ANNALES DE L'INSTITUT FOURIER

PHILIPPE CASSOU-NOGUÈS

Quelques théorèmes de base normale d'entiers

Annales de l'institut Fourier, tome 28, nº 3 (1978), p. 1-33

<http://www.numdam.org/item?id=AIF_1978__28_3_1_0>

Ann. Inst. Fourier, Grenoble
28, 3 (1978), 1-33

QUELQUES THÉORÈMES DE BASE NORMALE D'ENTIERS

par Philippe CASSOU-NOGUÈS*

1. Introduction.

Soit K un corps de nombres et soit N une extension galoisienne finie de K dont le groupe de Galois est noté Γ. Pour tout corps de nombres L on note O_L son anneau d'entiers. Nous nous intéressons à la structure de module galoisien de O_N c'est-à-dire à sa structure de module sur l'algèbre de groupe $\mathbf{Z}[\Gamma]$ et plus particulièrement à la recherche de cas où O_N est un $\mathbf{Z}[\Gamma]$-module libre. On sait que O_N est un $\mathbf{Z}[\Gamma]$-module projectif si et seulement si N est une extension modérément ramifiée de K ; en particulier seuls les anneaux d'entiers d'extensions modérément ramifiées de K peuvent être des $\mathbf{Z}[\Gamma]$-modules libres ; on suppose cette hypothèse désormais réalisée. Lorsque K est le corps $\mathbf{Q}$ des rationnels on remarque que la propriété pour O_N d'être un $\mathbf{Z}[\Gamma]$-module libre équivaut à l'existence d'une base normale d'entiers c'est-à-dire d'un entier formant avec ses conjugués une base du $\mathbf{Z}$-module O_N.

On sait, par un résultat ancien de Hilbert et Speiser ([18]), que toute extension abélienne modérément ramifiée de $\mathbf{Q}$ possède une base normale d'entiers, par contre Martinet, ([21]), a construit une extension galoisienne de $\mathbf{Q}$ dont le groupe de Galois est le groupe quaternionien H_8 et dont l'anneau d'entiers n'est pas un $\mathbf{Z}[H_8]$-module stablement libre. Ceci nous montre que l'ordre de l'élément $U_{N/K}$ défini par O_N dans le groupe projectif $C(\mathbf{Z}[\Gamma])$ n'est pas toujours égal à 1. Il est apparu récemment qu'il existait un lien très

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

intéressant entre le problème de la structure de module galoisien de O_N et de l'ordre de $U_{N/K}$ et le problème de la détermination des signes des constantes d'équation fonctionnelle des séries L-d'Artin généralisées associées aux caractères symplectiques de Γ. Fröhlich conjecture que $U_{N/K}^2 = 1$ et même que $U_{N/K} = 1$ si les constantes $W(\chi, N/K)$ associées aux caractères symplectiques χ de Γ sont égales à 1. Les théorèmes généraux qui relient $U_{N/K}$ et les constantes $W(, N/K)$ ([5]) ont permis à Fröhlich de démontrer que $U_{N/K}$ appartient au noyau $D(\mathbf{Z}[\Gamma])$ de l'homomorphisme induit par l'extension des scalaires de $C(\mathbf{Z}[\Gamma])$ sur le groupe projectif associé à un ordre maximal de $\mathbf{Q}[\Gamma]$ contenant $\mathbf{Z}[\Gamma]$, ce qui avait été conjecturé par Martinet lorsque K est égal à $\mathbf{Q}$; si K est égal à $\mathbf{Q}$ le théorème de Hilbert et Speiser implique que $U_{N/K}$ appartient au noyau $D_0(\mathbf{Z}[\Gamma])$ de l'homomorphisme naturel défini de $D(\mathbf{Z}[\Gamma])$ sur $D(\mathbf{Z}[\Gamma^{ab}])$ où Γ^{ab} désigne le groupe Γ rendu abélien. Pour tout nombre premier l, Fröhlich définit un groupe $E_l(\Gamma)$ et une projection $h_l(\Gamma)$ de $D(\mathbf{Z}[\Gamma])$ sur ce groupe et en utilisant le lien général qui existe entre $U_{N/K}$ et les sommes de Gauss galoisiennes associées aux caractères de Γ il démontre que $U_{N/K}^2$ ou $U_{N/K}$ appartient au noyau de $h_l(\Gamma)$. Ces résultats ont permis de démontrer la conjecture lorsque Γ est un groupe métacyclique d'ordre lq où l est un nombre premier impair et où K est égal à $\mathbf{Q}$ ([8]) ou un 2-groupe diédral ou quaternionien ([11]).

On peut définir ([5]) un groupe $E(\Gamma)$ et une projection $h(\Gamma)$ de $D(\mathbf{Z}[\Gamma])$ sur $E(\Gamma)$ faisant intervenir simultanément tous les nombres premiers l. Dans un article précédent ([3]) nous avons démontré que $U_{N/K}^2$ ou $U_{N/K}$ appartient au noyau de $h(\Gamma)$, en général strictement contenu ([4a]) dans l'intersection des noyaux des $h_l(\Gamma)$. De manière plus précise, $U_{N/K}$ se décompose dans $D(\mathbf{Z}[\Gamma])$ en un produit $t^+(W_{N/K})\, V_{N/K}$ où $t^+(W_{N/K})$ est un élément d'ordre 1 ou 2 défini à partir des constantes d'équation fonctionnelle des séries L-d'Artin et où $V_{N/K}$ appartient au noyau de $h(\Gamma)$. Dans cet article, nous étudions par les méthodes de la théorie des algèbres de groupes, l'exposant du groupe $\operatorname{Ker} h(\Gamma)$ pour un groupe Γ fini et nous en déduisons des résultats pour l'ordre de $V_{N/K}$ lorsque Γ est le groupe de Galois de N sur K. Le résultat obtenu le plus général est le suivant :

"Pour toute extension modérément ramifiée N d'un corps de nombres K l'ordre de $V_{N/K}$ divise le degré de N sur K, que l'on note $[N : K]$, et même $[N : K]/2$ lorsque ce degré est pair". Une meilleure majoration de cet exposant pour certains groupes métabéliens nous permet de donner des exemples d'extensions N d'un corps de nombres K pour lesquelles $V_{N/K}$ est égal à 1 c'est-à-dire de démontrer la conjecture de Fröhlich dans de nouveaux cas particuliers (corollaires 3.3, 3.5 et 3.6). Plus généralement, pour toute extension N de K dont le groupe de Galois est le groupe quaternionien H_{4m} où m est un nombre entier impair, on montre que la 2-composante de $U_{N/K}$ est égale à $t^+(W_{N/K})$. Ces résultats généralisent les résultats que nous avions obtenus dans [4]. Lorsque Γ est un l-groupe, le groupe $\mathrm{Ker}\, h(\Gamma)$ est égal au groupe $D(\mathbf{Z}[\Gamma])$ et la méthode précédemment décrite ne donne pas de résultats. Notons que dans ce cas M. Taylor ([27]) a défini un autre sous-groupe de $D(\mathbf{Z}[\Gamma])$ auquel appartient $U_{N/K}$ et obtenu l'existence d'une base normale d'entiers lorsque Γ est un groupe métacyclique d'ordre l^3.

Nous avons dans cet article adopté le plan suivant : le paragraphe 2 contient les principales notations. Dans le paragraphe 3 nous donnons les résultats obtenus et nous les démontrons dans les paragraphes 4 et 5 ; enfin, dans le paragraphe 6, nous montrons comment dans le cas particulier du groupe quaternionien H_{4ln} on peut améliorer les résultats généraux du paragraphe 3.

L'article se termine par deux appendices. Dans le premier, nous donnons une interprétation algébrique du sous-groupe $\mathrm{Ker}\, h(\Gamma)$ et des sous-groupes $\mathrm{Ker}\, h_l(\Gamma)$ définis par Fröhlich ([6]) du groupe $D(\mathbf{Z}[\Gamma])$. Dans le second, nous montrons comment les résultats des paragraphes 3 et 6, et de très récents résultats de M. Taylor, dont l'auteur a eu connaissance lors de la rédaction de cet article, permettent de démontrer la conjecture de Fröhlich dans de nouveaux cas particuliers lorsque N est une extension d'un corps de nombres K dont le degré et le discriminant sur K sont premiers entre eux.

