'invariant relatif de réseaux sur une algèbre de groupes. Ceci permet de définir le discriminant d'un réseau par rapport à une forme hermitienne à valeurs dans $K[\Gamma]$. On généralise ensuite la notion de radical introduite par Fröhlich ([8]). Ceci permet de donner une nouvelle définition de la résolvante d'une base normale d'un corps de nombre introduite par Fröhlich ([11]).

Dans la troisième partie, on utilise la deuxième partie pour étendre la définition des résolvantes des anneaux d'entiers d'extensions modérément ramifiées donnée par Fröhlich ([10]) à tous les anneaux d'entiers. On donne leurs principales propriétés fonctorielles.

La dernière partie donne la démonstration des théorèmes 1 et 3. Elle est basée sur une propriété fondamentale des résolvantes des anneaux d'entiers (théorème 4.1). Plus précisément, on démontre que les résolvantes sont représentées par les sommes de Gauss. C'est cette relation qui réalise le passage entre la structure algébrique et la structure arithmétique des anneaux d'entiers.

Notation. – Pour tout anneau A, on note A^* le groupe des éléments inversibles de A.

1. Sommes de Gauss galoisiennes.

Soit G_K un sous-groupe ouvert de $G_{\mathbf{Q}}$, K son corps des invariants. Soit $\mathcal{P}(K)$ l'ensemble des places de K. On identifie $\mathcal{P}(\mathbf{Z}_K)$ et l'ensemble des places non archimédiennes de K. On a $\mathcal{P}(K) = \mathcal{P}(\mathbf{Z}_K) \cup \mathcal{P}_\infty(K)$ où $\mathcal{P}_\infty(K)$ est l'ensemble des places archimédiennes de K. L'indexation par un élément $\mathfrak{p} \in \mathcal{P}(K)$ désignera la complétion en $\mathfrak{p}$.

Soit $R(G_K)$ le groupe de Grothendieck de la catégorie des G_K-modules topologiques de dimension finie sur $\overline{\mathbf{Q}}$. Ce groupe est la limite inductive $\varinjlim \mathcal{K}_0(\overline{\mathbf{Q}}[G_K/G_F])$ où F parcourt l'ensemble des extensions galoisiennes finies de K incluses dans $\overline{\mathbf{Q}}$.

Soit V un G_K-module topologique de dimension finie sur $\overline{\mathbf{Q}}$. Tout élément g de G_K définit un $\overline{\mathbf{Q}}$-endomorphisme de V. On obtient ainsi un homomorphisme de G_K dans $\mathrm{End}_{\overline{\mathbf{Q}}}(V)$. En composant avec la trace, on définit une application de G_K dans $\overline{\mathbf{Q}}$ appelée le caractère de V. L'application qui à V associe son caractère définit un homomorphisme, noté Tr, de $R(G_K)$ dans l'anneau des fonctions centrales de G_K dans $\overline{\mathbf{Q}}$. Les deux applications qui à tout G_K-module topologique V de dimension finie sur $\overline{\mathbf{Q}}$ associent la dimension de V sur $\overline{\mathbf{Q}}$ et l'homomorphisme qui $g \in G_K$ associent le déterminant du $\overline{\mathbf{Q}}$-endomorphisme de V défini par g, définissent deux homomorphismes :

$$\dim : R(G_K) \longrightarrow \mathbf{Z}$$

$$\det : R(G_K) \longrightarrow \mathrm{Hom}(G_K, \overline{\mathbf{Q}}^*).$$

Si G_F est un sous-groupe ouvert de G_K, on définit V^{G_F} comme étant l'ensemble des éléments de V fixe par G_F. Par linéarité on définit ρ^{G_F} pour tout $\rho \in R(G_K)$. On appelle noyau de $\rho = [V]$ l'ensemble $\{g \in G_K, g(v) = v, \forall v \in V\}$. C'est un sous-groupe ouvert de G_K et $\mathcal{K}_0(\overline{\mathbf{Q}}[G_K/G_F])$ s'identifie au sous-groupe de $R(G_K)$ formé des éléments ρ tels que $\mathrm{Ker}\,\rho \supset G_F$.

Si G_F est un sous-groupe ouvert de G_K, on définit les homomorphismes d'induction $\mathrm{Ind}_F^K : R(G_F) \longrightarrow R(G_K)$ correspondant à l'extension des scalaires $\rho = [V] \longrightarrow [\mathbf{Q}[G_K/\mathrm{Ker}\,\rho] \otimes_{\mathbf{Q}[G_F/\mathrm{Ker}\rho]} V]$ et de restriction $\mathrm{Res}_K^F\ R(G_K) \longrightarrow R(G_F)$ correspondant à la restriction des scalaires.

A partir du conducteur d'Artin, on définit une fonction f_K de $\bigcup_{K \subset \overline{\mathbf{Q}}} R(G_K)$ dans $\mathbf{Q}^*$ où K parcourt l'ensemble des extensions de degré fini de $\mathbf{Q}$ incluse dans $\overline{\mathbf{Q}}$ caractérisée par les propriétés suivantes :

1) $\forall \rho \in R(G_K)$, $f_K(\rho) = \prod_{\mathfrak{p} \in \mathfrak{P}(K)} f_{K,\mathfrak{p}}(\rho)$

2) $\forall \mathfrak{p} \in \mathfrak{P}(K)$, l'application $\rho \longrightarrow f_{K,\mathfrak{p}}(\rho)$ est un homomorphisme de $R(G_K)$ dans $\mathbf{Q}^*$

3) Soit $(G_K^i)_{i \in \mathbf{R}}$ les groupes supérieurs de ramification (voir [19], p. 83) pour une place $\mathfrak{P}$ de $\overline{\mathbf{Q}}$ au-dessus de $\mathfrak{p} \in \mathfrak{P}(K)$. Soit $\rho \in R(G_K)$ de dimension 1 ; on note $n_{K,\mathfrak{p}}(\rho)$ le plus petit entier t tel que $\rho(G_K^t) = 1$. On a

$f_{K,\mathfrak{p}}(\rho) = \mathrm{Card}(\mathbf{Z}_K/\mathfrak{p})^{n_{K,\mathfrak{p}}(\rho)}$ si $\mathfrak{p}$ est une place non archimédienne

$f_{K,\mathfrak{p}}(\rho) = (-1)^{n_{K,\mathfrak{p}}(\rho)}$ si $\mathfrak{p}$ est une place archimédienne.

4) Soit G_F un sous-groupe ouvert de G_K, $\rho \in R(G_F)$ de dimension 0, alors $f_K, (\mathrm{Ind}_{F/K}(\rho)) = \prod_{\mathfrak{P}/\mathfrak{p}} f_{1.,\mathfrak{P}}(\rho)$ où $\mathfrak{P}$ parcourt les places de F au-dessus de $\mathfrak{p} \in \mathfrak{P}(K)$.

On montre que $n_{K,\mathfrak{p}}(\rho) = \int_0^{+\infty} (\dim \rho - \dim \rho^{G_K^t})\ dt$ est un entier, ne dépendant pas du choix de la place $\mathfrak{P}$ de $\overline{\mathbf{Q}}$ au-dessus de $\mathfrak{p}$. On a $\forall \rho \in R(G_K)$

$\mathfrak{f}_{K,\mathfrak{p}}(\rho) = \mathrm{card}(\mathbf{Z}_K/\mathfrak{p})^{n_{K,\mathfrak{p}}(\rho)}$ si $\mathfrak{p}$ est une place non archimédienne

$\mathfrak{f}_{K,\mathfrak{p}}(\rho) = (-1)^{n_{K,\mathfrak{p}}(\rho)}$ si $\mathfrak{p}$ est une place archimédienne.

L'entier $n_{K,\mathfrak{p}}(\rho)$ est égal à $n_{K,\mathfrak{p}}(\mathrm{Res}_K^{K_0}(\rho))$ où K_0 est le corps d'inertie de $\mathfrak{P}$. Le groupe $G_{\mathbf{Q}}$ opère sur $R(G_K)$, (voir [18], § 2) et l'on a :

$$\forall \mathfrak{p} \in \mathfrak{P}(K),\ \forall g \in G_{\mathbf{Q}},\ \forall \rho \in R(G_K),\ n_{K,\mathfrak{p}}(\rho^g) = n_{K,\mathfrak{p}}(\rho).$$

Soit $R^b(G_K)$ (resp. $R^s(G_K)$) le sous-groupe de $R(G_K)$ engendré par les classes des G_K-modules topologiques V munis d'une forme bilinéaire non dégénérée invariante par G_K (resp. alternée).

PROPOSITION 1.1. – *Pour tout* $\rho \in R^b(G_K)$ *et pour tout* $\mathfrak{p} \in \mathfrak{P}(\mathbf{Z}_K)$, $\mathfrak{f}_{K,\mathfrak{p}}(\rho)$ *est congru à* 0 *ou à* $\mathfrak{f}_{K,\mathfrak{p}}(\det \rho)$ *modulo* 4.

Remarque. – Cette proposition est une généralisation du théorème de Stikelberger sur les discriminants. En effet, soit G_F un sous-groupe ouvert de $G_{\mathbf{Q}}$, et ρ la classe du $G_{\mathbf{Q}}$-module $\overline{\mathbf{Q}}[G_{\mathbf{Q}}/G_F]$; $\mathfrak{f}_{K,\mathfrak{p}}(\rho)$ est la valeur absolue du discriminant de F sur $\mathbf{Q}$; $\det \rho$ a pour caractère la signature de la permutation définie par les éléments de $G_{\mathbf{Q}}/G_F$ sur lui même ; $\mathfrak{f}(\det \rho)$ est la valeur absolue du discriminant de $F^{\mathrm{Ker}(\det \rho)}$ sur $\mathbf{Q}$, qui est une extension quadratique de $\mathbf{Q}$. Ces deux discriminants ont le même signe.

Démonstration. – Tout élément de $R^b(G_K)$ est combinaison $\mathbf{Z}$-linéaire d'éléments ρ des trois types suivants (voir [17]) :

type 1 : $\rho = [V \oplus V^*]$ où V est simple et V^* est le dual de V, la forme sur $V \oplus V^*$ est la forme hyperbolique.

type 2 : $\rho = [V]$ où V est simple et la forme sur V est symétrique.

type 3 : $\rho = [V]$ où V est simple et la forme sur V est alternée.

Par linéarité il suffit de démontrer le résultat pour ρ de chacun des trois types précédents. Comme $\mathfrak{f}_{K,\mathfrak{p}}(\rho) = \prod_{\mathfrak{P}/\mathfrak{p}} \mathfrak{f}_{F,\mathfrak{P}}(\mathrm{Res}_K^F \rho)$ où F est un corps de décomposition de $\mathfrak{p}$, on peut supposer que $\overline{\mathbf{Q}}^{\mathrm{Ker}\,\rho}$ est une extension non décomposée de K.

Soit $\rho = [V \oplus V^*]$ du type 1, on a $\mathfrak{f}_{K,\mathfrak{p}}(\rho) = \mathfrak{f}_{K,\mathfrak{p}}([V])^2$ d'où le résultat car $\det \rho$ est trivial.

Soit $\rho = [V]$ du type 2 ; le résultat est une conséquence du théorème de Serre ([21]).

Soit $\rho = [V]$ du type 3 ; $\det \rho$ est trivial ; le groupe $G_K/\mathrm{Ker}\,\rho$ est hyper-résoluble. Il existe donc un sous-groupe ouvert G_L de G_K contenant $\mathrm{Ker}\,\rho$ et $\sigma \in R(G_L)$ de dimension 2 tel que $\rho = \mathrm{Ind}_L^K(\sigma)$ et $G_L/\mathrm{Ker}(\sigma)$ est un groupe quaternionien H_{4m}, (voir [17]). On a donc :

$$f_{K,\mathfrak{p}}(\rho) = f_{K,\mathfrak{p}}(\mathrm{Ind}_L^K(\sigma)) = f_{K,\mathfrak{p}}(\mathrm{Ind}_L^K(\sigma - 2.1_{G_L}))\, f_{K,\mathfrak{p}}(\mathrm{Ind}_K^L 1_{G_L})^2$$
$$= f_{K,\mathfrak{p}}(\mathrm{Ind}_L^K(1_{G_L})) \prod_{\mathfrak{P}/\mathfrak{p}} f_{L,\mathfrak{P}}(\sigma).$$

Il suffit donc de démontrer le résultat pour σ.

Si l'extension $\overline{\mathbf{Q}}^{\mathrm{Ker}\,\sigma}/L$ n'est pas totalement ramifiée, son groupe d'inertie est inclus dans le groupe cyclique distingué d'ordre $2m$ de $G_L/\mathrm{Ker}(\sigma)$. La restriction de σ à ce groupe d'inertie est du type 1, donc $n_{L,\mathfrak{P}}(\sigma)$ est pair, ce qui démontre le résultat ; on peut donc supposer que l'extension $\overline{\mathbf{Q}}^{\mathrm{Ker}\,\sigma}$ de L est totalement ramifiée.

Si $2 \in \mathfrak{p}$, m est une puissance de 2, les propositions 4.4 et 4.5 de [13] montrent que ou bien les nombres supérieurs de ramifications de $G_L/\mathrm{Ker}\,\sigma$ sont des entiers ou bien $\mathbf{Z}_L/\mathfrak{P}$ contient les racines cubiques de l'unité on en déduit que $n_{L,\mathfrak{P}}(\sigma)$ est pair dans le premier cas et que $N_{L/\mathbf{Q}}(\mathfrak{P})$ est un carré dans le deuxième cas, donc $f_{L,\mathfrak{P}}(\sigma)$ est au carré.

Si $\mathfrak{p}$ est un idéal au-dessus de p, $p \neq 2$ et $p \equiv -1 \mod 4$, alors m est une puissance de p ; l'extension modérée maximale de L dans $\overline{\mathbf{Q}}^{\mathrm{Ker}\,\rho}$ est de degré 4, donc $\mathbf{Z}_L/\mathfrak{P}$ contient les racines quatrièmes de l'unité. Comme $p \equiv -1 \mod 4$, l'indice d'inertie de p dans L est pair ; donc, $N_{L/\mathbf{Q}}(\mathfrak{P})$ et par suite $f_{L,\mathfrak{P}}(\sigma)$ sont des carrés.

Soit J(K) le groupe des idèles de K ; pour tout $\mathfrak{p} \in \mathcal{P}(K)$, on plonge $K_{\mathfrak{p}}^*$ dans J(K) et on plonge K^* dans la diagonale de J(K).