2. Notations.

On note A^* le groupe multiplicatif des éléments inversibles d'un anneau A. Si M est une extension de F on note $G(M/F)$ le groupe de Galois de M sur F. Les symboles $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ et $\overline{\mathbf{Q}}$

désignent l'anneau des entiers relatifs, le corps des nombres rationnels, réels, complexes et la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$. Un corps de nombres K est une extension finie de $\mathbf{Q}$ contenue dans $\overline{\mathbf{Q}}$ et l'on note Ω_K le groupe de Galois de $\overline{\mathbf{Q}}$ sur K et U(K) le groupe des idèles unités de K ; le groupe $U(\overline{\mathbf{Q}})$ est défini comme la limite inductive des groupes U(K) lorsque K parcourt l'ensemble des corps de nombres. Les extensions modérément ramifiées de K sont supposées galoisiennes sur K. Si Γ est un groupe fini on note $|\Gamma|$ son ordre et R_Γ le groupe additif de ses caractères virtuels. On entend par caractère irréductible (resp. de degré 1) un caractère absolument irréductible (resp. irréductible de degré 1). Le groupe $\Omega_{\mathbf{Q}}$ opère naturellement sur les groupes R_Γ, $O^*_{\overline{\mathbf{Q}}}$ et $U(\overline{\mathbf{Q}})$ et l'on définit le groupe $\operatorname{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, U(\overline{\mathbf{Q}}))$ et son sous-groupe $\operatorname{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, O^*_{\overline{\mathbf{Q}}})$. Si $R_\Gamma^{(s)}$ désigne le sous-groupe de R_Γ des caractères symplectiques on note $\overset{+}{\operatorname{Hom}}_{\Omega_{\mathbf{Q}}}(R_\Gamma, U(\overline{\mathbf{Q}}))$ (resp. $\overset{+}{\operatorname{Hom}}_{\Omega_{\mathbf{Q}}}(R_\Gamma, O^*_{\overline{\mathbf{Q}}})$) le sous-groupe de $\operatorname{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, U(\overline{\mathbf{Q}}))$ (resp. $\operatorname{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, O^*_{\overline{\mathbf{Q}}})$) des éléments f qui vérifient :

$f(\chi)_v > 0$ pour tout élément χ de $R_\Gamma^{(s)}$ et toute place infinie v complexe ou réelle de $\overline{\mathbf{Q}}$. On définit un homomorphisme noté det. du groupe des idèles unités $U(\mathbf{Z}[\Gamma])$ de $\mathbf{Z}[\Gamma]$ dans $\overset{+}{\operatorname{Hom}}_{\Omega_{\mathbf{Q}}}(R_\Gamma, U(\overline{\mathbf{Q}}))$ en prolongeant par linéarité à R_Γ l'application qui à α associe $\det(\alpha)$ définie pour le caractère χ d'une représentation T par :

$\det_\chi(\alpha) = \det(T(\alpha))$ où $\det(T(\alpha))$ est le déterminant usuel. Fröhlich ([6]) a défini un isomorphisme du groupe $D(\mathbf{Z}[\Gamma])$ sur le groupe :

$$\overset{+}{\operatorname{Hom}}_{\Omega_{\mathbf{Q}}}(R_\Gamma, U(\overline{\mathbf{Q}})) / \overset{+}{\operatorname{Hom}}_{\Omega_{\mathbf{Q}}}(R_\Gamma, O^*_{\overline{\mathbf{Q}}}) . \det(U(\mathbf{Z}[\Gamma])) .$$

A tout nombre premier l qui divise $|\Gamma|$ on associe le sous-groupe $\operatorname{Ker} d_{l,\Gamma}$ de R_Γ des caractères χ de Γ tels que :

$\chi(\gamma) = 0$ pour tout élément γ l-régulier de Γ et le radical $\mathcal{L}$ de l dans $O_{\overline{\mathbf{Q}}}$. L'homomorphisme de restriction de R_Γ à $\operatorname{Ker} d_{l,\Gamma}$ et la surjection naturelle de $U(\overline{\mathbf{Q}})$ sur le groupe $(O_{\overline{\mathbf{Q}}}/\mathcal{L})^*$, noté V_l, permettent de définir un homomorphisme surjectif $r_{l,\Gamma}$ de $\operatorname{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, U(\overline{\mathbf{Q}}))$ sur $\operatorname{Hom}_{\Omega_{\mathbf{Q}}}(\operatorname{Ker} d_{l,\Gamma}, V_l)$; on sait ([6]) que l'image par $r_{l,\Gamma}$ de $\det(U(\mathbf{Z}[\Gamma]))$ est réduite à l'élément neutre. Si S désigne l'ensemble des nombres premiers qui divisent $|\Gamma|$ l'homomorphisme $(\prod_{l \in S} r_{l,\Gamma})$, qu'on note r_Γ, définit par passage au quotient un homomorphisme $h(\Gamma)$ de $D(\mathbf{Z}[\Gamma])$ sur le groupe $E(\Gamma)$ défini par l'égalité :

$$\mathrm{E}(\Gamma) = r_\Gamma(\overset{+}{\underset{\Omega_{\mathbf{Q}}}{\mathrm{Hom}}}(\mathrm{R}_\Gamma, \mathrm{U}(\overline{\mathbf{Q}}))) / r_\Gamma(\overset{+}{\underset{\Omega_{\mathbf{Q}}}{\mathrm{Hom}}}(\mathrm{R}_\Gamma, \mathrm{O}^*_{\overline{\mathbf{Q}}})).$$

On s'intéressera dans cet article au sous-groupe $\mathrm{Ker}\, h(\Gamma)$ (resp. $\mathrm{Ker}\, h_0(\Gamma)$ égal $\mathrm{Ker}\, h(\Gamma) \cap \mathrm{D}_0(\mathbf{Z}[\Gamma])$) de $\mathrm{D}(\mathbf{Z}[\Gamma])$ (resp. $\mathrm{D}_0(\mathbf{Z}[\Gamma])$).

Soit T l'homomorphisme de R_Γ dans $\mathrm{R}_\Gamma^{(s)}$ défini par $\mathrm{T}(\chi) = \chi + \overline{\chi}$ où $\overline{\chi}$ désigne le caractère complexe conjugué de χ. Le groupe $\Omega_{\mathbf{Q}}$ opère (resp. opère trivialement) sur le groupe quotient $\mathrm{R}_\Gamma^{(s)}/\mathrm{T}(\mathrm{R}_\Gamma)$ (resp. réduit à deux éléments $\{\pm 1\}$). Tout élément f de $\underset{\Omega_{\mathbf{Q}}}{\mathrm{Hom}}(\mathrm{R}_\Gamma^{(s)}/\mathrm{T}(\mathrm{R}_\Gamma), \pm 1)$ se relève en un élément, encore noté f, de $\underset{\Omega_{\mathbf{Q}}}{\mathrm{Hom}}(\mathrm{R}_\Gamma, \pm 1)$ (on pose $f(\chi) = 1$ pour tout caractère irréductible non symplectique de Γ). On associe à -1 l'élément (x_v) de $\mathrm{U}(\overline{\mathbf{Q}})$ défini par : $x_v = -1$ (resp. 1) pour toute place v finie (resp. infinie) et ainsi à tout élément f de $\underset{\Omega_{\mathbf{Q}}}{\mathrm{Hom}}(\mathrm{R}_\Gamma, \pm 1)$ on associe l'élément f^+ de $\overset{+}{\underset{\Omega_{\mathbf{Q}}}{\mathrm{Hom}}}(\mathrm{R}_\Gamma, \mathrm{U}(\overline{\mathbf{Q}}))$ défini pour tout caractère irréductible χ de Γ par : $f^+(\chi) = (x_v)$ (resp. 1) si $f(\chi)$ est égal à -1 (resp. 1) ; on note $t^+(f)$ l'élément de $\mathrm{D}(\mathbf{Z}[\Gamma])$ défini par f^+ et $k(\Gamma)$ l'homomorphisme de $\underset{\Omega_{\mathbf{Q}}}{\mathrm{Hom}}(\mathrm{R}_\Gamma^{(s)}/\mathrm{T}(\mathrm{R}_\Gamma), \pm 1)$ dans $\mathrm{E}(\Gamma)$ égal à $h(\Gamma) \circ t^+$.

Si Γ est le groupe de Galois d'une extension modérément ramifiée N d'un corps de nombres K on note $\mathrm{U}_{\mathrm{N/K}}$ l'élément défini par O_N dans $\mathrm{D}(\mathbf{Z}[\Gamma])$ et h et k les homomorphismes $h(\Gamma)$ et $k(\Gamma)$. L'application de $\mathrm{R}_\Gamma^{(s)}$ dans ± 1 définie par $(\chi \longrightarrow \mathrm{W}(\chi, \mathrm{N/K}))$, où $\mathrm{W}(\chi, \mathrm{N/K})$ désigne la constante de l'équation fonctionnelle de la série L-d'Artin associée au caractère symplectique χ, définit par passage au quotient un élément $\mathrm{W}_{\mathrm{N/K}}$ de $\underset{\Omega_{\mathbf{Q}}}{\mathrm{Hom}}(\mathrm{R}_\Gamma^{(s)}/\mathrm{T}(\mathrm{R}_\Gamma), \pm 1)$. On a montré ([3]) le théorème suivant :

THEOREME. – *On a l'égalité* : $h(\mathrm{U}_{\mathrm{N/K}}) = k(\mathrm{W}_{\mathrm{N/K}})$.