La définition des sommes de Gauss galoisiennes fait intervenir la théorie du corps de classes. *L'application d'Artin est normalisée de telle sorte que les Frobenius géométriques correspondent aux uniformisantes* (voir [7]). La théorie du corps de classes donne donc un homomorphisme de $J(K)/K^*$ dans G_K^{ab} ; on le note

$x \longmapsto (x, */K)$, (voir [19], p. 226 ou [7]). Si π est une uniformisante de $K_\mathfrak{p}$, on a donc $(\pi, */K) = F_{K,\mathfrak{p}}^{-1}$ où $F_{K,\mathfrak{p}}$ provient de la substitution de Frobenius, générateur topologique canonique du groupe de Galois d'une clôture algébrique du corps résiduel $\mathbf{Z}_{K_\mathfrak{p}}/\mathfrak{p}\,\mathbf{Z}_{K_\mathfrak{p}}$ de $K_\mathfrak{p}$. Pour tout sous-groupe ouvert H de J(K) contenant K^*, il existe une unique extension abélienne L de K telle que $H = K^* N_{L/K}(J(L^*))$, appelée corps de classes de H. Par passage aux quotients, l'homomorphisme $x \longmapsto (x, */K)$ induit un isomorphisme de $J(K)/K^* N_{L/K}(J(L^*))$ sur le groupe de Galois de L sur K ; on le note $x \longmapsto (x, L/K)$. En particulier, soit $\mathfrak{c} = \prod_{\mathfrak{p} \in \mathfrak{P}(K)} \mathfrak{p}^{m(\mathfrak{p})}$, un « cycle » de K ($m(\mathfrak{p}) \geqslant 0$ et $m(\mathfrak{p}) = 0$ pour presque tout $\mathfrak{p}$) ; on appelle corps de classes de rayon $\mathfrak{c}$, le corps de classes du sous-groupe $H_\mathfrak{c}$ de J(K) égal à $K^* U_\mathfrak{c}$ où $U_\mathfrak{c}$ est formé des idèles $(\alpha_\mathfrak{p})_{\mathfrak{p} \in \mathfrak{P}(K)}$ vérifiant : $\alpha_\mathfrak{p}$ est une unité pour tout $\mathfrak{p} \in \mathfrak{P}(\mathbf{Z}_K)$ et si $m(\mathfrak{p}) > 0$

pour $\mathfrak{p}$ une place non archimédienne, $\alpha_\mathfrak{p} \equiv 1 \mod \mathfrak{p}^{m(\mathfrak{p})}$

pour $\mathfrak{p}$ une place archimédienne et réelle, $\alpha_\mathfrak{p}$ est réel et positif.

Pour la suite on fixe un caractère additif non trivial ψ_K du groupe A(K)/K dans $\overline{\mathbf{Q}}^*$, où A(K) est le groupe des adèles de K. On note $\psi_{K,\mathfrak{p}}$ sa restriction à $K_\mathfrak{p}$: $\psi_{K,\mathfrak{p}} : K_\mathfrak{p} \longrightarrow A(K)/K \xrightarrow{\psi} \overline{\mathbf{Q}}$.

Si ψ'_K est un autre caractère additif de A(K), il existe $a \in A(K)$ tel que $\psi'_K(x) = \psi_K(ax)$, $\forall x \in A(K)$ (voir [16], XW, § 6, théorèmes 10 et 11). Le caractère ψ'_K est trivial sur K si et seulement si $a \in K$. Soit $d_\mathfrak{p}$ ou simplement d un générateur de l'idéal $\mathfrak{p}^n \mathbf{Z}_{K_\mathfrak{p}}$ où n est le plus petit entier tel que $\psi_{K,\mathfrak{p}}(\mathfrak{p}^{-n}\mathbf{Z}_{K_\mathfrak{p}}) = 1$. L'idéal $\mathfrak{p}^n \mathbf{Z}_{K_\mathfrak{p}}$ est appelé le conducteur de $\psi_{K,\mathfrak{p}}$. Tous les caractères additifs de A(K) s'expriment à l'aide du caractère canonique de conducteur la différente $\mathcal{D}_{K_\mathfrak{p}/\mathbf{Q}_p}$ de $K_\mathfrak{p}$ sur $\mathbf{Q}_p$; ce caractère est donné par la composition des homomorphismes

$$K_\mathfrak{p} \xrightarrow{(1)} \mathbf{Q}_p \xrightarrow{(2)} \mathbf{Q}_p/\mathbf{Z}_p \xrightarrow{(3)} \mathbf{Q}/\mathbf{Z} \xrightarrow{(4)} \mathbf{C}^*$$

où (1) est la trace de $K_\mathfrak{p}$ sur $\mathbf{Q}_p$

(2) est la surjection canonique

(3) est l'injection canonique qui applique $\mathbf{Q}_p/\mathbf{Z}_p$ sur la p-composante du groupe divisible $\mathbf{Q}/\mathbf{Z}$

(4) est l'application exponentielle $x \longrightarrow e^{2i\pi x}$.

Soit N une extension abélienne K contenue dans $\mathbf{Q}$. Il existe un plus petit corps de classes de rayon $\mathfrak{c}$ contenant N. On note $\mathfrak{p}^{\ell}$ la $\mathfrak{p}$-composante de $\mathfrak{c}$. Le cycle $\mathfrak{c}$ est le plus grand cycle tel que :

$$N_{N/K}(J(N))\, K^* \supset K^*\, U_{\mathfrak{c}}.$$

On pose :

$$U^{(0)}_{K,\mathfrak{p}} = \mathbf{Z}^*_{K_{\mathfrak{p}}} \quad \text{et pour } i > 0 \quad U^{(i)}_{K,\mathfrak{p}} = 1 + \mathfrak{p}^i \mathbf{Z}_{K_{\mathfrak{p}}}.$$

Si ℓ est supérieur ou égal à 1, on pose pour i compris entre 1 et ℓ

$$t^i_{\mathfrak{p}}(L/K) = [U^{(i)}_{K,\mathfrak{p}} : U^{(\ell)}_{K,\mathfrak{p}}]^{-1} \sum_{x \in U^{(0)}_{K,\mathfrak{p}}/U^{(\ell)}_{K,\mathfrak{p}}} (x/\pi^i d, L/K)^{-1}\, \psi_{K,\mathfrak{p}}(x/\pi^i d).$$

Cet élément de $\overline{\mathbf{Q}}[G_K/G_L]^*$ ne dépend pas du choix de l'uniformisante π de $K_{\mathfrak{p}}$ et ne dépend pas du choix du générateur d du conducteur de $\psi_{K,\mathfrak{p}}$. Comme i est positif, $[U^{(i)}_{K,\mathfrak{p}} : U^{(\ell)}_{K,\mathfrak{p}}]$ est une puissance de la caractéristique p de $\mathbf{Z}_{K_{\mathfrak{p}}}/\ \mathbf{Z}_{K_{\mathfrak{p}}}$; il existe donc un entier n tel que :

$$p^n\, t^i_{\mathfrak{p}}(L/K) \in \overline{\mathbf{Z}}[G_K/G_L].$$

On note $t^i_{\mathfrak{p}}(N/K)$ l'image de $t^i_{\mathfrak{p}}(L/K)$ par la surjection :

$$\overline{\mathbf{Q}}[G_K/G_L]^* \longrightarrow \overline{\mathbf{Q}}[G_K/G_N]^*.$$

Soit Det l'application définie par A. Fröhlich ([10]) (voir [18], § 2).

LEMME 1.2. – *Soit* $\rho \in R(G_K)$ *tel que* $\dim \rho = 1$ *et* $\operatorname{Ker} \rho \supset G_L$.

1) *Si* $i < n_{K,\mathfrak{p}}(\rho)$, $\operatorname{Det}_\rho(t^i_{\mathfrak{p}}(L/K)) = 0$

2) *Si* $i > \max(n_{K,\mathfrak{p}}(\rho), 1)$, $\operatorname{Det}_\rho(t^i_{\mathfrak{p}}(L/K)) = 0$

3) *Si* $n_{K,\mathfrak{p}}(\rho) = 0$, $\operatorname{Det}_\rho(t^1_{\mathfrak{p}}(L/K)) = -\operatorname{Det}_\rho((\pi d, L/K))$.

Démonstration. – Ce lemme se démontre comme les résultats classiques analogues sur les sommes de Gauss.

Comme dans [7], on peut unifier ces trois formules de la façon suivante : pour tout $\rho \in R(G_K)$, on pose

$$s\omega_{K,\mathfrak{p}}(\rho) = n_{K,\mathfrak{p}}(\rho) - \dim(\rho - \rho^{G^0_K}) = \int_1^{+\infty} (\dim \rho - \dim \rho^{G^t_K})\, dt.$$

DEFINITION 1.3. – *Soit* $\rho \in R(G_K)$ *de dimension 1 ; on appelle somme de Gauss abélienne l'élément* $\tau^{ab}_{K,\mathfrak{p}}(\rho) = \prod_{\mathfrak{p} \in \mathfrak{P}(K)} \tau^{ab}_{K,\mathfrak{p}}(\rho)$, *où* $\tau^{ab}_{K,\mathfrak{p}}(\rho)$ *est défini par :*

si $\mathfrak{p}$ *est une place archimédienne,* $\tau^{ab}_{K,\mathfrak{p}}(\rho) = 1$

si $\mathfrak{p}$ *est une place non archimédienne,*

$$\tau^{ab}_{K,\mathfrak{p}}(\rho) = \Big(\sum_{x \in U^{(0)}_{K,\mathfrak{p}}/U^{(n)}_{K,\mathfrak{p}}} \rho_{\mathfrak{p}}(x/\gamma d_{\mathfrak{p}})^{-1}\, \psi_{K,\mathfrak{p}}(x/\gamma d_{\mathfrak{p}}) \Big) \operatorname{Det}_{\rho G^0_K}(-F_{K,\mathfrak{p}})^{-1},$$

où $\rho_{\mathfrak{p}}$ *est la composée des applications*

$$K^*_{\mathfrak{p}} \longrightarrow J(K)/K^* \longrightarrow G^{ab}_K \xrightarrow{\det_\rho} \overline{\mathbf{Q}}$$

et γ *est un élément de valuation* $n = s\omega_{K,\mathfrak{p}}(\rho) + 1$.

THEOREME 1.4. – *Il existe une unique application* τ_K *de* $\bigcup_{K \subset \overline{\mathbf{Q}}} R(G_K)$ *dans* $\overline{\mathbf{Q}}^*$ *où* K *parcourt l'ensemble des sous-extensions de* $\overline{\mathbf{Q}}$ *de degré fini sur* $\mathbf{Q}$ *vérifiant :*

1) $\tau_K(\rho) = \prod_{\mathfrak{p} \in \mathfrak{P}(K)} \tau_{K,\mathfrak{p}}(\rho)$ *quels que soient* $\rho \in R(G_K)$ *et* $K \subset \overline{\mathbf{Q}}$

2) $\forall \rho, \rho' \in R(G_K)$, $\tau_{K,\mathfrak{p}}(\rho + \rho') = \tau_{K,\mathfrak{p}}(\rho)\, \tau_{K,\mathfrak{p}}(\rho')$

3) *Si* ρ *est de dimension* 1, $\tau_{K,\mathfrak{p}}(\rho) = \tau^{ab}_{K,\mathfrak{p}}(\rho)$

4) *Soit* G_F *un sous-groupe ouvert d'indice fini de* G_K *et soit* $\rho \in R(G_F)$ *de dimension 0, alors*

$$\tau_{K,\mathfrak{p}}(\mathrm{Ind}^K_F(\rho)) = \prod_{\mathfrak{p}|\mathfrak{p}} \tau_{K,\mathfrak{p}}(\rho).$$

On appelle somme de Gauss galoisienne l'application τ définie ci-dessus. on a :

$$\tau_{K,\mathfrak{p}}(\rho) = 1 \quad \text{si} \quad n_{K,\mathfrak{p}}(\rho) = 0 \quad \text{et} \quad d_{\mathfrak{p}} = 0$$

le produit $\prod_{\mathfrak{p} \in \mathfrak{P}(K)} \tau_{K,\mathfrak{p}}(\rho)$ a donc bien un sens.

Démonstration. – Soit π un plongement de $\overline{\mathbf{Q}}$ dans $\mathbf{C}$; la fonction $\rho \longrightarrow \pi(\tau_{K,\mathfrak{p}}(\rho))$ est égale à la fonction $\epsilon(\pi \circ \rho, \pi \circ \psi, dx)$ définie par Deligne dans [7] pour dx la mesure telle que

$$\int_{\mathbf{Z}_{K_{\mathfrak{p}}}} dx = N_{K_{\mathfrak{p}}/\mathbf{Q}_p}(\mathfrak{D}_{K_{\mathfrak{p}}/\mathbf{Q}_p})^{-1/2}$$

et $\rho \in R(G_K)$ de dimension 1. Deligne a montré que la fonction ϵ était prolongeable à $\underset{K \subset \bar{\mathbf{Q}}}{\cup} R(G_K)$ en une fonction vérifiant les quatre propriétés précédentes. L'image réciproque par π de cette fonction répond à la question. L'unicité découle du théorème de Brauer.

Remarque. – Il serait intéressant d'avoir une démonstration algébrique de ce théorème. Ceci a été fait par A. Fröhlich et M. Taylor ([15]) pour les représentations modérément ramifiées. Comme on le verra plus loin, la détermination d'un élément $t_{K,\mathfrak{p}} \in \bar{\mathbf{Q}}[G]$ tel que $\mathrm{Det}_\rho(t_{K,\mathfrak{p}}) = \tau_{K,\mathfrak{p}}(\rho)\ \forall \rho \in R(G)$, est fondamentale pour l'étude de la structure des anneaux d'entiers.

PROPOSITION 1.5. – *Soit* L *un corps de rayon divisible par* $\mathfrak{p}^{\mathfrak{q}}$; *pour tout* $\rho \in R(G_K)$ *tel que* $\mathrm{Ker}\,\rho \supset G_L$, *on a en posant*

$$t_{\mathfrak{p}}(L/K) = \sum_{i=1}^{\mathfrak{q}} t_{\mathfrak{p}}^i(L/K) :$$

$$\mathrm{Det}_\rho(t_{\mathfrak{p}}(L/K)) = \tau_{K,\mathfrak{p}}^{ab}(\rho) \cdot \mathrm{Det}_{\rho^{G_K^0}}(-F_{K,\mathfrak{p}}).$$

Démonstration. – Par linéarité, il suffit de démonter le résultat lorsque ρ est de dimension 1.

Si $\rho^{G_K^0} = 0$, $s\omega_{K,\mathfrak{p}}(\rho) = n_{K,\mathfrak{p}}(\rho) - 1 \geqslant 0$. D'après les parties 1 et 2 du lemme 1.2, $\mathrm{Det}_\rho\left(\sum_{i=1}^{\mathfrak{q}} t_{\mathfrak{p}}^i(L/K)\right) = \mathrm{Det}_\rho(t_{\mathfrak{p}}^{n_{K,\mathfrak{p}}(\rho)}(L/K))$ est aussi égal à $\tau_{K,\mathfrak{p}}^{ab}(\rho)$. Si $\rho^{G_K^0} = \rho$, $n_{K,\mathfrak{p}}(\rho) = 0 = s\omega_{K,\mathfrak{p}}(\rho)$.

$$\tau_{K,\mathfrak{p}}^{ab}(\rho) = \left(\sum_{x \in U_{K,\mathfrak{p}}^{(0)}/U_{K,\mathfrak{p}}^{(1)}} \rho_{\mathfrak{p}}(x/\pi d)^{-1}\, \psi_{K,\mathfrak{p}}(x/\pi d)\right)(-\rho_{\mathfrak{p}}(\pi))^{-1} = \rho_{\mathfrak{p}}(d).$$

Remarque. – La motivation du choix de la normalisation de l'application d'Artin précédente sont les suivantes : l'équation fonctionnelle locale de Tate (voir [7], 3.3.1) conduit naturellement à définir les sommes de Gauss abéliennes par la formule donnée dans la définition 1.3 ; la normalisation de l'application d'Artin est imposée par des raisons topologiques (voir [7], 3.6) et des raisons algébriques (l'action de $G_{\mathbf{Q}}$ sur les sommes de Gauss et sur les résolvantes est identique, (proposition 1.6 et proposition 1.5 de [10])).