D'où le corollaire :

COROLLAIRE. – *L'élément* $\mathrm{U}_{\mathrm{N/K}}\, t^+(\mathrm{W}_{\mathrm{N/K}})^{-1}$ *appartient au sous-groupe* $\mathrm{Ker}\, h(\Gamma)$ (*resp.* $\mathrm{Ker}\, h_0(\Gamma)$ *lorsque* $\mathrm{K} = \mathbf{Q}$) *de* $\mathrm{D}(\mathbf{Z}[\Gamma])$ (*resp.* $\mathrm{D}_0(\mathbf{Z}[\Gamma])$).

Pour tout nombre entier d on note $\mathbf{Q}^{(d)}$ (resp. $\mathbf{Z}^{(d)}$) la d-ème extension cyclotomique (resp. son anneau d'entiers). On désigne par $\mathfrak{M}$ un ordre maximal de $\mathbf{Z}$ dans $\mathbf{Q}[\Gamma]$ contenant $\mathbf{Z}[\Gamma]$ et, pour tout nombre premier l, on pose $\mathfrak{M}_l = \mathfrak{M} \underset{\mathbf{Z}}{\otimes} \mathbf{Z}_l$ où $\mathbf{Z}_l$ désigne l'anneau des entiers du corps l-adique $\mathbf{Q}_l$. On sait que $\mathfrak{M}_l$ est un ordre maximal de $\mathbf{Z}_l$ dans $\mathbf{Q}_l[\Gamma]$ contenant $\mathbf{Z}_l[\Gamma]$.

3. Enoncé des résultats.

Ce paragraphe contient les principaux résultats que nous avons obtenus dans l'étude de l'exposant du sous-groupe $\mathrm{Ker}\, h(\Gamma)$ (resp. $\mathrm{Ker}\, h_0(\Gamma)$) de $D(\mathbf{Z}[\Gamma])$ (resp. $D_0(\mathbf{Z}[\Gamma])$) et leurs applications arithmétiques. On rappelle que pour toute extension modérément ramifiée N du corps de nombres K on note $U_{N/K}$ l'élément de $D(\mathbf{Z}[G(N/K)])$ défini par l'anneau des entiers de N et $t^+(W_{N/K})$ l'élément d'ordre 1 ou 2 de $D(\mathbf{Z}[G(N/K)])$ défini à partir des constantes d'équations fonctionnelles. On note $|\Gamma|$ l'ordre du groupe fini Γ et (,) désigne le P.G.C.D.

THEOREME 3.1. – *Si Γ est un groupe fini, alors l'exposant du groupe $\mathrm{Ker}\, h(\Gamma)$ est un diviseur de l'entier $|\Gamma|/(2, |\Gamma|)$.*

COROLLAIRE 3.1. – *Si N est une extension galoisienne modérément ramifiée d'un corps de nombres K alors l'ordre de $U_{N/K}$ divise le degré de N sur K. En outre l'ordre de $U_{N/K}$ est impair lorsque le degré de N sur K n'est pas divisible par 4.*

En effet on a défini $V_{N/K}$ tel qu'on ait dans le groupe $D(\mathbf{Z}[G(N/K)])$ l'égalité $U_{N/K} = t^+(W_{N/K})\, V_{N/K}$ et l'on sait par le théorème 3.1. que l'ordre de $V_{N/K}$ divise $[N:K]/(2,[N:K])$. Si $[N:K]$ n'est pas divisible par 4 l'ordre de $V_{N/K}$ est impair, en outre le groupe G(N/K) n'a pas de caractère irréductible et symplectique ce qui implique que $t^+(W_{N/K})$ est égal à l'élément neutre.

DEFINITION. – *Soit Γ un groupe métabélien, c'est-à-dire une extension d'un groupe abélien F par un groupe abélien H. On dit que Γ vérifie la condition* (C) *si l'on a les deux conditions suivantes :*

(i) *Les entiers $|F|$ et $|H|$ sont premiers entre eux.*

(ii) *Tout sous-groupe U de H tel que H/U soit cyclique est distingué dans Γ.*

Remarques

1) La condition (i) implique que Γ est égal à un produit semi-direct d'un sous-groupe H abélien et distingué par un sous-groupe F abélien. Si le sous-groupe H est cyclique la condition (ii) est vérifiée.

2) On montre dans le paragraphe 5 que tout caractère irréductible ψ d'un groupe Γ vérifiant la condition (C) est induit par un caractère de degré 1 d'un sous-groupe Γ_ψ de Γ déterminé de manière unique. On note $e_0(\Gamma)$ le P.P.C.M. des entiers $|\Gamma_\psi|$ lorsque ψ parcourt les caractères irréductibles de Γ de degré strictement supérieur à 1 et $e_0'(\Gamma)$ (resp. $e'(\Gamma)$) le produit des nombres premiers qui divisent $e_0(\Gamma)$ (resp. $|\Gamma|$).

THEOREME 3.2. – *Si* Γ *est un groupe métabélien qui vérifie la condition* (C) *alors* :

(i) *L'exposant du groupe* $\mathrm{Ker}\, h(\Gamma)$ *divise l'entier* $|\Gamma|/e'(\Gamma)$

(ii) *Si* H *est cyclique, l'exposant du groupe* $\mathrm{Ker}\, h_0(\Gamma)$ *divise l'entier* $e_0(\Gamma)/e_0'(\Gamma)$.

Dans l'énoncé des corollaires qui suivent nous notons Γ le groupe $G(N/K)$.

COROLLAIRE 3.2. – *Si* N *est une extension galoisienne modérément ramifiée d'un corps de nombres* K *dont le groupe de Galois est métabélien et vérifie la condition* (C), *alors on a l'égalité suivante dans* $D(\mathbf{Z}[\Gamma])$:

$$U_{N/K} = t^+(W_{N/K}) \,.\, V_{N/K} \,,$$

où $V_{N/K}$ *est un élément de* $D(\mathbf{Z}[\Gamma])$ *dont l'ordre divise* $|\Gamma|/e'(\Gamma)$.

Ce corollaire est une conséquence immédiate du théorème 3.2 (i) et du théorème 6.2 ([3]).

COROLLAIRE 3.3. – *L'anneau des entiers d'une extension* N *galoisienne modérément ramifiée d'un corps de nombres* K *dont le degré sur* K *est sans facteur carré est un* $\mathbf{Z}[\Gamma]$*-module libre.*

On sait (théorème de Zassenhaus) que tout groupe fini dont les sous-groupes de Sylow sont cycliques est métacyclique et vérifie la condition (C). Le corollaire 3.2. implique qu'on a l'égalité : $U_{N/K} = t^+(W_{N/K})$. En outre, puisque l'ordre de Γ n'est pas divisible par 4, on sait que Γ n'a pas de caractère symplectique irréductible, d'où l'égalité $U_{N/K} = 1$, et que l'algèbre $\mathbf{Q}[\Gamma]$ a la propriété de simplification, ce qui achève la démonstration de ce corollaire.

Remarque. – Si K est le corps $\mathbf{Q}$ des rationnels, le corollaire 3.3. signifie que N possède une base normale d'entiers.

COROLLAIRE 3.4. – *Sous les hypothèses du théorème 3.2. (ii), l'ordre de l'élément* $V_{N/K}$ *divise* $e_0(\Gamma)/e'_0(\Gamma)$ *dans les cas particuliers suivants* :

(i) K *est le corps* $\mathbf{Q}$ *des rationnels.*

(ii) *Le groupe* $\Gamma^{(ab)}$ *est cyclique d'ordre 4, 6, 8, 9, 10, 14, ou un nombre premier, ou non cyclique d'ordre 4.*

Il suffit de montrer que $V_{N/K}$ appartient au groupe $\operatorname{Ker} h_0(\Gamma)$ et d'appliquer le théorème 3.2. (ii). Or si $K = \mathbf{Q}$ c'est une conséquence du théorème de Hilbert et Speiser et si $\Gamma^{(ab)}$ est un des groupes définis en (ii) alors on sait ([2] et [23]) que $D(\mathbf{Z}[\Gamma^{(ab)}])$ est réduit à l'élément neutre.

Remarque. – Sous les hypothèses du corollaire 3.4. la conjecture de Fröhlich est démontrée lorsque $e_0(\Gamma)$ est sans facteur carré. On généralise ainsi un théorème de base normale donné par Fröhlich ([8]).

Notons $G_{l^n q}$ le groupe métacyclique engendré par les éléments ω et σ qui vérifient les égalités : $\omega^{l^n} = 1 = \sigma^q$ et $\sigma\omega\sigma^{-1} = \omega^r$ où r est une racine primitive q-ème de 1 modulo l, l un nombre premier régulier et impair et q un diviseur de $(l-1)$.