Si $\rho = [V]$, on note $\rho^* = [\mathrm{Hom}_{\mathbf{Q}}(V, \mathbf{Q})]$; on définit ainsi une involution sur $R(G_K)$, (voir § 2.b).

PROPOSITION 1.6.

1) $\tau_{K,\mathfrak{p}}(\rho) \cdot \tau_{K,\mathfrak{p}}(\rho^*) = \mathfrak{f}_{K,\mathfrak{p}}(\rho)\ (\det \rho)_{\mathfrak{p}}(-1)$ *où* $(\det \rho)_{\mathfrak{p}}$ *est le composé des applications*

$$K_{\mathfrak{p}} \longrightarrow J(K)/K^* \longrightarrow G_K^{ab} \xrightarrow{\det \rho} \overline{\mathbf{Q}}^*.$$

2) *Soit* $\mathrm{Ver}_{K/\mathbf{Q}}$ *le transfert de* $G_{\mathbf{Q}}$ *dans* G_K

$$\forall g \in G_Q\ ,\ g\tau_K(\rho^{g^{-1}}) = \tau_K(\rho)\ \det \rho \circ \mathrm{Ver}_{K/\mathbf{Q}}(g).$$

Démonstration. – Elle découle du résultat 7.2 de [17] en tenant compte de la normalisation choisie de l'application d'Artin.

PROPOSITION 1.7.

1) *Soit* $\rho \in R(G_K)$ *tel que* $\det_\rho = 1$. *Pour tout* $\mathfrak{p} \in \mathfrak{P}_\infty(K)$ $n_{K,\mathfrak{p}}(\rho)$ *est pair.*

2) *Soit* π *un plongement de* $\overline{\mathbf{Q}}$ *dans* $\mathbf{C}$ *; il existe*

$$\gamma_K \in \mathrm{Hom}_{G_{\mathbf{Q}}}(R(G_K), \overline{\mathbf{Z}}^*)$$

tel que $\forall \omega \in G_{\mathbf{Q}}$, $\forall \rho \in R^b(G_K)$ *tel que* $\det \rho = 1$,

$$\pi \circ \omega(\gamma_K(\rho)\ \tau_K(\rho) \prod_{\mathfrak{p} \in \mathfrak{P}_\infty(K)} (-1)^{n_{K,\mathfrak{p}}(\rho)/2})$$

soit réel et positif.

Démonstration. –

1) Soit i un nombre complexe tel que $i^2 = -1$. On a : $(i^{-n_{K,\mathfrak{p}}(\rho)})^2 = (-1)^{n_{K,\mathfrak{p}}(\rho)} = \mathfrak{f}_{K,\mathfrak{p}}(\rho)$ pour $\mathfrak{p} \in \mathfrak{P}_\infty(K)$. Si ρ est de dimension 1, $\mathfrak{f}_{K,\mathfrak{p}}(\rho) = (\det \rho)_{\mathfrak{p}}(-1)$; donc, pour tout ρ, $\mathfrak{f}_{K,\mathfrak{p}}(\rho) = (\det \rho)_{\mathfrak{p}}(-1)$. Par la théorie du corps de classes, -1 correspond au Frobenius à l'infini. Comme $\det \rho = 1$, $(\det \rho)_{\mathfrak{p}}(-1) = 1$. Donc $n_{K,\mathfrak{p}}(\rho)$ est pair et $i^{n_{K,\mathfrak{p}}(\rho)}$ est réel.

2) Soit W_K la constante de l'équation fonctionnelle de la fonction L d'Artin. On a :

$$\pi \circ \omega(\tau_K(\rho)) \prod_{\mathfrak{p} \in \mathfrak{P}_\infty(K)} i^{n_{K,\mathfrak{p}}(\rho)} = W_K(\pi \circ \omega(\rho)) \prod_{\mathfrak{p} \in \mathfrak{P}(\mathbf{Z}_K)} \sqrt{\mathfrak{f}_{K,\mathfrak{p}}(\rho)}.$$

On utilise le système de générateur de $R^b(G)$ donné dans la démonstration de la proposition 1.1 pour définir y_K. Si $\rho = \rho^*$, on sait que $W_K(\pi \circ \omega(\rho)) = +1$ pour tout $\omega \in G_{\mathbf{Q}}$ (voir [14]); on pose $y_K(\rho) = 1$. Sinon, $\rho = [V]$, V étant un $\overline{\mathbf{Q}}[G]$-module simple muni d'une forme alternée non dégénérée invariante par G; on a $\det_\rho = 1$. Alors :

$$\pi \circ \omega(\tau_K(\rho) \prod_{\mathfrak{p} \in \mathfrak{P}_\infty(K)} (-1)^{n_{K,\mathfrak{p}}(\rho)/2}) = \pi \circ \omega \circ \pi^{-1} \circ \pi(\tau_K(\rho) \prod_{\mathfrak{p} \in \mathfrak{P}_\infty(K)} (-1)^{n_{K,\mathfrak{p}}(\rho)/2}) = W_K(\pi\rho) \prod_{\mathfrak{p} \in \mathfrak{P}_\infty(K)} \pi \circ \omega \circ \pi^{-1}(\sqrt{f_{K,\mathfrak{p}}(\rho)})$$

car $W_K(\pi\rho) = \pm 1$, d'où :

$$W_K(\pi \circ \omega(\rho))/W_K(\pi\rho) = \prod_{\mathfrak{p} \in \mathfrak{P}(\mathbf{Z}_K)} (\pi \circ \omega \circ \pi^{-1}(\sqrt{f_{K,\mathfrak{p}}(\rho)}))/\sqrt{f_{K,\mathfrak{p}}(\rho)}.$$

D'autre part,

$$W_K(\rho) = \prod_{\in \mathfrak{P}(\mathbf{Z}_K)} W_{K,\mathfrak{p}}(\rho),$$

et on a de même :

$$W_{K,\mathfrak{p}}(\pi \circ \omega(\rho))/W_{K,\mathfrak{p}}(\pi\rho) = (\pi \circ \omega \circ \pi^{-1}(\sqrt{f_{K,\mathfrak{p}}(\rho)}))/\sqrt{f_{K,\mathfrak{p}}(\rho)},$$

(voir [11]).

Le signe de $W_{K,\mathfrak{p}}(\pi\rho)$ ne dépend donc que de la restriction de $\pi \circ \omega \circ \pi^{-1}$ à $\mathbf{Q}(\sqrt{f_{K,\mathfrak{p}}(\rho)})$.

Si $f_{K,\mathfrak{p}}(\rho)$ est un carré, $W_{K,\mathfrak{p}}(\pi\rho) = W_{K,\mathfrak{p}}(\pi \circ \omega\rho)$; on prend $y_K(\rho)$ égal au signe de $W_{K,\mathfrak{p}}(\pi\rho)$.

Si $f_{K,\mathfrak{p}}(\rho)$ n'est pas un carré, alors d'après la proposition 1.1, $\mathbf{Q}(\sqrt{f_{K,\mathfrak{p}}(\rho)}) = \mathbf{Q}(\sqrt{p})$ où $p \not\equiv -1 \mod 4$. Il existe dans $\mathbf{Q}(\sqrt{p})$ une unité de norme -1; on choisit ρ dans une classe de $G_{\mathbf{Q}}$-conjugaison de $R^s(G_K)$, on choisit $\epsilon_{\mathfrak{p}}(\pi\rho)$ ayant le signe de $W_{K,\mathfrak{p}}(\pi\rho)$, et on pose, pour $\sigma \in G_{\mathbf{Q}}$,

$$y_K(\rho^\sigma) = \prod_{\mathfrak{p} \in \mathfrak{P}(\mathbf{Z}_K)} \sigma \circ \pi^{-1}(\epsilon_{\mathfrak{p}}(\pi\rho)).$$

La fonction y_K ainsi construite répond à la question.

Remarque. – La deuxième partie de cette proposition est une généralisation de la proposition 6.1 de [11] établie dans le cas où ρ est une représentation de G_K fidèle sur un groupe quaternionien.

Soit ℓ un nombre premier, on note $\mathrm{Ker}\, d_\ell$ l'ensemble des éléments ρ de $R(G_K)$ dont le caractère est nul sur les éléments d'ordre premier à ℓ de $G_K/\mathrm{Ker}\,\rho$ où $\mathrm{Ker}\,\rho$ a été défini comme étant le plus grand sous-groupe ouvert de G_K tel que ρ appartienne à $\mathcal{K}_0(\overline{\mathbf{Q}}[G_K/\mathrm{Ker}\,\rho])$. Comme ρ est de dimension 0, le caractère de ρ est nul sur $\mathrm{Ker}\,\rho$.

Soit $\mathfrak{L}$ l'ensemble des idéaux premiers de $\overline{\mathbf{Z}}$ au-dessus de ℓ ($\mathfrak{L} \cap \mathbf{Z} = \ell\mathbf{Z}$). Soit $x, y \in \mathbf{Z}$ on dit que x est congru à y mod $\mathfrak{L}$, on le note $x \equiv y \mod \mathfrak{L}$, si et seulement si $x - y$ appartient à tous les idéaux premiers de $\mathfrak{L}$.

On a la proposition suivante (voir [7] théorème 6.5) :

PROPOSITION 1.8. – *Pour tout idéal premier $\mathfrak{p}$ de $\mathbf{Z}_K$ et pour tout nombre premier ℓ tel que $\ell \notin \mathfrak{p}$, on a :*

$$\forall \rho \in \mathrm{Ker}\, d_\ell \qquad \tau_{K,\mathfrak{p}}(\rho) \equiv \mathrm{Det}_{\rho^{G_K^0}}(-F_{K,\mathfrak{p}})^{-1} \mod \mathfrak{L}.$$

COROLLAIRE 1.9. – *Pour tout idéal premier $\mathfrak{p}$ de $\mathbf{Z}_K$ et pour tout nombre premier ℓ tel que $\ell \notin \mathfrak{p}$; on a :*

$$\forall \rho \in \mathrm{Ker}\, d_\ell \qquad f_{K,\mathfrak{p}}(\rho) \equiv 1 \mod \mathfrak{L}.$$

Démonstration. – Le corollaire 1.9 se déduit de la proposition 1.8 et de la proposition 1.6. Montrons la proposition 1.8 ; le groupe $\mathrm{Ker}\, d_\ell$ est engendré par les éléments de la forme $\mathrm{Ind}_F^K(\rho' - \rho'')$ où ρ' et ρ'' sont de dimension 1 et $\mathrm{Tr}\,\rho' \equiv \mathrm{Tr}\,\rho'' \mod \mathfrak{L}$ ([7], proposition 1.8). La propriété d'invariance par induction permet de se ramener au cas où $G_K/\mathrm{Ker}\,\rho$ est abélien, et $\rho = \rho' - \rho''$ où ρ' et ρ'' sont de dimension 1 et $\mathrm{Tr}\,\rho' \equiv \mathrm{Tr}\,\rho'' \mod \mathfrak{L}$. On a alors :

$$\tau_{K,\mathfrak{p}}(\rho)\ \mathrm{Det}_{\rho^{G_K^0}}(-F_{K,\mathfrak{p}}) = \mathrm{Det}_\rho(t_{\mathfrak{p}}(L/K))$$

où L est un corps de rayon assez gros contenant $\overline{\mathbf{Q}}^{\mathrm{Ker}\,\rho}$. Il existe un entier n tel que $t(L/K)$ appartienne à $p^n\overline{\mathbf{Z}}[G_n/G_L]$ où p est la caractéristique de $\mathbf{Z}_K/\mathfrak{p}\mathbf{Z}_K$. Comme $\ell \neq p$, on déduit que $\mathrm{Det}_{\rho'}(t(L/K))$ est une unité en $\mathfrak{L}$ et

$$\mathrm{Det}_{\rho'}(t(L/K)) \times \mathrm{Det}_{\rho''}(t(L/K))^{-1} \equiv 1 \text{ modulo } \mathfrak{L}.$$

On introduit la notation suivante qui sera utilisée dans le paragraphe 4. On pose pour $\rho \in R(G_K)$

$$\tau^0_{K,\mathfrak{p}}(\rho) = \tau_{K,\mathfrak{p}}(\rho)\ \mathrm{Det}_{\rho^{G^0_K}}(-F_{K,\mathfrak{p}}).$$

On a donc :

$$\tau^0_{K,\mathfrak{p}}(\rho) \equiv 1 \mod \mathfrak{L} \quad \text{pour tout} \quad \rho \in \mathrm{Ker}\, d_\ell \quad \text{et tout} \quad \ell \notin \mathfrak{p}.$$

Soit G_N un sous-groupe ouvert de G_K et $\Delta_{N/K}$ le discriminant de N sur K, on pose pour $\rho \in R(G_K)$ tel que $\mathrm{Ker}\,\rho \supset G_N$

$$\tau^0_{N/K,\mathfrak{p}}(\rho) = \tau^0_{K,\mathfrak{p}}(\rho),$$

$\tau^0_{N/K}(\rho)$ égal au produit des $\tau^0_{K,\mathfrak{p}}(\rho)$ pour $\mathfrak{p}$ divisant $\Delta_{N/K} \prod_{\mathfrak{p}} \mathfrak{p}^{d_{\mathfrak{p}}(\psi_K)}$. Pour tout nombre premier p, on pose :

$$\tau^0_{N/K,p} = \prod_{\mathfrak{p}/p} \tau^0_{N/K,\mathfrak{p}}.$$

On définit ainsi des homomorphismes de $\mathcal{K}_0(\mathbf{Q}[G_K/G_N])$ dans $\overline{\mathbf{Q}}^*$ vérifiant les propriétés 1 à 4 du théorème 1.4.

2. Résolvante.

a) *Invariant relatif de* $\mathfrak{o}[\Gamma]$*-réseaux*

On introduit tout d'abord une généralisation aux algèbres de groupes de la notion d'invariant relatif de deux réseaux.

Soit $\mathfrak{o}$ un anneau de Dedekind, K son corps des fractions, $\mathcal{P}(\mathfrak{o})$ l'ensemble des idéaux premiers non nuls de $\mathfrak{o}$. On suppose que K est de caractéristique 0 et que pour tout $\mathfrak{p} \in \mathcal{P}(\mathfrak{o})$, $\mathfrak{o}/\mathfrak{p}\mathfrak{o}$ est un corps fini.

Soit Γ un groupe fini. On note $R(\Gamma)$ le groupe des caractères de Γ à valeurs dans un clôture algébrique $\overline{K}$ de K. Il s'identifie au groupe de Grothendieck $\mathcal{K}_0(\overline{K}[\Gamma])$. Pour tout idéal $\mathfrak{p}$ de $\mathfrak{o}$, on note $P_{\mathfrak{p}}(\Gamma)$ le sous-groupe de $R(\Gamma)$ formé des caractères nuls sur les éléments de Γ d'ordre appartenant à $\mathfrak{p}$.

On fixe une partie S de l'ensemble $\mathcal{P}(\mathfrak{o})$. L'indexation par un élément $\mathfrak{p}$ de $\mathcal{P}(\mathfrak{o})$ désignera la complétion en $\mathfrak{p}$. Ainsi $\overline{K}_{\mathfrak{p}}$ désigne l'algèbre commutative $\overline{K} \otimes_K K_{\mathfrak{p}}$ et $\overline{\mathfrak{o}}_{\mathfrak{p}}$ l'algèbre $\overline{\mathfrak{o}} \otimes_{\mathfrak{o}} \overline{\mathfrak{o}}_{\mathfrak{p}}$ où $\overline{\mathfrak{o}}$ est la clôture intégrale de $\mathfrak{o}$ dans $\overline{K}$.

Soit $\mathcal{K}^S_{0,\mathrm{rel}}(\mathfrak{o}[\Gamma])$ le groupe de Grothendieck relatif de la catégorie $\mathcal{C}^S_{\ell p}(\mathfrak{o}[\Gamma])$ des $\mathfrak{o}[\Gamma]$-modules de type fini, sans $\mathfrak{o}$-torsion et localement projectifs pour tout $\mathfrak{p}$ dans $\mathcal{P}(\mathfrak{o}) - S$. Ce groupe est engendré par les classes d'isomorphismes d'éléments de la forme

$[M, \alpha, N]$ où M, N sont dans $\mathcal{C}^S_{\mathfrak{L}_p}([\Gamma])$ et α est un $K[\Gamma]$ automorphisme de $K \otimes_{\mathfrak{o}} M$ dans $K \otimes_{\mathfrak{o}} N$ (voir [18], § 1).

Le groupe $\mathcal{K}^S_{0,\mathrm{rel}}(\mathfrak{o}[\Gamma])$ est isomorphe à la somme directe $\bigoplus_{\mathfrak{p} \notin S} \mathcal{K}_{0,\mathrm{rel}}(\mathfrak{o}_{\mathfrak{p}}[\Gamma]) \bigoplus_{\mathfrak{p} \in S} \mathcal{G}^t_0(\mathfrak{o}_{\mathfrak{p}}[\Gamma])$ où $\mathcal{K}_{0,\mathrm{rel}}(\mathfrak{o}_{\mathfrak{p}}[\Gamma])$ s'identifie au groupe de Grothendieck de la catégorie des $\mathfrak{o}_{\mathfrak{p}}[\Gamma]$-modules de $\mathfrak{o}_{\mathfrak{p}}$-torsion qui sont quotient de deux $\mathfrak{o}_{\mathfrak{p}}[\Gamma]$-modules projectifs et $\mathcal{G}^t_0(\mathfrak{o}_{\mathfrak{p}}[\Gamma])$ est le groupe de Grothendieck de la catégorie des $\mathfrak{o}_{\mathfrak{p}}[\Gamma]$-modules de $\mathfrak{o}_{\mathfrak{p}}$-torsion.

Soient X et Y deux $\mathfrak{o}[\Gamma]$-réseaux d'un $K[\Gamma]$-module V de type fini, et appartenant à $\mathcal{C}^S_{\mathfrak{L}_p}(\mathfrak{o})$; on appelle invariant relatif de X et Y l'élément $\chi^S_{\mathfrak{o}[\Gamma]}(X, Y) = [X, 1, Y]$ de $\mathcal{K}^S_{0,\mathrm{rel}}(\mathfrak{o}[\Gamma])$.

Si S est fixé, on le notera plus simplement $\chi_{\mathfrak{o}[\Gamma]}(X, Y)$.

Si $\alpha \in J(M_n(K[\Gamma]))$, groupe des idèles de l'algèbre $M_n(K[\Gamma])$, et X un $\mathfrak{o}[\Gamma]$-réseau de $K[\Gamma]^n$ appartenant à $\mathcal{C}^S_{\mathfrak{L}_p}(\mathfrak{o}[\Gamma])$, on définit $\delta(\alpha)$ par $\delta(\alpha) = \chi_{\mathfrak{o}[\Gamma]}(X, \alpha X)$ où αX est l'unique réseau vérifiant $(\alpha X)_{\mathfrak{p}} = \alpha_{\mathfrak{p}} X_{\mathfrak{p}}$, pour tout $\mathfrak{p}$ dans $\mathcal{P}(\mathfrak{o})$ ($\delta(\alpha)$ ne dépend pas du choix de X).

Pour chaque idéal $\mathfrak{p}$ de $\mathcal{P}(\mathfrak{o})$, on choisit un idéal $\mathfrak{P}$ de $\bar{\mathfrak{o}}$ au-dessus de $\mathfrak{p}$ et on note $G_{K_{\mathfrak{p}}}$ le groupe de Galois de $\overline{K}_{\mathfrak{P}}$ sur $K_{\mathfrak{p}}$; le théorème 6.1 de [18] montre que pour tout $\mathfrak{p} \in \mathcal{P}(\mathfrak{o})$, l'application $\delta_{\mathfrak{p}}$ se factorise par l'application Det en un isomorphisme $\Delta_{\mathfrak{p}}$ rendant commutatif :

– pour $\mathfrak{p} \notin S$, le diagramme suivant :

$$\begin{array}{ccc} \mathrm{Hom}_{G_{K_{\mathfrak{p}}}}(R(\Gamma), \overline{K}^*_{\mathfrak{P}})/\mathrm{Det}(\mathfrak{o}_{\mathfrak{p}}[\Gamma]^*) & \xrightarrow{\Delta_{\mathfrak{p}}} & \mathcal{K}_{0,\mathrm{rel}}(\mathfrak{o}_{\mathfrak{p}}[\Gamma]) \\ & \nwarrow^{\mathrm{Det}} \quad \nearrow_{\delta_{\mathfrak{p}}} & \\ & \mathcal{K}_1(K_{\mathfrak{p}}[\Gamma]) & \end{array}$$

– pour $\mathfrak{p} \in S$ le diagramme suivant :

$$\begin{array}{ccc} \mathrm{Hom}_{G_{K_{\mathfrak{p}}}}(R(\Gamma), \overline{K}^*_{\mathfrak{P}})/H(\mathcal{G}^t_0(\mathfrak{o}_{\mathfrak{p}}[\Gamma])) & \xrightarrow{\Delta_{\mathfrak{p}}} & \mathcal{G}^t_0(\mathfrak{o}_{\mathfrak{p}}[\Gamma]) \\ & \nwarrow^{\mathrm{Det}} \quad \nearrow_{\delta_{\mathfrak{p}}} & \\ & \mathcal{K}_1(K_{\mathfrak{p}}[\Gamma]) & \end{array}$$

où $\mathcal{K}_1(K_\mathfrak{p}[\Gamma])$ est le quotient de $\varinjlim GL_n(K_\mathfrak{p}[\Gamma]))$ par son sous-groupe des commutateurs et

$$H(\mathcal{G}_0^t(o_\mathfrak{p}[\Gamma])) = \{f \in \mathrm{Hom}_{G_{K_\mathfrak{p}}}(R(\Gamma), \overline{K}_\mathfrak{P}^*),\ f(P_\mathfrak{p}(\Gamma)) \subset \overline{o}_\mathfrak{P}^*\}.$$

Si K est un corps de nombres, on en déduit, en utilisant les résultats de [18], (théorème 6.1), le diagramme commutatif suivant : soit Ω^S le groupe

$$\bigoplus_{\mathfrak{p}\notin S} \mathrm{Hom}_{G_{K_\mathfrak{p}}}(R(\Gamma), \overline{K}_\mathfrak{P}^*)/\mathrm{Det}(o_\mathfrak{p}[\Gamma]^*) \qquad \bigoplus_{\mathfrak{p}\in S} \mathrm{Hom}_{G_{K_\mathfrak{p}}}(R(\Gamma), \overline{K}_\mathfrak{P}^*)/H(\mathcal{G}_0^t(o_\mathfrak{p}[\Gamma]))$$

$$\begin{array}{ccc} \mathcal{K}^S_{0,\mathrm{rel}}(o[\Gamma]) & \xrightarrow{\ \sim\ } & \bigoplus_{\mathfrak{p}\notin S} \mathcal{K}_{0,\mathrm{rel}}(o_\mathfrak{p}[\Gamma]) \bigoplus_{\mathfrak{p}\in S} \mathcal{G}_0^t(o_\mathfrak{p}[\Gamma]) \\ \Delta \uparrow\wr & & \oplus\Delta_{o_\mathfrak{p}} \uparrow\wr \\ \mathrm{Hom}_{G_K}(R(G), J(\overline{K}))/H^S(\mathcal{C}^S_{\mathfrak{L}_p}(o[\Gamma])) & \xrightarrow{\ \sim\ } & \Omega^S \end{array}$$

où $H^S(\mathcal{C}^S_{\mathfrak{L}_p}(o[\Gamma]))$ est l'ensemble des $f \in \mathrm{Hom}_{G_K}(R(\Gamma), J(\overline{K}))$ vérifiant :

si $\mathfrak{p} \in S$, $f(P_\mathfrak{p}(\Gamma))_\mathfrak{p} \subset \overline{o}_\mathfrak{P}^*$;

si $\mathfrak{p} \in \mathfrak{P}(o) - S$, il existe $\alpha \in o_\mathfrak{p}[\Gamma]^*$ tel que $\mathrm{Det}_\rho(\alpha) = f(\rho)_\mathfrak{p}$ pour tout $\rho \in R(\Gamma)$;

si $\mathfrak{p} \in \mathfrak{P}_\infty(K)$, $\mathfrak{p}$ réelle, $f(\rho)_\mathfrak{p}$ est réel et positif pour tous les caractères ρ symplectiques de Γ (i.e. $\rho \in R^s(\Gamma)$).

Ces applications étant toutes des isomorphismes, on identifiera ces groupes. On a donc la relation suivante : pour tout $\alpha \in J(M_n(K[\Gamma]))$

$$\chi_{o[\Gamma]}(X, \alpha X) = \mathrm{Det}(\alpha).$$

Il est clair que

$$\chi_{o[\Gamma]}(X, Y) = (\chi_{o_\mathfrak{p}[\Gamma]}(X_\mathfrak{p}, Y_\mathfrak{p}))_{\mathfrak{p}\in\mathfrak{P}(o)}$$

où X et Y sont deux $o[\Gamma]$-réseaux de $K[\Gamma]^n$ dans $\mathcal{C}^S_{\mathfrak{L}_p}(o[\Gamma])$.

b) *Discriminant d'un $o[\Gamma]$-réseau par rapport à une forme hermitienne*

L'algèbre $K[\Gamma]$ est munie d'une involution, notée $\lambda \longrightarrow \overline{\lambda}$, définie par $\overline{\lambda} = \sum_{\gamma\in\Gamma} a_\gamma \gamma^{-1}$ si $\lambda = \sum_{\gamma\in\Gamma} a_\gamma \gamma$. Cette involution se prolonge à $J(M_n(K[\Gamma]))$.

Le groupe $R(\Gamma)$ est muni d'une involution, notée $\rho \longrightarrow \rho^*$, par prolongement de l'application qui à un $\overline{K}[\Gamma]$-module V de type fini associe $\mathrm{Hom}_{\overline{K}}(V, \overline{K})$. Par suite, le groupe $\mathrm{Hom}_{G_K}(R(\Gamma), J(\overline{K}))$ est muni d'une involution $f \longmapsto \overline{f}$ où $\overline{f}(\rho) = f(\rho^*)$ pour tout $\rho \in R(\Gamma)$.

On en déduit une involution sur $\mathcal{K}^S_{0,\mathrm{rel}}(o[\Gamma])$. On a $\mathrm{Det}(\overline{\alpha}) = \overline{\mathrm{Det}(\alpha)}$ quel que soit $\alpha \in J(M_n(K[\Gamma]))$ (voir [10], Appendice IX, proposition 2).

Soit V un $K[\Gamma]$-module de rang défini r. Une forme hermitienne sur V est une application T de $V \times V$ dans $K[\Gamma]$ vérifiant les deux conditions suivantes :

i) $\forall v \in V$, l'application $v \longmapsto T(v, v')$ est $K[\Gamma]$-linéaire

ii) $\forall v \in V$, $\forall v \in V'$, $T(v, v') = \overline{T(v', v)}$.

PROPOSITION 2.1. – *Soit* V *un* $K[\Gamma]$*-module de rang défini* r *muni d'une forme hermitienne* T. *Soit* X *un* $o[\Gamma]$ *réseau de* V *localement libre en dehors de* S *et* L *un* $o[\Gamma]$*-réseau libre de base* $(e_1, e_2, \ldots, e_r)$. *L'élément*

$$\mathrm{Det}((T(e_i, e_j))_{i,j})\ \chi_{o[\Gamma]}(L, X)\ \overline{\chi_{o[\Gamma]}(L, X)}$$

de $\mathcal{K}^S_{0,\mathrm{rel}}(o[\Gamma])$ *ne dépend pas du choix du réseau libre* L.

Démonstration. – Soit L' un autre $o[\Gamma]$-réseau libre de base $(e'_1, \ldots, e'_r)$, et soit P la matrice de passage de la base $(e_1, e_2, \ldots, e_r)$ dans la base $(e'_1, e'_2, \ldots, e'_r)$. On a d'une part :

$$\mathrm{Det}((T(e'_i, e'_j))_{i,j}) = \mathrm{Det}(P)\ \mathrm{Det}((T(e_i, e_j)_{i,j}))\ \overline{\mathrm{Det}\, P},$$

et d'autre part

$$\chi_{o[\Gamma]}(L', X) = \mathrm{Det}(P)^{-1}\, \chi_{o[\Gamma]}(L, X).$$

DEFINITION 2.2. – *On appelle discriminant de* X *l'élément*

$$\mathrm{Det}((T(e_i, e_j))_{i,j}))\ \chi_{o[\Gamma]}(L, X)\ \overline{\chi_{o[\Gamma]}(L, X)}\ \textit{de}\ \mathcal{K}^S_{0,\mathrm{rel}}(o[\Gamma])$$

défini par la proposition précédente. On le note $D_T(X)$.

PROPOSITION 2.3. –

1) $D_T(X) = (D_T(X_\mathfrak{P}))_{\mathfrak{P} \in \mathfrak{X}(o)}$.

2) $D_T(X) = D_T(Y)\,\chi_{o[\Gamma]}(X, Y)\,\overline{\chi_{o[\Gamma]}(X, Y)}$ *pour tout* $o[\Gamma]$-*réseau* Y *de* V *dans le* S-*genre de* X.

3) *Si* X *est un* $o[\Gamma]$-*module libre,* $D_T(X) = \mathrm{Det}(T(e_i, e_j)_{i,j})$ *où* $(e_1, \ldots, e_r)$ *est une base de* X *sur* $o[\Gamma]$.

La démonstration découle immédiatement de la définition.

Soit X un $o[\Gamma]$-réseau de V ; on pose

$$X^* = \{v \in V,\ \forall x \in X,\ T(x, v) \in o[\Gamma]\} ;$$

X^* est appelé le dual de X. Il s'identifie à $\mathrm{Hom}_{o[\Gamma]}(X, o[\Gamma])$ en faisant opérer $o[\Gamma]$ par : f^γ est l'homomorphisme $x \longmapsto f(x)\,\gamma^{-1}$, pour tout γ dans Γ.