COROLLAIRE 3.5. – *Si* N *est une extension galoisienne modérément ramifiée d'un corps de nombres* K *dont le groupe de Galois est isomorphe au groupe* $G_{l^n q}$, *on a l'égalité* : $U_{N/K} = t^+(W_{N/K})$ *dans l'un des deux cas particuliers suivants* :

(i) $K = \mathbf{Q}$

(ii) q *est un nombre premier ou est égal à 4, 6, 8, 9, 10, 14.*

On sait, par le corollaire 3.4, que sous l'hypothèse (i) ou (ii) l'ordre de $V_{N/K}$ est égal à une puissance de l. Or Keating a montré ([20]) que lorsque l est un nombre premier régulier, le groupe $D_0(G_{l^n q})$ est un l'-groupe ; ceci démontre que $V_{N/K}$ est égal à 1.

On note x_2 la 2-composante d'un élément x d'un groupe abélien.

COROLLAIRE 3.6. – *Si* N *est une extension galoisienne modérément ramifiée d'un corps de nombres* K *dont le groupe de Galois est isomorphe au groupe quaternionien* H_{4m} *où* m *est un nombre entier impair, alors on a les égalités* :

(i) $U_{N/K,2} = t^+(W_{N/K})$

(ii) *Si* m *est sans facteur carré* : $U_{N/K} = t^+(W_{N/K})$.

Nous sommes en effet dans les hypothèses (ii) du corollaire 3.4. et l'entier $e_0(H_{4m})/e_0'(H_{4m})$ est impair (resp. égal à 1) si m est impair (resp. impair et sans facteur carré).

4. Démonstration du théorème 3.1.

On utilise les notations que l'on a rappelées au paragraphe 2. On a identifié le groupe noyau $D(\mathbf{Z}[\Gamma])$ et le groupe quotient :

$$\operatorname{Hom}^+_{\Omega_{\mathbf{Q}}}(R_\Gamma, U(\overline{\mathbf{Q}}))/\operatorname{Hom}^+_{\Omega_{\mathbf{Q}}}(R_\Gamma, O^*_{\overline{\mathbf{Q}}}) . \det(U(\mathbf{Z}[\Gamma])) .$$

On a alors la suite exacte de groupes et d'homomorphismes :

$$1 \longrightarrow \operatorname{Hom}^+_{\Omega_{\mathbf{Q}}}(R_\Gamma, O^*_{\overline{\mathbf{Q}}}) . \operatorname{Ker} r_\Gamma/\operatorname{Hom}^+_{\Omega_{\mathbf{Q}}}(R_\Gamma, O^*_{\overline{\mathbf{Q}}}) . \det(U(\mathbf{Z}[\Gamma])) \longrightarrow D(\mathbf{Z}[\Gamma]) \xrightarrow{h(\Gamma)} E(\Gamma) \longrightarrow 1 .$$

Le groupe $\operatorname{Ker} h(\Gamma)$ est donc isomorphe au groupe quotient :

$$\operatorname{Ker} r_\Gamma/\det(U(\mathbf{Z}[\Gamma]))\,(\operatorname{Hom}^+_{\Omega_{\mathbf{Q}}}(R_\Gamma, O^*_{\overline{\mathbf{Q}}}) \cap \operatorname{Ker} r_\Gamma) . \tag{1}$$

Tout élément de $\operatorname{Ker} h(\Gamma)$ possède donc un représentant dans $\operatorname{Ker} r_\Gamma$, c'est-à-dire un représentant $\det(\alpha)$ dans $\operatorname{Hom}^+_{\Omega_{\mathbf{Q}}}(R_\Gamma, U(\overline{\mathbf{Q}}))$ où α désigne un élément (α_l) de $U(\mathfrak{M})$ tel que, pour tout nombre premier l, α_l est un élément de $\mathfrak{M}_l^*$ qui vérifie les congruences : $\det_\theta(\alpha_l) \equiv 1 \pmod{\mathfrak{L}}$ pour tout θ de $\operatorname{Ker} d_{l,\Gamma}$. Nous nous proposons de trouver pour tout élément de $\operatorname{Ker} h(\Gamma)$ un représentant dans $\operatorname{Ker} r_\Gamma$ plus facile à utiliser.

PROPOSITION 4.1. – *Soit* α_l *un élément de* $\mathfrak{M}_l^*$ *qui vérifie les congruences* : $\det_\theta(\alpha_l) \equiv 1$ (*mod.* $\mathfrak{L}$) *pour tout* θ *de* $\operatorname{Ker} d_{l,\Gamma}$. *Alors, il existe un élément* β_l *de* $\mathfrak{M}_l^*$ *qui satisfait les propriétés (i) et (ii) suivantes* :

(i) $\det_\theta(\beta_l) \equiv 1$ (*mod.* $\mathfrak{L}$) *pour tout* θ de R_Γ

(ii) $\det(\beta_l) \equiv \det(\alpha_l)$ *mod.* $\det.(\overline{\mathbf{Z}}_l[\Gamma]^*)$.

COROLLAIRE 4.1. – *Tout élément de* $\operatorname{Ker} h(\Gamma)$ *possède un représentant dans* $\operatorname{Ker} r_\Gamma$ *de la forme* $\det(\alpha)$ *où* $\alpha = (\alpha_l)$ *est un élément de* $U(\mathfrak{M})$ *qui vérifie pour tout* l *les congruences* : $\det_\theta(\alpha_l) \equiv 1$ (*mod.* $\mathfrak{L}$) *pour tout caractère* θ *de* Γ.

La démonstration de ce corollaire est immédiate. En effet, soient x un élément de $\mathrm{Ker}\, h(\Gamma)$ et $\alpha = (\alpha_l)$ un élément de $U(\mathfrak{M})$ tel que $\det \alpha$ soit un représentant de x dans $\mathrm{Ker}\, r_\Gamma$. Pour tout nombre premier l la proposition 4.1. permet d'associer à α_l un élément β_l de $\mathfrak{M}_l^*$ qui vérifie les conditions (i) et (ii) de cette proposition ; notons β l'élément (β_l) de $U(\mathfrak{M})$. La congruence : $\det \beta \equiv \det \alpha$ mod. $\det(U(\mathbf{Z}[\Gamma]))$ implique que $\det \beta$ est un représentant de x ; en outre il satisfait les congruences : $\det_\theta(\beta_l) \equiv 1$ (mod. $\mathfrak{L}$) pour tout caractère θ de Γ et tout nombre premier l.

Nous démontrons maintenant la proposition 4.1. Si l ne divise pas $|\Gamma|$ alors $\mathbf{Z}_l[\Gamma]$ est un ordre maximal de $\mathbf{Z}_l$ dans $\mathbf{Q}_l[\Gamma]$, les ordres $\mathbf{Z}_l[\Gamma]$ et $\mathfrak{M}_l$ sont égaux et la proposition est immédiate. Nous supposons maintenant que l divise $|\Gamma|$.

On désigne par K un corps local, extension finie de $\mathbf{Q}_l$, sur lequel les caractères absolument irréductibles de Γ sont réalisables et on sait que ces caractères peuvent être associés à des représentations de Γ à coefficients dans l'anneau d'entiers O_K de K ; on note P l'idéal maximal de K et k son corps résiduel. Pour tout élément α_l de $\mathfrak{M}_l^*$ et pour tout caractère θ d'une représentation T de Γ on considère l'élément $\det T(\alpha_l)$ de O_K^* qu'on note $\det_\theta(\alpha_l)$ et on étend par linéarité à R_Γ l'application $\theta \longrightarrow \det_\theta(\alpha_l)$. Avec ces notations, la proposition 4.1. s'énonce de la manière suivante :

PROPOSITION 4.2. – *Soit* α_l *un élément de* $\mathfrak{M}_l^*$ *qui vérifie les congruences* : $\det_\theta(\alpha_l) \equiv 1$ (*mod.* P) *pour tout caractère* θ *de* $\mathrm{Ker}\, d_{l,\Gamma}$, *alors il existe un élément* β_l *de* $\mathfrak{M}_l^*$ *qui satisfait les propriétés (i) et (ii)*

(i) $\det_\theta(\beta_l) \equiv 1$ (*mod.* P) *pour tout caractère* θ *de* Γ ;

(ii) $\det(\beta_l) \equiv \det(\alpha_l)$ *mod.* $\det(\mathbf{Z}_l[\Gamma]^*)$.

Notons d l'homomorphisme de décomposition $d_{l,\Gamma}$. C'est une application surjective de $R_K(\Gamma)$ sur $R_k(\Gamma)$. Selon les cas on considère le groupe $R_K(\Gamma)$ (resp. $R_k(\Gamma)$) comme le groupe abélien libre engendré par les classes de $K[\Gamma]$ –(resp. $k[\Gamma]$–) modules simples ou comme le groupe des K-caractères (resp. k-caractères modulaires) virtuels de Γ. L'application d est alors définie par : $d(\theta)(x) = \theta(x)$ pour tout $\theta \in R_K(\Gamma)$ et tout élément x de Γ l-régulier.