PROPOSITION 2.4. – *Soit* X *un* $o[\Gamma]$-*réseau de* V *localement libre pour tout* $\mathfrak{p} \in \mathfrak{P}(o)$.

1) $\overline{\chi_{o[\Gamma]}(X, Y)} = \chi_{o[\Gamma]}(Y^*, X^*)$ *pour tout* $o[\Gamma]$-*réseau* Y *de* V *dans* $\mathfrak{C}_{\mathfrak{Q}\mathfrak{p}}(o[\Gamma])$.

2) $D_T(X) = \chi_{o[\Gamma]}(X, X^*)$.

Démonstration. – En complétant on se ramène au cas où X est libre sur $o_\mathfrak{p}[\Gamma]$. Soit $(e_1, \ldots, e_r)$ une base, il existe alors une base duale $(e_1^*, \ldots, e_r^*)$. Il est clair que X^* a pour base $(e_1^*, \ldots, e_r^*)$. Il existe $\alpha \in \mathrm{GL}_n(o_\mathfrak{p}[\Gamma])$ tel que $X = \alpha Y$, $\chi_{o_\mathfrak{p}[\Gamma]}(X, Y) = \mathrm{Det}(\alpha)$. On a $Y^* = \overline{\alpha} X^*$. Donc $\overline{\mathrm{Det}(\alpha)} = \chi_{o_\mathfrak{p}[\Gamma]}(Y^*, X^*)$.

c) *Radicaux*

Ce paragraphe unifie les notions introduites par A. Fröhlich dans [8], [9] et l'appendice de [10] en généralisant la définition de radical.

Soit $\mathcal{K}_1(\overline{K}[\Gamma])$ le groupe de Whitehead de la catégorie suivante : les objets sont les couples (V, f) où V est un $\overline{K}[\Gamma]$-module de type fini et f est un $\overline{K}[\Gamma]$-automorphisme de V ; les morphismes de (V, f) dans (V', f') sont les applications φ de V dans V' telles que $\varphi \circ f = f' \circ \varphi$ (voir [18], § 1).

On suppose pour la suite que l'application induite par l'extension des scalaires de $\mathcal{K}_1(K[\Gamma])$ *dans* $\mathcal{K}_1(\overline{K}[\Gamma])$ est injective. C'est en particulier le cas lorsque K est un corps de nombres (voir [18], proposition 2.8) ou un corps local.

DEFINITION 2.5. – *On appelle radical de* $\mathcal{K}_1(\overline{K}[\Gamma])$ *un élément* x *vérifiant : il existe un entier* n *tel que* $nx \in \mathcal{K}_1(K[\Gamma])$.

Les radicaux de $\mathcal{K}_1(\overline{K}[\Gamma])$ forment un groupe, noté $\mathcal{R}(\Gamma, K)$.

Ce groupe est le sous-groupe de $\mathcal{K}_1(\overline{K}[\Gamma])$ engendré par les classes des couples (V, f) où V est un $\overline{K}[\Gamma]$-module de type fini sur lequel G_K opère par automorphisme semi-linéaire, (c'est-à-dire que pour tout $g \in G_K$, il existe un K-automorphisme, encore noté g, de V dans V tel que $\forall \lambda \in \overline{K}$, $\forall v \in V$, $g(\lambda v) = g(\lambda)\, g(v)$) et f est tel qu'il existe un entier n tel que f^n commute avec l'action de G_K. Ces conditions entraînent que (V, f^n) est rationnel sur K (voir [1], § 8, n° 7).

On note $\mathfrak{R}(\Gamma, K)$ le quotient de $\mathcal{R}(\Gamma, K)$ par $\mathcal{K}_1(K[\Gamma])$. On a donc une suite exacte

$$1 \longrightarrow \mathcal{K}_1(K[\Gamma]) \longrightarrow \mathcal{R}(\Gamma, K) \longrightarrow \mathfrak{R}(\Gamma, K) \longrightarrow 1.$$

Comme K est assez gros, l'application Det est un isomorphisme de $\mathcal{K}_1(\overline{K}[\Gamma])$ sur $\mathrm{Hom}(R(\Gamma), \overline{K}^*)$ ([18], proposition 2.2). Le groupe $\mathcal{R}(\Gamma, K)$ a pour image l'ensemble des homomorphismes h de $R(\Gamma)$ dans $\overline{K}^*$ tels que h^n appartienne à $\mathrm{Det}(\mathcal{K}_1(K[\Gamma]))$ pour un certain entier n. Le groupe $\mathrm{Det}(\mathcal{K}_1(K[\Gamma]))$ est égal à l'image de $K[\Gamma]^*$ par l'application Det définie par A. Fröhlich ([10]).

On fait opérer G_K sur $\mathrm{Hom}(R(\Gamma), \overline{K}^*)$ en posant, pour $\rho \in R(\Gamma)$, $h^g(\rho) = g h(\rho^{g^{-1}})$; pour cette action, $\mathrm{Hom}(R(\Gamma), \overline{K}^*)$ est un G_K-module topologique et $\mathrm{Hom}_{G_K}(R(\Gamma), \overline{K}^*)$ est l'ensemble des éléments fixes par G_K. On a

$$\mathrm{Det}(\mathcal{K}_1(K[\Gamma])) \subset \mathrm{Hom}_{G_K}(R(\Gamma), \overline{K}^*).$$

On en déduit une action de G_K sur $\mathcal{R}(\Gamma, K)$, $\mathfrak{R}(\Gamma, K)$ et $\mathcal{K}_1(\overline{K}[\Gamma])$. Cette action est l'action naturelle définie dans [18], § 2.

Soit $\Phi = \mathrm{Hom}(G_K, \mathcal{K}_1(K[\Gamma]))$ l'ensemble des homomorphismes continus de G_K dans $\mathcal{K}_1(K[\Gamma])$. On note $\mathcal{R}_\Phi(\Gamma, K)$ le sous-groupe de $\mathcal{R}(\Gamma, K)$ tel que

$$\mathcal{R}_\Phi(\Gamma, K) = \{h \in \mathcal{R}(\Gamma, K),\ \exists \phi \in \Phi,\ h^g = \phi(g)\, h,\ \forall g \in G_K\} ;$$

c'est le sous-groupe de $\mathcal{R}(\Gamma, K)$ engendré par les éléments (V, f) tels que V est un $\overline{K}[G]$-module de type fini sur lequel G_K opère par automorphismes semi-linéaires et tel que pour tout $g \in G_K$, il existe φ_g un $\overline{K}[\Gamma]$-automorphisme de V commutant avec l'action de

G_K et ψ_g un $\overline{K}[\Gamma]$-homomorphisme de V sur V^g tels que $\psi_g^{-1} \circ f \circ \psi_g = f \circ \varphi_g$.

On a $\mathcal{R}(\Gamma, K)^{G_K} \subset \mathcal{R}_\Phi(\Gamma, K) \subset \mathcal{R}(\Gamma, K)$. En effet, le sous-groupe de G_K laissant un élément h de $\mathrm{Det}(\mathcal{R}_\Phi(\Gamma, K))$ fixe est d'indice fini n ; il est clair que $h^n \in \mathrm{Hom}_{G_K}(R(\Gamma), \overline{K}^*)$. Comme $\mathrm{Det}(\mathcal{K}_1(K[\Gamma]))$ est d'indice fini dans $\mathrm{Hom}_{G_K}(R(\Gamma), \overline{K}^*)$, il existe un entier n' tel que $h^{n'}$ appartienne à $\mathrm{Det}(\mathcal{K}_1(K[\Gamma]))$. Soit $\overline{x} \in \mathfrak{R}(\Gamma, K)^{G_K}$ représenté par $x \in \mathcal{R}(\Gamma, K)$; l'application ϕ^x définie par $\phi^x(g) = x^g x^{-1}$ appartient à Φ.

PROPOSITION 2.6. – *L'application* $x \longrightarrow \phi^x$ *est un homomorphisme surjectif de* $\mathfrak{R}(\Gamma, K)^{G_K}$ *dans* Φ *de noyau*

$$\mathcal{R}(\Gamma, K)^{G_K} / \mathcal{K}_1(K[\Gamma]).$$

Démonstration. – On considère la suite exacte :

$$1 \longrightarrow \mathcal{R}(\Gamma, K) \longrightarrow \mathcal{K}_1(\overline{K}[\Gamma]) \longrightarrow \mathcal{K}_1(\overline{K}[\Gamma])/\mathcal{R}(\Gamma, K) \longrightarrow 1 .$$

Le groupe $\mathcal{K}_1(\overline{K}[\Gamma/)/\mathcal{R}(\Gamma, K)$ est par définition sans torsion ; comme $H^0(G_K, \mathcal{K}_1(K[\Gamma])/\mathcal{R}(\Gamma, K))$ est de torsion, ce dernier groupe est trivial. Par le théorème 90 de Hilbert $H^1(G_K, \mathcal{K}_1(\overline{K}[\Gamma]))$ est trivial ; donc $H^1(G_K, \mathcal{R}(\Gamma, K))$ est trivial. En utilisant la suite exacte :

$$1 \longrightarrow \mathcal{K}_1(K[\Gamma]) \longrightarrow \mathcal{R}(\Gamma, K) \longrightarrow \mathfrak{R}(\Gamma, K) \longrightarrow 1$$

on déduit la suite exacte :

$$\mathcal{K}_1(K[\Gamma]) \longrightarrow \mathcal{R}(\Gamma, K)^{G_K} \longrightarrow \mathfrak{R}(\Gamma, K)^{G_K} \xrightarrow{\partial} \mathrm{Hom}(G_K, \mathcal{K}_1(K[\Gamma])) \longrightarrow 1 .$$

Il est clair que le cobord ∂ donne l'application de la proposition 2.5.

La suite suivante est exacte :

$$1 \longrightarrow \mathcal{K}_1(K[\Gamma]) \longrightarrow \mathcal{R}_\Phi(\Gamma, K) \longrightarrow \mathfrak{R}(\Gamma, K)^{G_K} \longrightarrow 1 .$$

Au moyen de l'application Det, on identifie $\mathcal{K}_1(\overline{K}[\Gamma])$ et $\mathrm{Hom}(R(\Gamma), \overline{K}^*)$; ainsi $\mathcal{K}_1(K[\Gamma])$ s'identifie à un sous-groupe de $\mathrm{Hom}_{G_K}(R(\Gamma), \overline{K}^*)$ et Φ à $\mathrm{Hom}(G_K, \mathrm{Det}(\mathcal{K}_1(K[\Gamma])))$.

On note $\mathrm{Hom}_{G_K, \Phi}(R(\Gamma), J(\overline{K}))$, l'ensemble des homomorphismes h de $R(\Gamma)$ dans $J(\overline{K})$ tels qu'il existe ϕ appartenant à Φ vérifiant :

$$\forall \rho \in R(\Gamma),\ \forall g \in G_K,\ h^g(\rho) = h(\rho)\ \phi_\rho(g).$$

On note $\mathfrak{R}^S(\Gamma, o)$ *le quotient de* $\mathrm{Hom}_{G_{K,\Phi}}(R(\Gamma), J(\overline{K}))$ *par le sous-groupe* $H^S(\mathcal{C}^S_{\mathfrak{L}\rho}(o[\Gamma]))$ (voir 1.a).

Le groupe $\mathfrak{R}(\Gamma, K)$ est isomorphe à

$$\mathrm{Hom}_{G_{K,\Phi}}(R(\Gamma), J(\overline{K}))/\mathrm{Hom}_{G_K}(R(\Gamma), J(\overline{K})).$$

On en déduit un diagramme commutatif avec suites exactes :

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{K}_1(K[\Gamma]) & \longrightarrow & \mathcal{R}_\Phi(\Gamma, K) & \longrightarrow & \mathfrak{R}(\Gamma, K)^{G_K} & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \delta} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathcal{K}^S_{0,\mathrm{rel}}(o[\Gamma]) & \longrightarrow & \mathfrak{R}^S(\Gamma, o) & \longrightarrow & \mathfrak{R}(\Gamma, K)^{G_K} & & \\
 & & \downarrow{\scriptstyle \nu} & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \widetilde{\mathcal{K}}^S_0(o[\Gamma]) & = & \widetilde{\mathcal{K}}^S_0(o[\Gamma]) & \longrightarrow & 1 & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1 & & & &
\end{array}$$

où la suite de gauche a été introduite dans [18] (théorème 1.14) et $\widetilde{\mathcal{K}}^S_0(o(\Gamma))$ est le sous-groupe de torsion du groupe de Grothendieck $\mathcal{K}^S_0(o(\Gamma))$ de la catégorie des $o(\Gamma)$-modules de type fini sans o-torsion localement projectifs en dehors de S.

Ce diagramme est l'analogue du diagramme 2.A.II de [9].

Si $h \in \mathrm{Hom}_{G_{K,\Phi}}(R(\Gamma), J(\overline{K}))$, il existe un entier n tel que h^n appartienne à $\mathrm{Hom}_{G_K}(R(\Gamma), J(\overline{K}))$. L'application $h \longrightarrow \Delta(h^n) \otimes (1/n)$ se factorise en un homomorphisme j de $\mathfrak{R}^S(\Gamma, o)$ dans

$$\mathcal{K}^S_{0,\mathrm{rel}}(o[\Gamma]) \otimes_{\mathbf{Z}} \mathbf{Q}.$$

On en déduit un diagramme commutatif avec suites exactes :

$$\begin{array}{ccccccc}
1 \longrightarrow \mathcal{K}^S_{0,\mathrm{rel}}(o[\Gamma]) & \longrightarrow & \mathfrak{R}^S(\Gamma, o) & \longrightarrow & \mathfrak{R}(\Gamma, K)^{G_K} & & \\
\| & & \downarrow{\scriptstyle h} & & \downarrow & & \\
\mathcal{K}^S_{0,\mathrm{rel}}(o[\Gamma]) & \longrightarrow & \mathcal{K}^S_{0,\mathrm{rel}}(o[\Gamma]) \otimes_{\mathbf{Z}} \mathbf{Q} & \longrightarrow & \mathcal{K}^S_{0,\mathrm{rel}}(o[\Gamma]) \otimes_{\mathbf{Z}} (\mathbf{Q}/\mathbf{Z}) & \longrightarrow & 1
\end{array}$$

d) *Résolvante*

Dans ce paragraphe, on applique les résultats des paragraphes précédents à la situation suivante : soit N une extension finie de K et Γ un groupe d'automorphismes de N laissant K fixe ($N^{\Gamma} \supset K$). Soit $tr_{N/K}$ l'application trace de N sur K.

Le corps N est un $K[\Gamma]$-module de rang r égal au degré $[N^{\Gamma} : K]$, de N^{Γ} sur K. On construit à partir de l'application $tr_{N/K}$ une forme hermitienne sur N dans $K[\Gamma]$ en posant :

$$\forall x, y \in N, \quad Tr_{N/K}(x, y) = \sum_{\gamma \in \Gamma} tr_{N/K}(x\gamma(y))\,\gamma = \sum_{\gamma \in \Gamma} tr_{N/K}(\gamma^{-1}(x)\,y)\,\gamma.$$

Soit $\mathcal{B} = (e_1, \ldots, e_r)$ une base de N sur $K[\Gamma]$. Les conjugués des éléments de $\mathcal{B}$ engendrent une K-base de N sur K, appelée base normale de N sur K.