Soit $\{\psi_i\}$, $1 \leqslant i \leqslant n$, une famille de K-caractères virtuels de Γ dont les images par d engendrent $R_k(\Gamma)$. On a le lemme suivant :

LEMME 4.1. – *Soit un élément α_l de $\mathfrak{M}_l^*$ vérifiant les congruences :* $\det_\theta(\alpha_l) \equiv 1$ *(mod.* P) *pour tout caractère θ de* $\operatorname{Ker} d$. *S'il existe a_l de $\mathbf{Z}_l[\Gamma]^*$ tel qu'on ait :* $\det_{\psi_i}(\alpha_l) \equiv \det_{\psi_i}(a_l)$ *(mod.* P), $1 \leqslant i \leqslant n$, *alors il existe un élément β_l de $\mathfrak{M}_l^*$ qui vérifie les propriétés (i) et (ii) de la proposition 4.2.*

Notons β_l l'élément $\alpha_l a_l^{-1}$ de $\mathfrak{M}_l^*$ et montrons qu'il vérifie les propriétés (i) et (ii). Par définition même de β_l la propriété (ii) est vérifiée. Soit θ un caractère virtuel de Γ ; il existe des entiers $\{m_i\}$, $1 \leqslant i \leqslant n$, et un caractère u de $\operatorname{Ker} d$ tels qu'on ait l'égalité :

$$\theta = u + \sum_{i=1}^{n} m_i \psi_i .$$

On en déduit :

$$\det_\theta(\beta_l) = \det_u(\beta_l) \prod_{i=1}^{n} \det_{\psi_i}(\beta_l)^{m_i} .$$

Par hypothèse on a : $\det_{\psi_i}(\beta_l) \equiv 1$ (mod. P), $1 \leqslant i \leqslant n$, et donc on a :

$$\prod_{i=1}^{n} \det_{\psi_i}(\beta_l)^{m_i} \equiv 1 \pmod{\mathrm{P}}.$$

En outre on a : $\det_u(\alpha_l) \equiv 1$ (mod. P) puisque u appartient à $\operatorname{Ker} d$. Or pour tout x de $\mathbf{Z}_l[\Gamma]^*$ et tout caractère u de $\operatorname{Ker} d$ on a : $\det_u(x) \equiv 1$ (mod. P). On en déduit la congruence : $\det_u(\beta_l) \equiv 1$ (mod. P), ce qui montre que $\det(\beta_l)$ vérifie la propriété (i).

Le lemme 4.1. ramène donc la démonstration de la proposition 4.2. à celle du lemme :

LEMME 4.2. – *Soit* $\{\psi_i\}$, $1 \leqslant i \leqslant n$, *une famille de K-caractères de Γ qui relèvent les k-caractères modulaires irréductibles de Γ. Alors pour tout élément α_l de $\mathfrak{M}_l^*$ il existe un élément a_l de $\mathbf{Z}_l[\Gamma]^*$ tel qu'on ait les congruences :* $\det_{\psi_i}(\alpha_l) \equiv \det_{\psi_i}(a_l)$ *(mod.* P), $1 \leqslant i \leqslant n$.

On suppose pour simplifier la démonstration que Γ vérifie les hypothèses du théorème de Fong-Swan et que pour tout i, $1 \leqslant i \leqslant n$, ψ_i est le caractère d'une représentation T_i de Γ dans $GL_{n_i}(O_K)$. La surjection canonique $(O_K \longrightarrow k)$ induit un homomorphisme surjectif de $M_{n_i}(O_K)$ sur $M_{n_i}(k)$ qu'on note π'. Alors $\pi' \circ T_i$ définit une k-représentation irréductible de Γ que l'on note $\overline{T}_i$, de caractère $\overline{\psi}_i$, qui définit un homomorphisme, encore noté $\overline{T}_i$, de $\mathbf{F}_l[\Gamma]$ dans $M_{n_i}(k)$. Le diagramme suivant est commutatif :

$$\begin{tikzcd} \mathbf{Z}_l[\Gamma] \arrow[r, "T_i"] \arrow[d, "\pi"'] & M_{n_i}(O_K) \arrow[d, "\pi'"] \\ \mathbf{F}_l[\Gamma] \arrow[r, "\overline{T}_i"] & M_{n_i}(k) \end{tikzcd}$$

où π désigne l'homomorphisme d'algèbre induit par la surjection canonique $(\mathbf{Z}_l \longrightarrow \mathbf{F}_l)$. On sait ([22], théorème 6.10.) que π induit par passage au quotient un homomorphisme surjectif de $\mathbf{Z}_l[\Gamma]/\mathrm{rad}(\mathbf{Z}_l[\Gamma])$ sur $\mathbf{F}_l[\Gamma]/\mathrm{rad}(\mathbf{F}_l[\Gamma])$ et on en déduit que la restriction de π au groupe des unités de $\mathbf{Z}_l[\Gamma]^*$ est un homomorphisme surjectif de $\mathbf{Z}_l[\Gamma]^*$ sur $\mathbf{F}_l[\Gamma]^*$. Pour démontrer le lemme 4.2. il suffit donc de démontrer, pour tout élément α_l de $\mathfrak{M}_l^*$, l'existence d'un élément b_l de $\mathbf{F}_l[\Gamma]^*$ tel qu'on ait dans k les égalités :

$$\overline{\det_{\psi_i}(\alpha_l)} = \det_{\overline{\psi}_i}(b_l), \quad 1 \leqslant i \leqslant n \tag{1}$$

où on note $\overline{x}$ la classe dans k de l'élément x de O_K.

Le groupe $G(k/\mathbf{F}_l)$ opère sur l'ensemble des k-caractères irréductibles de Γ et désignons par $\{\overline{\psi}_j\}$, $j \in J$, une famille de représentants des orbites. Montrons qu'il suffit de montrer (1) pour $j \in J$. Soit b_l un élément de $\mathbf{F}_l[\Gamma]^*$ tel qu'on ait (1), pour $j \in J$. Si $\overline{\psi}_i$ est un caractère irréductible de Γ il existe $j \in J$ et un élément $\overline{\sigma}$ de $G(k/\mathbf{F}_l)$, qui se relève en un élément σ de $G(K/\mathbf{Q}_l)$ tel qu'on ait l'égalité $\overline{\psi}_i = \overline{\psi}_j^{\overline{\sigma}}$ et on suppose qu'on a choisi l'ensemble $\{\psi_i\}$ de façon que $\psi_i = \psi_j^{\sigma}$. On a alors les égalités :

$$\overline{\det_{\psi_i}(\alpha_l)} = \overline{\det_{\psi_j}(\alpha_l)}^{\overline{\sigma}} = \det_{\overline{\psi}_j}(b_l)^{\overline{\sigma}} = \det_{\overline{\psi}_i}(b_l)$$

et donc l'égalité (1) est vérifiée pour tout i, $1 \leqslant i \leqslant n$. Il nous suffit donc de démontrer l'existence d'une unité b_l de $\mathbf{F}_l[\Gamma]$ telle qu'on ait l'égalité (1) pour tout $i \in J$. La $\mathbf{F}_l$-algèbre : $\mathbf{F}_l[\Gamma]/\mathrm{rad}(\mathbf{F}_l[\Gamma])$ est semi-simple et se décompose en une somme directe d'algèbres simples $\{A_i\}$, $i \in J$. Pour tout $i \in J$ on note k_i le centre de l'algèbre A_i et N_i la norme réduite de A_i dans k_i. On a la suite exacte :

$$1 \longrightarrow \mathrm{rad}(\mathbf{F}_l[\Gamma]) \longrightarrow \mathbf{F}_l[\Gamma] \longrightarrow \prod_{i\in J}^{n} A_i \longrightarrow 1 .$$

On en déduit la nouvelle suite :

$$1 \longrightarrow \mathrm{rad}(\mathbf{F}_l[\Gamma]) \underset{\mathbf{F}_l}{\otimes} k \longrightarrow k[\Gamma] \longrightarrow \prod_{i\in J} A_i \underset{\mathbf{F}_l}{\otimes} k \longrightarrow 1 .$$

On a l'égalité : $\mathrm{rad}\, k[\Gamma] = \mathrm{rad}(\mathbf{F}_l[\Gamma]) \underset{\mathbf{F}_l}{\otimes} k$ ([34]) ; on sait en outre, puisque k est une extension séparable de $\mathbf{F}_l$, que pour $i \in J$ l'algèbre $A_i \underset{\mathbf{F}_l}{\otimes} k$ est une k-algèbre semi-simple. Les facteurs simples de $k[\Gamma]/\mathrm{rad}(k[\Gamma])$ sont donc obtenus en décomposant en somme d'algèbres simples les facteurs simples de $\mathbf{F}_l[\Gamma]/\mathrm{rad}(\mathbf{F}_l[\Gamma])$ étendus à k. Si α_l appartient à $\mathfrak{M}_l^*$ alors $\overline{(\det_{\psi_i}(\alpha_l))}_{i\in J}$ définit un élément de $\prod_{i\in J} \mathbf{F}_l(\psi_i)^*$ et donc un élément $(\alpha_i)_{i\in J}$ de $\prod_{i\in J} k_i^*$. L'homomorphisme de groupe $N_i : A_i^* \longrightarrow k_i^*$ est surjectif et il existe donc un élément $a = (a_i)_{i\in J}$ tel que $(\alpha_i)_{i\in J} = (N_i(a_i))_{i\in J}$. Or toute unité de $\prod_{i\in J} A_i^*$ se relève en une unité de $\mathbf{F}_l[\Gamma]/\mathrm{rad}(\mathbf{F}_l[\Gamma])$ et donc en une unité de $\mathbf{F}_l[\Gamma]$. On a donc montré l'existence d'un élément b_l de $\mathbf{F}_l[\Gamma]^*$ tel que : $\overline{\det_{\psi_i}(\alpha_l)} = \det_{\overline{\psi}_i}(b_l)$ pour tout $i \in J$, ce qui achève la démonstration de la proposition.

Revenons à la démonstration du théorème 3.1.

L'isomorphisme (1) nous donne la suite exacte de groupes et d'homomorphismes suivante :

$$\begin{aligned} 1 \longrightarrow \overset{+}{\mathrm{Hom}}_{\Omega_{\mathbf{Q}}}(R_\Gamma, O_{\overline{\mathbf{Q}}}^*) \cap \mathrm{Ker}\, r_\Gamma / \overset{+}{\mathrm{Hom}}_{\Omega_{\mathbf{Q}}}(R_\Gamma, O_{\overline{\mathbf{Q}}}^*) \cap \det(U(\mathbf{Z}[\Gamma])) \\ \longrightarrow \prod_{l\,|\,|\Gamma|} (\mathrm{Ker}\, r'_{l,\Gamma}/\det(\mathbf{Z}_l[\Gamma]^*)) \longrightarrow \mathrm{Ker}\, h(\Gamma) \longrightarrow 1 \end{aligned}$$

où $r'_{l,\Gamma}$ désigne le composé par $r_{l,\Gamma}$ de l'injection canonique de $\det(\mathfrak{M}_l^*)$ dans $\det U(\mathfrak{M})$. On note $\det^{(1)}(\mathfrak{M}_l^*)$ (resp. $\det^{(1)}(\mathbf{Z}_l[\Gamma]^*)$) le sous-groupe de $\det(\mathfrak{M}_l^*)$ (resp. $\det(\mathbf{Z}_l[\Gamma]^*)$) des éléments $\det(\alpha_l)$ où α_l appartient à $\mathfrak{M}_l^*$ (resp. $\mathbf{Z}_l[\Gamma]^*$) et vérifie : $\det_\theta(\alpha_l) \equiv 1$ (mod. $\mathcal{L}$) pour tout caractère θ de Γ.

La proposition 4.1. permet d'identifier les groupes $\mathrm{Ker}\, r'_{l,\Gamma}$ et $\det(\mathbf{Z}_l[\Gamma]^*) . \det^{(1)}(\mathfrak{M}_l^*)$.

On en déduit l'isomorphisme de groupe suivant :

$$\mathrm{Ker}\, r'_{l,\Gamma}/\det(\mathbf{Z}_l[\Gamma]^*) \simeq \det^{(1)}(\mathfrak{M}_l^*)/\det^{(1)}(\mathbf{Z}_l[\Gamma]^*) .$$

Pour achever la démonstration du théorème 3.1. il suffit de démontrer la proposition suivante où $|\Gamma|_l$ désigne l'ordre d'un l-sous-groupe de Sylow de Γ.

PROPOSITION 4.3. – *L'exposant du groupe* $\det^{(1)}(\mathfrak{M}_l^*)/\det^{(1)}(\mathbf{Z}_l[\Gamma]^*)$ *divise* $|\Gamma|_l$. *En outre lorsque* l *est égal à* 2 *et divise* $|\Gamma|$, *alors il divise* $|\Gamma|_2/2$.

Nous adoptons dans la démonstration de cette proposition les notations suivantes : on désigne par $\{\theta_i\}$, $1 \leqslant i \leqslant m$, une famille de représentants des orbites de l'ensemble des caractères irréductibles de Γ sur lequel opère le groupe $G(\overline{\mathbf{Q}}_l/\mathbf{Q}_l)$. A tout entier i, $1 \leqslant i \leqslant m$, on associe un facteur simple A_i de $\mathbf{Q}_l[\Gamma]$. C'est une algèbre de matrice $M_{n_i}(D_i)$ sur un corps gauche D_i de centre K_i et on note m_i^2 le degré de A_i sur K_i. On désigne par L_i une extension non ramifiée de K_i qui est un sous-corps commutatif maximal de D_i. On note O_{K_i} (resp. O_{L_i}) l'anneau des entiers de K_i (resp. L_i) et P_i (resp. $\mathfrak{P}_i$) l'idéal maximal de O_{K_i} (resp. O_{L_i}). Si P est l'idéal maximal d'un anneau de valuation discrète A de corps des fractions E on note π_E une uniformisante de E, v_P la valuation P-adique et U_E^1 le sous-groupe des unités x de E telles qu'on ait l'inégalité : $v_P(x-1) \geqslant 1$. L'ordre maximal $\mathfrak{M}_l$ se décompose en un produit direct $\prod_{i=1}^{m} \mathfrak{M}_i$ où $\mathfrak{M}_i$ est un ordre maximal de $\mathbf{Z}_l$ dans A_i qui contient O_{L_i}.

La norme réduite de A_i sur K_i est notée N_i ; en outre la restriction à L_i de la norme réduite définie sur D_i coïncide avec la norme usuelle de corps de L_i dans K_i que l'on note $N_{L_i|K_i}$. On sait qu'il existe pour tout i un isomorphisme g_i de K_i sur $\mathbf{Q}_l(\theta_i)$ tel que pour tout α de $\mathbf{Q}_l[\Gamma]$ on ait l'égalité :

$$g_i(N_i(\alpha_i)) = \det_{\theta_i}(\alpha)$$

où α_i désigne la composante de α sur A_i. Le conducteur central F de $\mathfrak{M}_l$ dans $\mathbf{Z}_l[\Gamma]$ se décompose en un produit direct : $F = \prod_{i=1}^{m} F_i$ où F_i est l'idéal entier de K_i défini par l'égalité ([19]) : $F_i = l^n/m_i\, d(K_i)$ où l^n est égal à l'entier $|\Gamma|_l$ et où $d(K_i)$ désigne la différente de K_i.

Soit α un élément de $\mathfrak{M}_l^*$ qui définit l'élément $\det(\alpha)$ de $\det^{(1)}(\mathfrak{M}_l^*)$. Pour tout i, g_i associe à $\det_{\theta_i}(\alpha)$ un élément $N_i(\alpha_i)$ de $U_{K_i}^1$. Puisque L_i est une extension non ramifiée de K_i, il existe ([24]) un élément a_i de $U_{L_i}^1$ tel qu'on ait l'égalité : $N_{L_i|K_i}(a_i) = N_i(\alpha_i)$.

LEMME 4.3. – *Pour tout entier* i, $1 \leqslant i \leqslant m$, *et tout élément* a_i *de* $U_{L_i}^1$ *on a les inégalités*

(i) *si* l *est différent de* 2 : $v_{\mathfrak{T}_i}(a_i^{l^n} - 1) \geqslant v_{\mathfrak{T}_i}(l^n/m_i\, d(\mathrm{K}_i))$

(ii) *si* l *est égal à* 2 : $v_{\mathfrak{T}_i}(a_i^{2^{n-1}} - 1) \geqslant v_{\mathfrak{T}_i}(2^n/m_i\, d(\mathrm{K}_i))$.

Nous démontrons (i) et nous indiquons comment démontrer (ii). Pour cela montrons l'inégalité :

$$v_{\mathfrak{T}_i}(a_i^{l^n} - 1) \geqslant v_{\mathfrak{T}_i}(l^n/d(\mathrm{K}_i)). \tag{1}$$

L'élément a_i se met sous la forme $a_i = 1 + \pi_{\mathrm{L}_i} u_i$ avec u_i appartenant à $\mathrm{O}_{\mathrm{L}_i}$. On utilise la formule du binôme et on montre que l'inégalité (1) est une conséquence de l'inégalité (2) que nous allons démontrer :

$$v_{\mathfrak{T}_i}\left[\binom{l^n}{k}\pi_{\mathrm{L}_i}^k\right] \geqslant v_{\mathfrak{T}_i}(l^n/d(\mathrm{K}_i)) \tag{2}$$

pour tout entier k avec $1 \leqslant k \leqslant l^n$.