Soit $(\sigma_1, \ldots, \sigma_r)$ un système de représentants des orbites de Γ dans l'ensemble noté $Is_K(N, \overline{K})$ des K-isomorphismes de N dans $\overline{K}$.

Les notions utilisées dans le lemme suivant ont été introduites par A. Fröhlich dans [11]. Je renvoie à [11] pour les démonstrations des résultats de ce paragraphe.

LEMME 2.8. — *Soit* $M_{\mathcal{B}}$ *la matrice*

$$\left(\sum_{\gamma \in \Gamma} \sigma_j \circ \gamma(e_i)\,\gamma^{-1} \right)_{i,j} \in M_r(\overline{K}[\Gamma])$$

alors $(T(e_i, e_j))_{i,j} = M_{\mathcal{B}}\,{}^t\overline{M}_{\mathcal{B}}$, $M_{\mathcal{B}}$ *appartient à* $GL_r(\overline{K}[\Gamma])$.

Soit $\mathcal{B}'$ *une autre base de* N *sur* $K[\Gamma]$ *et soit* $\lambda \in GL_r(K[\Gamma])$ *la matrice de changement de base, alors* $\mathrm{Det}(M_{\mathcal{B}'}) = \mathrm{Det}(M_{\mathcal{B}}) \cdot \mathrm{Det}(\lambda)$.

La classe de $(\overline{K} \otimes_K N, M_{\mathcal{B}})$ *dans* $\mathfrak{R}(\Gamma, K)$ *ne dépend pas du choix du système de représentants des orbites de* Γ *dans* $Is_K(N, \overline{K})$ *ni de la base* $\mathcal{B}$.

DÉFINITION 2.9. — *On appelle résolvante de* N *la classe* $(\overline{K} \otimes_K N, M_{\mathcal{B}})$ *dans* $\mathfrak{R}(\Gamma, N)$.

On la note $r(N, K[\Gamma])$. L'image par l'application Det de $r(N, K[\Gamma])$ dans $\mathrm{Hom}(R(\Gamma), \overline{K}^*)/\mathrm{Det}(K[\Gamma]^*)$ est donnée par la classe de l'homomorphisme $\rho \longrightarrow \mathrm{Det}_{\rho}(M_{\mathcal{B}})$, noté aussi $\rho \longmapsto (\mathcal{B} \mid \rho)$.

PROPOSITION 2.10. — *Soit* ϕ^N *l'application de* G_K *dans* $\mathrm{Det}(K[\Gamma]^*)$ *définie par :*

$$\forall g \in G_K\ ,\ \phi_g^N(\rho) = \mathrm{Det}_\rho \circ \mathrm{Ver}_{N^\Gamma/K}(g)\ \mathrm{Det}_{r_{N^\Gamma/K}}(g)^{\dim \rho}$$

où $r_{N^\Gamma/K}$ *est la classe dans* $R(G_K)$ *du* G_K*-module défini par la permutation de* G_K *sur* G_K/G_{N^Γ}. *Alors* $r(N, K[\Gamma])$ *appartient à* $\mathfrak{R}(\Gamma, K)^{G_K}$ *et l'on a*

$$g(\mathcal{B} \mid \rho^{g^{-1}}) = (\mathcal{B} \mid \rho)\ \phi_g^N(\rho)\ ,\ \forall g \in G_K\ ,\ \forall \rho \in R(\Gamma)\ .$$

PROPOSITION 2.11. — *On a les propriétés suivantes :*

1) *Soit* b *une base de* N *sur* $N^\Gamma[\Gamma]$ *et* $(c_i)_{1 \leqslant i \leqslant r}$ *une* K*-base de* N, *alors :*

$$(\mathcal{B} \mid \rho) = \mathfrak{N}_{N^\Gamma/K}(b \mid \rho)\ (\det \sigma_j(c_i)_{i,j})^{\dim \rho}$$

où $\mathfrak{N}_{N^\Gamma/K}(b \mid \rho)$ *est égal à* $\prod_{j=1}^{r} \sigma_j(b \mid \rho^{\sigma_j^{-1}})$ et $\mathcal{B}$ est la base $(bc_i)_{1 \leqslant i \leqslant r}$.

2) *Soit* Δ *un sous-groupe de* Γ, *on note* $\mathcal{B}_\Delta$ *la base*

$$(\mu(e_i))_{1 \leqslant i \leqslant r,\, \mu \in \Gamma/\Delta}$$

de N *en tant que* $K[\Delta]$*-module,* $(\mathcal{B}_\Delta \mid \rho) = (\mathcal{B} \mid \mathrm{Ind}\ \rho)$ *pour tout* ρ *dans* $R(\Delta)$.

3. Résolvante d'un anneau d'entiers d'un corps de nombres.

On garde les hypothèses du paragraphe précédent. On suppose en plus que K est un corps de nombres et que S contient les idéaux premiers $\mathfrak{P}$ de K tels que Γ contienne un automorphisme sauvagement ramifié en $\mathfrak{P}$.

On appelle discriminant de $\mathbf{Z}_N$ (relativement à $\mathrm{Tr}_{N/K}$) l'élément $\Delta_{\mathrm{Tr}_{N/K}}(\mathbf{Z}_N)$ appartenant à $\mathcal{K}_{0,\mathrm{rel}}^S(\mathbf{Z}_K[\Gamma])$.

Soit $\mathcal{B}$ une base de N sur $K[\Gamma]$ et $L_{\mathcal{B}}$ le $\mathbf{Z}_K[\Gamma]$-module libre de base $\mathcal{B}$. On démontre comme au paragraphe 2.b, le lemme suivant :

LEMME 3.1. – *L'élément* $\chi_{\mathbf{Z}_K[\Gamma]}(L_{\mathcal{B}}, \mathbf{Z}_N)\,\mathrm{Det}(M_{\mathcal{B}})$ *de* $\mathfrak{R}^S(\Gamma, \mathbf{Z}_K)$ *ne dépend pas du choix de la base* $\mathcal{B}$ *de* N *sur* $K[\Gamma]$ *ni du choix du système de représentants des orbites de* Γ *dans* $\mathrm{Is}_K(N, \overline{K})$.

DEFINITION 3.2. – *On appelle résolvante de* $\mathbf{Z}_N$, *l'élément de* $\mathfrak{R}^S(\Gamma, \mathbf{Z}_K)$ *défini par le lemme 3.1.*

On le note $r(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])$. On note $r_\mathfrak{p}(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])$ sa composante locale en $\mathfrak{p} \in \mathcal{P}(K)$.

PROPOSITION 3.3. – *Il existe un* $\mathbf{Z}_K[\Gamma]$*-réseau* X *de* N *localement libre pour tout* $\mathfrak{p} \in \mathcal{P}(\mathbf{Z}_K)$ *tel que* $\chi_{\mathbf{Z}_K[\Gamma]}(X, \mathbf{Z}_N) = 0$ *dans* $\mathcal{K}^S_{0,\mathrm{rel}}(\mathbf{Z}_K[\Gamma])$.

Si $\mathcal{B}_\mathfrak{p}$ *est une base de* $X_\mathfrak{p}$ *sur* $\mathbf{Z}_{K_\mathfrak{p}}[\Gamma]$, $r(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])$ *est représenté par l'homomorphisme dont les composantes locales sont les homomorphismes*

$$\rho \longmapsto \mathrm{Det}_\rho(M_{\mathcal{B}_\mathfrak{p}}) = (\mathcal{B}_\mathfrak{p} \mid \rho), \quad (\rho \in R(\Gamma)).$$

Démonstration. – Soit $\mathcal{B}$ une base de N sur $K[\Gamma]$; la surjectivité de l'application $\delta_\mathfrak{p}$ pour tout $\mathfrak{p}$ de $\mathcal{P}(\mathbf{Z}_K)$ entraîne qu'il existe $\alpha \in J(M_r(K[\Gamma]))$ tel que $\chi_{\mathbf{Z}_K[\Gamma]}(L_{\mathcal{B}}, \mathbf{Z}_N) = \mathrm{Det}(\alpha)$. Le module $X = \alpha L_{\mathcal{B}}$ répond la question; l'image de $\mathcal{B}$ par $\alpha_\mathfrak{p}$ est une base de $X_\mathfrak{p}$ pour tout $\mathfrak{p}$. On a :

$$\begin{aligned}\chi_{\mathbf{Z}_K[\Gamma]}(L_{\mathcal{B}}, \mathbf{Z}_N)\,\mathrm{Det}(M_{\mathcal{B}}) &= \mathrm{Det}(\alpha)\,\mathrm{Det}(M_{\mathcal{B}}) \\ &= (\mathrm{Det}(M_{\mathcal{B}_\mathfrak{p}}))_{\mathfrak{p} \in \mathcal{P}(\mathbf{Z}_K)} \qquad \text{(lemme 2.8).}\end{aligned}$$

Remarque. – Si Γ ne contient pas d'automorphisme sauvagement ramifié on peut prendre S vide et X égal à $\mathbf{Z}_N$; $\mathcal{B}_\mathfrak{p}$ est alors une base locale de $\mathbf{Z}_{N_\mathfrak{p}} = \mathbf{Z}_{K_\mathfrak{p}} \otimes_{\mathbf{Z}_K} \mathbf{Z}_N$ sur $\mathbf{Z}_{K_\mathfrak{p}}[\Gamma]$.

On établit maintenant les propriétés fonctorielles des résolvantes. On suppose pour la suite que $N^\Gamma = K$. Le lemme 2.11 permet de généraliser au cas où N^Γ est différent de K. Ces propriétés généralisent celles obtenues par A. Fröhlich dans le cas où S est vide ([10]).

a) *Extension du corps de base.*

Soit Δ un sous-groupe de Γ et F le corps des invariants de Δ. On définit à partir de l'homomorphisme de restriction de $R(\Gamma)$

dans $R(\Delta)$ un homomorphisme, noté ${}^t\mathrm{Res}_\Gamma^\Delta$, de $\mathfrak{R}^S(\Delta, \mathbf{Z}_K)$ dans $\mathfrak{R}^S(\Gamma, \mathbf{Z}_K)$. Soit $f = [\Gamma : \Delta]$.

PROPOSITION 3.4. – *On suppose que* F *est une extension non ramifiée de* K, *alors*

$$ {}^t\mathrm{Res}_\Gamma^\Delta(\mathfrak{r}(\mathbf{Z}_N, \mathbf{Z}_K[\Delta]) = \mathfrak{r}(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])^f .$$

Démonstration. – L'application μ de $F \otimes_K N$ dans $\mathrm{Hom}_{F[\Gamma^0]}(F[\Gamma], N)$ définie par $\mu(x \otimes y)(\gamma) = x\gamma(y)$ est un isomorphisme de $F[\Gamma]$-modules. Comme $\mathfrak{p}$ est non ramifié dans F/K, $\mu(\mathbf{Z}_F \otimes_{\mathbf{Z}_K} \mathbf{Z}_N)$ est égal à $\mathrm{Hom}_{\mathbf{Z}_F[\Gamma^0]}(\mathbf{Z}_F(\Gamma), \mathbf{Z}_N)$ (voir [10] lemme 4.1).

Soit X un réseau libre de N de base b tel que $\chi_{\mathbf{Z}_K[\Gamma]}(X, \mathbf{Z}_N) = 0$. Le produit tensoriel par $\mathbf{Z}_F$ sur $\mathbf{Z}_K$ transforme les suites exactes de $\mathbf{Z}_K[\Gamma]$-modules en suites exactes de $\mathbf{Z}_F[\Gamma]$-modules. On a donc :

$$\chi_{\mathbf{Z}_F[\Gamma]}(\mathbf{Z}_F[\Gamma]\, b,\ \mathbf{Z}_F \otimes_{\mathbf{Z}_K} \mathbf{Z}_N) = 0 .$$

D'où :

$$\chi_{\mathbf{Z}_F[\Delta]}(\mathrm{Hom}_{\mathbf{Z}_F[\Delta]}(\mathbf{Z}_F[\Gamma],\ \mathbf{Z}_F[\Gamma]\, b),\ \mathrm{Hom}_{\mathbf{Z}_F[\Delta]}(\mathbf{Z}_F[\Gamma],\ \mathbf{Z}_N)) = 0 .$$

Soit $a \in N$ tel que $\chi_{\mathbf{Z}_F[\Delta]}(\mathbf{Z}_F[\Delta]\, a, \dot{\mathbf{Z}}_N) = 0$. Comme $\mathbf{Z}_F[\Gamma]$ est un $\mathbf{Z}_F[\Delta]$-module libre, on en déduit que :

$$\chi_{\mathbf{Z}_F[\Delta]}(\mathrm{Hom}_{\mathbf{Z}_F[\Delta]}(\mathbf{Z}_F[\Gamma],\ \mathbf{Z}_F[\Gamma]b),\ \mathrm{Hom}_{\mathbf{Z}_F[\Delta]}(\mathbf{Z}_F[\Gamma], \mathbf{Z}_F[\Delta]a)) = 0 .$$

En tant que $\mathbf{Z}_F[\Gamma]$-modules, les deux modules ci-dessus sont libres engendrés respectivement par f et φ donnés par

$$f(\gamma) = \begin{cases} \gamma(a) & \text{si } \gamma \in \Delta \text{ et } \varphi(\gamma) = \gamma(b) \quad \forall \gamma \in \Gamma \\ 0 & \text{si } \gamma \notin \Delta . \end{cases}$$

Il existe $\lambda \in F(\Gamma)^*$ tel que $\lambda f = \varphi$ et $\mathrm{Det}(\lambda)$ appartient à $H^S(\mathscr{C}^S_{\varrho_\rho}(\mathbf{Z}_F[\Gamma]))$. On a pour tout $\rho \in R(\Gamma)$

$$\begin{aligned}(b \mid \rho) &= \mathrm{Det}_\rho\Big(\sum_{\gamma\in\Gamma} \gamma(b)\,\gamma^{-1}\Big) = \mathrm{Det}_\rho\Big(\sum_{\gamma\in\Gamma} \varphi^\gamma(1)\,\gamma^{-1}\Big) \\ &= \mathrm{Det}_\rho\Big(\sum_{\gamma\in\Gamma} (\lambda f)^\gamma(1)\,\gamma^{-1}\Big) = \mathrm{Det}_\rho(\lambda)\ \mathrm{Det}_\rho\Big(\sum_{\gamma\in\Gamma} f^\gamma(1)\,\gamma^{-1}\Big) \\ &= \mathrm{Det}_\rho(\lambda)\ \mathrm{Det}_\rho\Big(\sum_{\gamma\in\Delta} f^\gamma(a)\,\gamma^{-1}\Big) = \mathrm{Det}_\rho(\lambda)\ (a \mid \mathrm{Res}_\Gamma^\Delta(\rho)) .\end{aligned}$$

Soit $(c_\sigma)_{\sigma\in\Gamma/\Delta}$ une base de $\mathbf{Z}_F$ sur $\mathbf{Z}_K$, alors $\mathcal{B} = (ac_\sigma)_{\sigma\in\Gamma/\Delta}$ est un $\mathbf{Z}_K[\Delta]$-base de $\mathbf{Z}_N$. La résolvante $r(\mathbf{Z}_N, \mathbf{Z}_K[\Delta])$ est représentée par

$$h(\rho') = (\mathcal{B}\,|\,\rho') = \mathfrak{N}_{F/K}(a, \rho')\,(\det(\sigma'(c_\sigma))_{\sigma,\sigma'\in\Gamma/\Delta})^{\dim\rho}$$

pour tout $\rho' \in R(\Delta)$ (proposition 2.11). On a donc pour tout ρ dans $R(\Gamma)$

$$h(\mathrm{Res}^\Delta_\Gamma(\rho)) = \mathfrak{N}_{F/K}(b\,|\,\rho)\left(\prod_{\sigma\in\Gamma/\Delta}\mathrm{Det}^\sigma_\rho(\lambda)\right)^{-1}(\det(\sigma'(c_\sigma))_{\sigma,\sigma'\in\Gamma/\Delta})^{\dim\rho'}$$

où $\lambda^\sigma = \sum_\gamma \sigma(\lambda_\gamma)\gamma$ si $\lambda = \sum_\gamma \lambda_\gamma\gamma$ avec $\lambda_\gamma \in F$.