Il nous suffit donc de montrer pour tout entier k, l'inégalité (3) suivante :

$$v_{\mathfrak{T}_i}((\pi_{\mathrm{K}_i}^k/k)\,.\,d(\mathrm{K}_i)) \geqslant 0\,. \tag{3}$$

L'isomorphisme g_i nous permet d'identifier les corps K_i et $\mathbf{Q}_l(\theta_i)$ et donc de considérer K_i comme une sous-extension de $\mathbf{Q}_l(\epsilon_u, \epsilon_{l^r})$ où ϵ_u (resp. ϵ_{l^r}) est une racine primitive u-ème (resp. l^r-ème) de l'unité où u est un entier non divisible par l. Notons E_i (resp. $\mathfrak{P}_i$) le corps $\mathrm{K}_i(\epsilon_u)$ (resp. son idéal maximal). Puisque $\mathbf{Q}_l(\epsilon_u)$ est une extension non ramifiée de $\mathbf{Q}_l$, E_i est une extension non ramifiée de K_i ; on en déduit, grâce à la formule de transitivité des différentes, l'égalité :

$$v_{\mathfrak{T}_i}((\pi_{\mathrm{K}_i}^k/k)\,.\,d(\mathrm{K}_i)) = v_{\mathfrak{P}_i}((\pi_{\mathrm{E}_i}^k/k)\,.\,d(\mathrm{E}_i))\,.$$

On remarque que E_i est une extension de $\mathbf{Q}_l(\epsilon_u)$ qui est une extension non ramifiée de $\mathbf{Q}_l$. En utilisant l'égalité précédente et la formule de transitivité des différentes, on remarque que l'inégalité (3) est équivalente à l'inégalité (4) :

$$v_{\mathfrak{P}_i}((\pi_{\mathrm{E}_i}^k/k)\,.\,d(\mathrm{E}_i \mid \mathbf{Q}_l(\epsilon_u))) \geqslant 0 \tag{4}$$

où $d(\mathrm{E} \mid \mathrm{K})$ désigne la différente de E sur K. Nous montrons l'inégalité (4) pour toute extension E, d'idéal maximal $\mathfrak{P}$, de $\mathbf{Q}_l(\epsilon_u)$ contenue dans $\mathbf{Q}_l(\epsilon_u, \epsilon_{l^r})$. Distinguons deux cas suivant la parité de l.

a) *l est différent de 2*

Le degré de E sur $\mathbf{Q}_l(\epsilon_u)$ est de la forme $l^t d$ où d est un entier qui divise $(l-1)$; E est une extension de $\mathbf{Q}_l(\epsilon_u)$ contenue dans $\mathbf{Q}_l(\epsilon_u, \epsilon_{l^{t+1}})$ et $\mathbf{Q}_l(\epsilon_u, \epsilon_{l^{t+1}})$ est modérément ramifiée sur E. Notons $\mathfrak{P}'$ l'idéal maximal de $\mathbf{Q}_l(\epsilon_u, \epsilon_{l^{t+1}})$. Pour démontrer (4) il suffit de montrer l'inégalité :

$$v_{\mathfrak{P}'}((\pi^k_{\mathbf{Q}_l(\epsilon_u, \epsilon_{l^{t+1}})}/k) \,.\, \overline{d(\mathrm{E}\,|\,\mathbf{Q}_l(\epsilon_u))}) \geqslant 0 \tag{5}$$

où $\overline{d(\mathrm{E}\,|\,\mathbf{Q}_l(\epsilon_u))}$ désigne l'idéal $d(\mathrm{E}\,|\,\mathbf{Q}_l(\epsilon_u)) \,.\, \mathrm{O}_{\mathbf{Q}_l(\epsilon_u, \epsilon_{l^{t+1}})}$. On a l'égalité :

$$v_{\mathfrak{P}'}(\overline{d(\mathrm{E}\,|\,\mathbf{Q}_l(\epsilon_u))}) = v_{\mathfrak{P}'}(d(\mathbf{Q}_l(\epsilon_u, \epsilon_{l^{t+1}}))) - v_{\mathfrak{P}'}(d(\mathbf{Q}_l(\epsilon_u, \epsilon_{l^{t+1}})\,|\,\mathrm{E})).$$

Or on a l'égalité :

$$v_{\mathfrak{P}'}(d(\mathbf{Q}_l(\epsilon_u, \epsilon_{l^{t+1}})/\mathrm{E})) = [\mathbf{Q}_l(\epsilon_u, \epsilon_{l^{t+1}}) : \mathrm{E}] - 1 .$$

On a donc l'inégalité :

$$v_{\mathfrak{P}'}(\overline{d(\mathrm{E}\,|\,\mathbf{Q}_l(\epsilon_u))}) \geqslant v_{\mathfrak{P}'}(d(\mathbf{Q}_l(\epsilon_u, \epsilon_{l^{t+1}}))/l)$$

et l'inégalité (5) est une conséquence immédiate d'un résultat de Ullom ([28], lemme 3.4).

b) *l est égal à 2*

Le degré de E sur $\mathbf{Q}_2(\epsilon_u)$ est de la forme 2^t et donc E est de la forme $\mathrm{M}(\epsilon_u)$ où M désigne l'une des sous-extensions de $\mathbf{Q}_l(\epsilon_{2^r})$ de degré 2^t. On sait ([28]) qu'on a l'inégalité :

$$v_{\mathfrak{P}'}((\pi^k_{\mathrm{M}(\epsilon_u)}/k) \,.\, d(\mathrm{M}(\epsilon_u))/2) \geqslant 0 .$$

On en déduit facilement l'inégalité (2) du lemme.

Nous pouvons achever la démonstration de la proposition 4.3. On peut naturellement associer à $a_i^{l^n}$ (resp. $a_i^{2^{n-1}}$) si l est différent de 2 (resp. égal à 2) un élément b_i de $1 + \mathrm{F}_l \mathfrak{M}_i$ tel qu'on ait :

$$\mathrm{N}_i(b_i) = \mathrm{N}_{\mathrm{L}_i|\mathrm{K}_i}(a_i)^{l^n} \quad (\text{resp. } \mathrm{N}_{\mathrm{L}_i|\mathrm{K}_i}(a_i)^{2^{n-1}})$$

si l est différent de 2 (resp. égal à 2). L'élément b de $\mathfrak{M}_l^*$ dont les composantes sur $\mathfrak{M}_i$ sont égales à b_i appartient à l'intersection $\mathbf{Z}_l[\Gamma] \cap \mathfrak{M}_l^*$; c'est donc une unité de $\mathbf{Z}_l[\Gamma]$. On a les égalités : $\det_{\theta_i}(b) = \det_{\theta_i}(\alpha)^{l^n}$ (resp. $\det_{\theta_i}(\alpha)^{2^{n-1}}$), $1 \leqslant i \leqslant m$, si l est différent de 2 (resp. égal à 2). Or tout caractère irréductible θ de Γ est conjugué d'un caractère θ_i ; on en déduit les égalités : $\det_\theta(b) = \det_\theta(\alpha)^{l^n}$ (resp. $\det_\theta(\alpha)^{2^{n-1}}$) si l est différent de 2 (resp. égal à 2) pour tout caractère irréductible de Γ et donc pour tout caractère θ de Γ.

5. Démonstration du théorème 3.2.

On suppose, dans ce paragraphe, que Γ est le produit semi-direct d'un sous-groupe H abélien, distingué et d'ordre m par un sous-groupe abélien F d'ordre s ; on suppose que m et s sont premiers entre eux.

a) *Représentations des groupes métabéliens*

Déterminons les représentations irréductibles du groupe Γ. Le groupe F opère sur les caractères de degré 1 de H et on note $\hat{\chi}$ l'orbite du caractère χ. A tout caractère χ de H on associe les éléments suivants qui ne dépendent que de $\hat{\chi}$: $\mathrm{F}_{\hat{\chi}}$ le sous-groupe d'isotropie de χ, $\Gamma_{\hat{\chi}}$ le produit semi-direct de H par $\mathrm{F}_{\hat{\chi}}$, $g_{\hat{\chi}}$ son ordre, c'est-à-dire l'ordre de l'image de H par χ. Tout caractère χ de H se prolonge en un caractère de degré 1 de $\Gamma_{\hat{\chi}}$ en posant : $\chi(hf) = \chi(h)$ pour tout h de H et f de $\mathrm{F}_{\hat{\chi}}$.