Comme l'extension F/K est non ramifiée, l'homomorphisme $\rho \longmapsto \det(\sigma'(c_\sigma))_{\sigma,\sigma'\in\Gamma/\Delta})^{\dim\rho}$ appartient à $H^S(\mathcal{C}^S_{\mathfrak{L}\rho}(\mathbf{Z}_F[\Gamma])$. Comme $\prod_{\sigma\in\Gamma/\Delta}\mathrm{Det}^\sigma_\rho(\lambda) = \mathrm{Det}_\rho\left(\prod_{\sigma\in\Gamma/\Delta}\lambda^\sigma\right)$ et que $\prod_{\sigma\in\Gamma/\Delta}\lambda^\sigma \in K[\Gamma]^*$, l'homomorphisme $\rho \longmapsto \prod_{\sigma\in\Gamma/\Delta}\mathrm{Det}_\rho(\lambda^\sigma)$ appartient à $H^S(\mathbf{Z}_F[\Delta])$. Comme $\mathfrak{N}_{F/K}(b/\rho) = (b/\rho)^f$ l'homomorphisme ${}^t\mathrm{Res}^\Delta_\Gamma(h)$ représente $r(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])^f$.

On a un homomorphisme de $\mathfrak{R}^S(\Delta, \mathbf{Z}_K)$ dans $\mathfrak{R}^S(\Delta, \mathbf{Z}_F)$, noté $\mathrm{Ext}^{\mathbf{Z}_F}_{\mathbf{Z}_K}$, donné par la surjection canonique de

$$\mathrm{Hom}_{G_K,\Phi}(R(\Gamma), J(\overline{\mathbf{Q}}))/H^S(\mathcal{C}^S_{\mathfrak{L}\rho}(\mathbf{Z}_K[\Gamma]))$$

dans $\mathrm{Hom}_{G_F,\Phi}(R(\Gamma), J(\overline{\mathbf{Q}}))/H^S(\mathcal{C}^S_{\mathfrak{L}\rho}(\mathbf{Z}_F[\Gamma]))$.

La démonstration de la proposition 3.5 donne le résultat plus précis suivant :

PROPOSITION 3.5. — *On a*

$${}^t\mathrm{Res}^\Delta_\Gamma(r(\mathbf{Z}_N, \mathbf{Z}_F[\Delta]) = \mathrm{Ext}^{\mathbf{Z}_F}_{\mathbf{Z}_K}(r(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma]))$$

dans $\mathfrak{R}^S(\Gamma, \mathbf{Z}_F)$.

b) *Restriction aux groupes de décomposition et aux groupes d'inertie.*

Soit $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$. Par complétion en $\mathfrak{p}$ on peut définir comme précédemment la résolvante de $\mathbf{Z}_{N\mathfrak{p}} = \mathbf{Z}_{K\mathfrak{p}} \otimes_{\mathbf{Z}_K} \mathbf{Z}_N$. C'est un élément de

$$\mathrm{Hom}_{G_K,\Phi}(R(\Gamma), \overline{\mathbf{Q}}^*_\mathfrak{p})/H^S(\mathcal{C}^S_{\mathfrak{L}\rho}(\mathbf{Z}_\mathfrak{p}[\Gamma])).$$

Il est clair que cet élément est égal à la $\mathfrak{p}$ -composante $\mathfrak{r}_{\mathfrak{p}}(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])$ de $\mathfrak{r}(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])$.

On choisit un idéal $\mathfrak{P}$ de $\overline{\mathbf{Z}}$ au-dessus de $\mathfrak{p}$ et soit $\mathfrak{q} = \mathfrak{P} \cap \mathbf{Z}_N$. On note $\Gamma(\mathfrak{q})$ le groupe de décomposition de $\mathfrak{q}$ dans Γ et $G_{K_{\mathfrak{p}}}$ le groupe de Galois de $\overline{\mathbf{Q}}_{\mathfrak{P}}$ sur $K_{\mathfrak{p}}(\Gamma(\mathfrak{q}) = G_{K_{\mathfrak{p}}} \cap \Gamma)$. On peut encore définir comme précédemment la résolvante de $\mathbf{Z}_{N_{\mathfrak{q}}}$ considéré comme $\mathbf{Z}_{K_{\mathfrak{p}}}[\Gamma(\mathfrak{q})]$-module ; c'est un élément de

$$\mathfrak{R}^S(\Gamma(\mathfrak{q}), \mathbf{Z}_{K_{\mathfrak{p}}}) = \mathrm{Hom}_{G_{K_{\mathfrak{p}}}\Phi}(R(\Gamma(\mathfrak{q})), \overline{\mathbf{Q}}^*_{\mathfrak{P}})/H^S(\mathcal{C}^S_{\mathfrak{Q}\rho}(\mathbf{Z}_{\mathfrak{p}}[\Gamma])$$

noté $\mathfrak{r}(\mathbf{Z}_{N_{\mathfrak{q}}}, \mathbf{Z}_{K_{\mathfrak{p}}}[\Gamma(\mathfrak{q})])$.

PROPOSITION 3.6. — *Pour tout* $\mathfrak{p} \in \mathcal{P}(\mathbf{Z}_K)$, *l'image de* $\mathfrak{r}_{\mathfrak{p}}(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])$ *dans* $\mathfrak{R}^S(\Gamma, \mathbf{Z}_{K_{\mathfrak{p}}})$ *est égale à*

$$^t\mathrm{Res}_{\Gamma}^{\Gamma(\mathfrak{q})}(\mathfrak{r}(\mathbf{Z}_{N_{\mathfrak{q}}}, \mathbf{Z}_{K_{\mathfrak{p}}}[\Gamma(\mathfrak{q})])).$$

Démonstration. — Soit X un réseau localement libre de N tel que $\chi_{\mathbf{Z}_K[\Gamma]}(X, \mathbf{Z}_N) = 0$ et soit $b_{\mathfrak{p}}$ un générateur de $X_{\mathfrak{p}}$ sur $\mathbf{Z}_{K_{\mathfrak{p}}}[\Gamma]$. On peut choisir $b_{\mathfrak{p}}$ tel que $b_{\mathfrak{p}}$ engendre une base d'un $\mathbf{Z}_{K_{\mathfrak{p}}}[\Gamma(\mathfrak{p})]$-réseau $X'_{\mathfrak{q}}$ de $N_{\mathfrak{q}}$ tel que $X_{\mathfrak{q}}$ soit isomorphe à $\mathbf{Z}_{K_{\mathfrak{p}}}[\Gamma] \otimes_{\mathbf{Z}_{K_{\mathfrak{p}}}[\Gamma(\mathfrak{q})]} X'_{\mathfrak{q}}$ et que $\chi_{\mathbf{Z}_{K_{\mathfrak{p}}}[\Gamma(\mathfrak{q})]}(X'_{\mathfrak{q}}, \mathbf{Z}_{N_{\mathfrak{q}}}) = 0$. Le résultat découle alors de la formule 1.4 de [12].

On reprend les notations précédentes. On note $\Gamma(\mathfrak{q})^0$ le groupe d'inertie de $\mathfrak{q}$ dans Γ. Soit $f_{\mathfrak{q}} = [\Gamma(\mathfrak{q}) : \Gamma(\mathfrak{q})^0]$ l'indice d'inertie de $\mathfrak{q}$.

Comme précédemment, on définit, à partir de l'homomorphisme de restriction de $R(\Gamma(\mathfrak{q}))$ dans $R(\Gamma(\mathfrak{q})^0)$, un homomorphisme, noté $^t\mathrm{Res}^{\Gamma(\mathfrak{q})^0}_{\Gamma(\mathfrak{q})}$ de $\mathfrak{R}^S(\Gamma(\mathfrak{q})^0, \mathbf{Z}_{K_{\mathfrak{p}}})$ dans $\mathfrak{R}^S(\Gamma(\mathfrak{q}), \mathbf{Z}_{K_{\mathfrak{p}}})$.

PROPOSITION 3.7. — *Pour tout* $\mathfrak{p} \in \mathcal{P}(\mathbf{Z}_K)$; *on a*

$$^t\mathrm{Res}^{\Gamma(\mathfrak{q})^0}_{\Gamma(\mathfrak{q})}(\mathfrak{r}(\mathbf{Z}_{N_{\mathfrak{q}}}, \mathbf{Z}_{K_{\mathfrak{p}}}[\Gamma(\mathfrak{q})^0]) = \mathfrak{r}(\mathbf{Z}_{N_{\mathfrak{q}}}, \mathbf{Z}_{K_{\mathfrak{p}}}[\Gamma(\mathfrak{q})])^{f_{\mathfrak{q}}}$$

et

$$^t\mathrm{Res}^{\Gamma(\mathfrak{q})^0}_{\Gamma(\mathfrak{q})}(\mathfrak{r}(\mathbf{Z}_{N_{\mathfrak{q}}}, \mathbf{Z}_{K^0_{\mathfrak{p}}}[\Gamma(\mathfrak{q})^0]) = \mathrm{Ext}^{\mathbf{Z}_{K^0_{\mathfrak{p}}}}_{\mathbf{Z}_{K_{\mathfrak{p}}}}(\mathfrak{r}(\mathbf{Z}_{N_{\mathfrak{q}}}, \mathbf{Z}_{K_{\mathfrak{p}}}[\Gamma(\mathfrak{q})])$$

dans $\mathfrak{R}^S(\Gamma(\mathfrak{q}), \mathbf{Z}_{K^0_{\mathfrak{p}}})$.

Démonstration. – Elle se fait comme celle de la proposition 3.5.

c) *Passage aux groupes quotients.*

Soit Δ un sous-groupe distingué de Γ tel que Δ ne contienne pas d'automorphismes sauvagement ramifiés et tel que l'ordre de Δ n'appartient à aucun $\mathfrak{p}$ dans S.

Soit Σ le quotient Γ/Δ et soit θ la surjection canonique de Γ sur Σ. On en déduit une application, notée θ^*, de $R[\Sigma]$ sur $R[\Gamma]$ en considérant les Σ-modules comme des Γ-modules sur lesquels Δ opère trivialement. Par transposition, on a une application ${}^t\theta^*$ de $\mathrm{Hom}_{G_K,\Phi}(R(\Gamma), J(\bar{\Omega}))$ dans $\mathrm{Hom}_{G_K,\Phi}(R(\Sigma), J(\bar{\Omega}))$, qui applique $H^S(\mathcal{C}^S_{\wp}(\mathbf{Z}_K[\Gamma]))$ dans $H^S(\mathcal{C}^S_{\wp}(\mathbf{Z}_K[\Sigma]))$ d'où une application encore notée ${}^t\theta^*$, de $\mathfrak{R}^S(\Gamma, \mathbf{Z}_K)$ sur $\mathfrak{R}^S(\Sigma, \mathbf{Z}_K)$.

PROPOSITION 3.8. – *On a*

$$ {}^t\theta^*(\mathfrak{r}(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])) = \mathfrak{r}(\mathbf{Z}_N^{\Delta}, \mathbf{Z}_K[\Sigma]). $$

Démonstration. – Soit X un réseau localement libre de N tel que $\chi_{\mathbf{Z}_K[\Gamma]}(X, \mathbf{Z}_N) = 0$ et soit $b_{\mathfrak{p}}$ tel que $X_{\mathfrak{p}} = \mathbf{Z}_K\,[\Gamma]\, b_{\mathfrak{p}}$; on a pour tout $\rho \in R(\Sigma)$,

$$ (b_{\mathfrak{p}} \mid \rho) = (\mathrm{tr}_{N/N^{\Delta}}(b_{\mathfrak{p}}) \mid \rho). $$

Comme, pour tout $\mathfrak{p}$ dans S, l'ordre de Δ n'appartient pas à $\mathfrak{p}$, on a :

$$ \chi_{\mathbf{Z}_K[\Gamma]}\Big(\Big(\sum_{\delta\in\Delta}\delta\Big)(X), \Big(\sum_{\delta\in\Delta}\delta\Big)(\mathbf{Z}_N)\Big) = 0. $$

Enfin comme Δ ne contient pas d'automorphisme sauvagement ramifié, on a : $\Big(\Big(\sum_{\delta\in\Delta}\delta\Big)(\mathbf{Z}_N)\Big) = \mathbf{Z}_N^{\Delta}$.

d) *Restriction du corps de base.*

Soit F un sous-corps de K et soit $\mathrm{Ver}_{K/F}$ le transfert de G_F dans G_K. Par transposition on en déduit un homomorphisme de $\Phi_K = \mathrm{Hom}(G_K, \mathrm{Det}(K[\Gamma]^*))$ dans $\Phi_F = \mathrm{Hom}(G_F, \mathrm{Det}(F[\Gamma]^*))$. L'application qui à $f \in \mathrm{Hom}_{G_K,\Phi_K}(R(\Gamma), J(\bar{\Omega}))$ associe l'homomorphisme $\mathcal{T}_{K/F}(f)$ défini par $\mathcal{T}_{K/f}(f)(\rho) = \prod_{\sigma\in G_K/G_F} \sigma f(\rho^{\sigma^{-1}})$ est un homomorphisme dans $\mathrm{Hom}_{G_F,\Phi_F}(R(\Gamma), J(\bar{\Omega}))$. Si ϕ est

l'homomorphisme de Φ_K associé à f, $\phi \circ \mathrm{Ver}_{K/F}$ est l'homomorphisme, associé à $\mathcal{T}_{K/F}(f)$. Par passage aux quotients, on en déduit un homomorphisme, encore noté $\mathcal{T}_{K/F}$, de $\mathfrak{R}^S(\Gamma, \mathbf{Z}_K)$ dans $\mathfrak{R}^S(\Gamma, \mathbf{Z}_F)$.

Soit $d_{K/F}$ l'élément de $\mathfrak{R}^S(\Gamma, \mathbf{Z}_F)$ défini de la façon suivante : $d_{K/F}$ est représenté par un homomorphisme dont les composantes locales sont données par $\rho \longrightarrow (\det(\sigma'(c_\sigma))_{\sigma',\sigma \in G_K/G_F})^{\dim \rho}$ où c_σ est une base locale de $\mathbf{Z}_F$ sur $\mathbf{Z}_K$. L'homomorphisme associé à $d_{K/F}$ est l'application qui à $g \in G_K$ associe $\rho \longrightarrow \det_{r_{F/K}}(g)^{\dim \rho}$ où $r_{F/K}$ est le caractère de la représentation de permutation de G_F sur G_F/G_K.

PROPOSITION 3.9. – *On a :*

$$\mathfrak{r}(\mathbf{Z}_N, \mathbf{Z}_F[\Gamma]) = d_{K/F}\, \mathcal{T}_{K/F}(\mathfrak{r}(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])).$$

Démonstration. – Le résultat découle immédiatement de la première partie de la proposition 2.11.

On a vu au paragraphe a) que $\mathfrak{R}^S(\Gamma, \mathbf{Z}_K)$ est isomorphe à $\bigoplus_{p \in \mathfrak{P}(\mathbf{Z}_K)} \mathfrak{R}^S(\Gamma, \mathbf{Z}_{K_p})$. Ce dernier se décompose sous la forme :

$$\bigoplus_{q \in \mathfrak{P}(\mathbf{Z}_F)} \bigoplus_{p \mid q} \mathfrak{R}^S(\Gamma, \mathbf{Z}_{K_p}).$$

On en déduit aisément que le diagramme suivant commute :

$$\begin{array}{ccc} \mathfrak{R}^S(\Gamma, \mathbf{Z}_K) & \xrightarrow{\sim} & \bigoplus_{p \in \mathfrak{P}(\mathbf{Z}_K)} \mathfrak{R}^S(\Gamma, \mathbf{Z}_{K_p}) \\ \downarrow \mathcal{T}_{K/F} & & \downarrow \bigoplus_{q \in \mathfrak{P}(\mathbf{Z}_F)} \left(\prod_{p/q} \mathcal{T}_{K_p/F_q} \right) \\ \mathfrak{R}^S(\Gamma, \mathbf{Z}_F) & \xrightarrow{\sim} & \bigoplus_{q \in \mathfrak{P}(\mathbf{Z}_F)} \mathfrak{R}^S(\Gamma, \mathbf{Z}_{F_q}). \end{array}$$

e) *Restriction aux sous-groupes.*

Soit Δ un sous-groupe de Γ, et $\mathrm{Ind}_\Delta^\Gamma$ l'homomorphisme d'induction de $R(\Delta)$ dans $R(\Gamma)$. Par transposition on en déduit un homomorphisme, noté ${}^t\mathrm{Ind}_\Delta^\Gamma$, de $\mathrm{Hom}_{G_{K,\Phi}}(R(\Gamma), J(\overline{\mathbf{Q}}))$ dans $\mathrm{Hom}_{G_{K,\Phi}}(R(\Delta), J(\overline{\mathbf{Q}}))$. Par passage aux quotients, on a donc un homomorphisme encore noté ${}^t\mathrm{Ind}_\Delta^\Gamma$ de $\mathfrak{R}(\Delta, \mathbf{Z}_K)$ dans $\mathfrak{R}(\Gamma, \mathbf{Z}_K)$.

PROPOSITION 3.10. – *On a :*

$${}^{r}\mathrm{Ind}_{\Delta}^{\Gamma}(r(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])) = r(\mathbf{Z}_N, \mathbf{Z}_K[\Delta]) = d_{N^{\Delta}/K}\, \mathcal{T}_{N^{\Delta}/K}(r(\mathbf{Z}_N, \mathbf{Z}_{N^{\Delta}}[\Delta])).$$

Démonstration. – La deuxième égalité résulte de la proposition 3.7.

Soit X un réseau localement libre de N tel que $\chi_{\mathbf{Z}_K[\Gamma]}(X, \mathbf{Z}_N) = 0$ et soit $b_{\mathfrak{p}}$ tel que $X_{\mathfrak{p}} = \mathbf{Z}_{K_{\mathfrak{p}}}[\Gamma]\, b$. Soit $\mathcal{B}_{\Delta,\mathfrak{p}}$ la base de $X_{\mathfrak{p}}$ sur $\mathbf{Z}_{K_{\mathfrak{p}}}[\Delta]$ égale à $(\sigma(b_{\mathfrak{p}}))_{\sigma\in\Gamma/\Delta}$. On a $(\mathcal{B}_{\Delta,\mathfrak{p}} \mid \rho) = (b_{\mathfrak{p}} \mid \mathrm{Ind}(\rho))$ pour tout $\rho \in R(\Delta)$ (proposition 2.11). Le résultat découle alors du fait que $\chi_{\mathbf{Z}_K[\Delta]}(X, \mathbf{Z}_N) = 0$.

4. Structure galoisienne des anneaux d'entiers.

On garde les notations et hypothèses de paragraphe 3.

On plonge $\overline{\mathbf{Q}}^*$ dans la diagonale de $J(\overline{\mathbf{Q}})$. Ainsi la fonction τ_K définie par le théorème 1.4 peut être considérée comme un élément $\mathrm{Hom}_{G_{\mathbf{Q},\Phi}}(R(\Gamma), J(\overline{\mathbf{Q}}))$. La fonction ϕ de Φ associée à τ_K est donnée par la proposition 1.6. On note T_K la classe de τ_K^0 dans $\mathfrak{R}^S(\Gamma, \mathbf{Z})$. Enfin on note $U(\overline{\mathbf{Q}})$ le groupe des idèles unités et $U_p(\overline{\mathbf{Q}}) = \mathbf{Z}_p \otimes_{\mathbf{Z}} \overline{\mathbf{Z}}$.

On suppose que $K = N^{\Gamma}$.

THEOREME 4.1. –

1) $\mathcal{T}_{K/\mathbf{Q}}(r(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma]))\, .\, T_K^{-1}$ *appartient à* $\mathcal{K}_{0,\mathrm{rel}}^S(\mathbf{Z}[\Gamma])$.

2) $\mathcal{T}_{K/\mathbf{Q}}(r(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma]))\, .\, T_K^{-1}$ *est inclus dans* $\mathrm{Hom}_{G_K}(R(\Gamma), U(\overline{\mathbf{Q}}))$.

La première partie de ce théorème découle du fait que la fonction ϕ associe à $\mathcal{T}_{K/\mathbf{Q}}(r(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma]))$ est aussi celle associée à T_K . La deuxième découle de la proposition suivante.

Soit $\mathfrak{p} \in \mathcal{P}(\mathbf{Z}_K)$, la fonction $\tau_{K,\mathfrak{p}}^0$ définit un élément de $\mathrm{Hom}_{G_{\mathbf{Q},\Phi}}(R(\Gamma), J(\overline{\mathbf{Q}}))$. La fonction ϕ de Φ associée à $\tau_{K,\mathfrak{p}}^0$ est donnée par le théorème 5.1 de [17]. On note $T_{K,\mathfrak{p}}$ sa classe dans $\mathfrak{R}^S(\Gamma, \mathbf{Z})$. On a $T_K = \prod_{\mathfrak{p}\in\mathcal{P}(\mathbf{Z}_K)} T_{K,\mathfrak{p}}$.

En utilisant le plongement de $\overline{\mathbf{Q}}_{\mathfrak{p}}^{*}$ dans $J(\overline{\mathbf{Q}})$, la résolvante locale $r_{\mathfrak{p}}(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])$, définie au paragraphe 3, définit un élément de $\mathfrak{R}^S(\Gamma, \mathbf{Z})$ égal à la $\mathfrak{p}$-composante de $r(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])$ à la place $\mathfrak{p}$ et 1 ailleurs. On a $r(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma]) = \prod_{\mathfrak{p} \in \mathfrak{P}(\mathbf{Z}_K)} r_{\mathfrak{p}}(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])$ (cette décomposition locale suffisante pour démontrer le théorème 4.1 n'est pas tout à fait satisfaisante car les fonctions ϕ associées à $r_{\mathfrak{p}}(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])$ et à $T_{K,\mathfrak{p}}$ ne sont pas les mêmes).

PROPOSITION 4.3. – *Si* Γ *ne contient pas d'automorphisme sauvagement ramifié en* $\mathfrak{p}$, $\mathfrak{N}_{K/\mathbf{Q}}(r_{\mathfrak{p}}(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])) \times T_{K,\mathfrak{p}}^{-1}$ *est inclus dans* $\mathrm{Hom}(R(\Gamma), U(\overline{\mathbf{Q}}))$; *sinon pour tout caractère* ρ *nul sur les éléments de* Γ *dont l'ordre appartient à* Γ,

est une unité. $(\mathfrak{N}_{K/\mathbf{Q}}(r_{\mathfrak{p}}(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma])) \cdot T_{K,\mathfrak{p}}^{-1})(\rho)$

Démonstration. – Si Γ ne contient pas d'automorphisme sauvagement ramifié en $\mathfrak{p}$, le résultat est dû à A. Fröhlich ([10], théorème (4.a) sinon on utilise le théorème de Brauer. Il s'agit de montrer que pour tout caractère ρ nul sur les éléments p-singuliers de Γ, on a :

$$\mathfrak{N}_{K/\mathbf{Q}}(r_{\mathfrak{p}}(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma]))(\rho)\, T_{K,\mathfrak{p}}^{-1}(\rho) \in \overline{\mathbf{Z}}_{\mathfrak{p}}^{*}.$$

Il existe une famille finie $\mathfrak{F}$ de sous-groupes élémentaires Δ de Γ et des éléments $\sigma_\Delta \in R(\Delta)$, de dimension 1 tels que :

$$1 = \sum_{\Delta \in \mathfrak{F}} \mathrm{Ind}_{\Delta}^{\Gamma}(\sigma_\Delta),$$

d'où :

$$\rho = \sum_{\Delta \in \mathfrak{F}} \rho\, \mathrm{Ind}_{\Delta}^{\Gamma}(\sigma_\Delta) = \sum_{\Delta \in \mathfrak{F}} \mathrm{Ind}_{\Delta}^{\Gamma}(\sigma_\Delta \mathrm{Res}_{\Gamma}^{\Delta}(\rho)).$$

Le caractère $\sigma_\Delta \mathrm{Res}_{\Gamma}^{\Delta}(\rho)$ est encore nul sur les éléments p-singuliers de Δ. Le groupe Δ est le produit direct d'un p-groupe et d'un groupe abélien C d'ordre premier à p. Il existe $\varphi_C \in R(C)$ tel que $\sigma_\Delta \mathrm{Res}_{\Gamma}^{\Delta}(\rho) = \mathrm{Ind}_{C}^{\Delta}(\varphi_C)$. L'extension N/N^C est modérément ramifiée. Le résultat découle donc de la formule d'induction (proposition 3.10) et du résultat du paragraphe 4 de [15].

Démonstration du théorème 1. – On remarque tout d'abord que :

$$\eta_{\mathbf{Z}[\Gamma]}(\mathfrak{N}_{K/\mathbf{Q}}(r(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma]))\, \mathfrak{N}_{K/\mathbf{Q}}(r(N, K[\Gamma])^{-1})) = \mathrm{Res}_{\mathbf{Z}_K}^{\mathbf{Z}}([\mathbf{Z}_N]\text{-}[\mathbf{Z}_K[\Gamma]])$$

où $\eta_{\mathbf{Z}[\Gamma]}$ est l'application définie dans [18], théorème 4.1. Comme $\mathbf{Z}_K$ est un $\mathbf{Z}$-module libre, on a :

$$\mathrm{Res}^{\mathbf{Z}}_{\mathbf{Z}_K}([\mathbf{Z}_K[\Gamma]]) = [K : \mathbf{Q}]\,[\mathbf{Z}[\Gamma]].$$

Le fait que $\mathcal{R}_{K/\mathbf{Q}}(r(\mathbf{Z}_N, \mathbf{Z}_K[\Gamma]))\,\mathcal{R}_{K/\mathbf{Q}}(r(N, K[\Gamma])^{-1})$ appartienne à $\mathrm{Hom}_{G_{\mathbf{Q}}}(R(\Gamma), \mathbf{Q}^*)\ H(\mathcal{G}^S_*(\mathbf{Z}[\Gamma]))$ (voir [18], théorème 6.1) se déduit du théorème 4.1, de la proposition 1.7 et du fait que $\mathfrak{N}_{K/\mathbf{Q}}(r(N, K[\Gamma])^{-1}(\rho)$ est du signe de $\prod_{\mathfrak{p} \in \mathfrak{P}_\infty(K)} (-1)^{n_{K,\mathfrak{p}}(\rho)/2}$ pour tout caractère simplectique ρ ([10], théorème 10).

Démonstration du théorème 2. – Cette démonstration se fait exactement comme celle du théorème 1 de M.J. Taylor [22] en utilisant les propositions 1.5 et 3.7.

BIBLIOGRAPHIE

[1] N. BOURBAKI, *Algèbre*, chapitre 2, Hermann, Paris, 1968.

[2] J. COUGNARD, Entiers d'une p-extension, *Compos. Math.*, 33 (1976), 303-336.

[3] J. COUGNARD, Une propriété de l'anneau des entiers des extensions galoisiennes non abéliennes de degré pq des rationnels, *Pub. Math., Fac. des Sciences de Besançon*, 1976-1977.

[4] Ph. CASSOU-NOGUES, Structure galoisienne des anneaux d'entiers, *Proc. London Math. Soc.*, 38 (1979), 545-576.

[5] Ph. CASSOU-NOGUES, Module de Frobenius et structure galoisienne des anneaux d'entiers, *J. of Algebra*, 71 (1981), 268-289.

[6] Ph. CASSOU-NOGUES et J. QUEYRUT, Structure galoisienne des anneaux d'entiers (*à paraître Ann. Inst. Fourier*, (1982)).

[7] P. DELIGNE, Les constantes des équations fonctionnelles des fonctions L, Modular functions of one variable II, p. 501-597, *Lecture Notes in Math.*, n° 349, Springer Verlag, 1973.

[8] A. FRÖHLICH, Radical modules over Dedekind domain, *Nagoya Math. Jour.*, 27 (1966), 173-198.

[10] A. FRÖHLICH, Arithmetic and Galois module structure for tame extensions, *J. reine angew. Math.*, 286-287 (1976), 380-439.

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

[12] A. FRÖHLICH, Resolvents and trace forms, *Math. Soc. Cam. Phil. Soc.*, 78 (1975), 185-210.

[13] J.-M. FONTAINE, Groupes de ramification et représentation d'Artin, *Ann. Scient. Ec. Norm. Sup.* 4e série, t. 4 (1971), 337-392.

[14] 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.

[15] A. FRÖHLICH, M.J. TAYLOR, The arithmetic theory of local Galois Gauss sums for tame characters, *Phil. Trans. Roy. Soc.*, 298 (1980), 141-181.

[16] S. LANG, *Algebraic Number Theory*, Addison Wesley.

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

[18] J. QUEYRUT, S-groupes des classes d'un ordre arithmétique (*à paraître J. of Algebra).*

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

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

[21] J.-P. SERRE, Conducteurs d'Artin des caractères réels, *Invent. Math.*, 14 (1971), 173-183.

[22] M.J. TAYLOR, Galois module structure of integers of relative abelian extensions, *J. reine angew. Math.*, 303-304 (1978), 97-101.

[23] M.J. TAYLOR, A logarithmic approach to class groups of integral group rings, *J. of Algebra*, 66 (1980), 321-353.

Jacques QUEYRUT,
U.E.R. de Mathématiques
et d'Informatique
Université de Bordeaux I
F 33405 Talence Cedex.

Manuscrit reçu le 13 mars 1980.
révisé le 17 décembre 1980.