Soit φ un caractère irréductible de $\mathrm{F}_{\hat{\chi}}$; en composant φ avec la surjection canonique : $(\Gamma_{\hat{\chi}} \longrightarrow \mathrm{F}_{\hat{\chi}})$ on définit un caractère de $\Gamma_{\hat{\chi}}$ de degré 1 et d'ordre g_φ. Le produit $\chi\varphi$ est donc un caractère de degré 1 de $\Gamma_{\hat{\chi}}$. On a alors le résultat suivant ([25]) :

PROPOSITION 5.1. –

(i) *Pour tous caractères irréductibles* χ *de* H *et* φ *de* $\mathrm{F}_{\hat{\chi}}$ *le caractère* $\mathrm{Ind}_{\Gamma_{\hat{\chi}}}^{\Gamma}(\chi\varphi)$ *est irréductible.*

(ii) *Les caractères* $\mathrm{Ind}_{\Gamma_{\hat{\chi}}}^{\Gamma}(\chi\varphi)$ *et* $\mathrm{Ind}_{\Gamma_{\hat{\chi}}}^{\Gamma}(\chi'\varphi')$ *sont égaux si et seulement si* $\hat{\chi} = \hat{\chi}'$ *et* $\varphi = \varphi'$.

(iii) *Tout caractère irréductible de* Γ *est de la forme* $\mathrm{Ind}_{\Gamma_{\hat{\chi}}}^{\Gamma}(\chi\varphi)$ *où* χ *(resp.* φ*) est un caractère de* H *(resp.* $\mathrm{F}_{\hat{\chi}}$*).*

Si ψ est un caractère irréductible de Γ il est donc induit par un caractère de degré 1 d'un unique sous-groupe de Γ qu'on note Γ_ψ et qui est égal au produit semi-direct de H par un sous-groupe F_ψ de F. On remarque que l'ordre de ce caractère de degré 1 ne dépend que de ψ, on le note g_ψ. Si ψ est induit par $\chi\varphi$, on note plus simplement $\psi = (\chi\varphi)^*$. Nous voulons déterminer le corps $\mathbf{Q}(\psi)$ obtenu par adjonction à $\mathbf{Q}$ des valeurs du caractère ψ. Nous nous plaçons dans l'hypothèse restrictive où le groupe Γ vérifie la condition (C) définie au paragraphe 3.

Si $\mathbf{Q}^{(g_\psi)}$ désigne le corps cyclotomique des racines g_ψ-ème de l'unité, on a la proposition suivante :

PROPOSITION 5.2. – *Si* ψ *est un caractère irréductible d'un groupe métabélien* Γ *qui satisfait la condition* (C) *alors* $\mathbf{Q}(\psi)$ *est le corps des invariants de* $\mathbf{Q}^{(g_\psi)}$ *par un sous-groupe de* $G(\mathbf{Q}^{(g_\psi)}/\mathbf{Q})$ *isomorphe à* F/F_ψ .

Démontrons cette proposition. On suppose que le caractère ψ est égal au caractère $(\chi\varphi)^*$ et on note a_χ un élément de H tel que $\chi(a_\chi)$ soit une racine primitive g_χ-ème de 1 ; on note ϵ_{g_χ} (resp. ϵ_{g_φ}) cette racine (resp. une racine primitive g_φ-ème de 1). Le sous-groupe $\operatorname{Ker}\chi$ de H est distingué dans Γ, donc, pour tout y de F, $\chi(ya_\chi y^{-1})$ est une racine primitive g_χ-ème de 1. On définit l'application $(y \longmapsto u_y)$ de F dans $G(\mathbf{Q}^{(g_\psi)}/\mathbf{Q})$ où u_y est le $\mathbf{Q}$-automorphisme de $\mathbf{Q}^{(g_\psi)}$ défini par : $u_y(\epsilon_{g_\chi}) = \chi(ya_\chi y^{-1})$ et $u_y(\epsilon_{g_\varphi}) = \epsilon_{g_\varphi}$. L'application $(y \longmapsto u_y)$ est un homomorphisme de groupe dont le noyau est le groupe F_ψ . On considère dans ce paragraphe F/F_ψ comme un sous-groupe de $G(\mathbf{Q}^{(g_\psi)}/\mathbf{Q})$. Soit K_ψ le corps des invariants de F/F_ψ dans $\mathbf{Q}^{(g_\psi)}$. Le caractère ψ vérifie les égalités : $\psi(x) = \mathrm{Tr}_{\mathbf{Q}^{(g_\psi)}/K_\psi}((\chi\varphi(x)))$ (resp. 0). Si x appartient (resp. n'appartient pas) à Γ_ψ . On en déduit l'égalité $\mathbf{Q}(\psi) = K_\psi$.

b) *Facteurs simples de* $\mathbf{Q}[\Gamma]$

L'algèbre de groupe $\mathbf{Q}[\Gamma]$ est semi-simple et se décompose en une somme directe de $\mathbf{Q}$-algèbres simples. On sait que toute algèbre simple sur un corps de nombres est un produit croisé. Nous nous proposons de déterminer, à un isomorphisme près, les produits croisés qui apparaissent, dans la décomposition en facteurs simples de l'algèbre $\mathbf{Q}[\Gamma]$, associée à un groupe métabélien, qui vérifie la condition (C). On peut trouver des résultats pour cette étude dans [29], [30], [31] ou [12]. Nous adoptons les notations de [22]. Soit L une extension galoisienne finie d'un corps de nombres K et soit G le groupe $G(L/K)$. A tout 2 cocycle f de $\mathbf{Z}^2(G, L^*)$ on peut associer une classe d'isomorphisme de K-algèbres centrales simples. On note $(L/K, f)$ un représentant de cette classe ; c'est une algèbre qui possède une base sur L de la forme $\{u_\sigma\}_{\sigma\in G}$ qui satisfait les propriétés suivantes : $u_\sigma . x = \sigma(x)\, u_\sigma$, $u_\sigma u_\tau = f(\sigma,\tau)\, u_{\sigma\tau}$ pour tous x de L et σ et τ de G.

Soit ψ un caractère irréductible de Γ. On sait (proposition 5.1) que $\psi = (\chi\varphi)^*$ où φ est déterminé de manière unique. Soit t une application de F/F_ψ dans F qui définit un système de représentants. On désigne par $f^{(\psi)}$ l'application de $F/F_\psi \times F/F_\psi$ dans $\mathbf{Q}^{(g_\psi)*}$ définie par l'égalité :

$$f^{(\psi)}(X, Y) = \varphi(t(X)\, t(Y)\, t(XY)^{-1}) \quad \text{pour } X \text{ et } Y \in F/F_\psi .$$

On montre facilement que $f^{(\psi)}$ est un 2-cocycle c'est-à-dire un élément de $\mathbf{Z}^2(F/F_\psi , \mathbf{Q}^{(g_\psi)*})$; on note $A^{(\psi)}$ le produit croisé $(\mathbf{Q}^{(g_\psi)}/\mathbf{Q}(\psi), f^{(\psi)})$ et on désigne par $\{u_X\}_{X\in F/F_\psi}$ une base de $A^{(\psi)}$ sur $\mathbf{Q}^{(g_\psi)}$. On définit un homomorphisme d'algèbre de $\mathbf{Q}[\Gamma]$ sur $A^{(\psi)}$, qu'on note $\Phi^{(\psi)}$, de la manière suivante : si x appartient à $\mathbf{Q}[\Gamma]$ il s'écrit $\sum_{X\in F/F_\psi} \alpha_X\, t(X)$ avec α_X appartenant à $\mathbf{Q}[\Gamma_\psi]$; on définit $\Phi^{(\psi)}(x)$ par l'égalité :

$$\Phi^{(\psi)}(x) = \sum_{X\in F/F_\psi} (\chi\varphi)(\alpha_X)\, u_X .$$

Le groupe $\Omega_{\mathbf{Q}}$ opère sur les caractères irréductibles de tout sous-groupe G de Γ. On note $\dot{G}$ l'ensemble des orbites des caractères de G. La notation $\chi \in \dot{\chi}$ signifie que χ parcourt un système de représentants des éléments de $\dot{G}$. On obtient un système de représentants S de $\dot{\Gamma}$ en considérant les caractères : $\{(\chi\varphi)^*$, avec $\chi \in \dot{H}$ et $\varphi \in \dot{F}_\chi\}$. On a la proposition suivante :

PROPOSITION 5.3. – *L'homomorphisme d'algèbre* $\Phi = \prod_{\psi\in S} \Phi^{(\psi)}$ *de* $\mathbf{Q}[\Gamma]$ *dans* $\prod_{\psi\in S} A^{(\psi)}$ *est un isomorphisme.*

On montre facilement que l'homomorphisme Φ est injectif et on achève la démonstration de cette proposition en montrant que les dimensions sur $\mathbf{Q}$ des algèbres $\mathbf{Q}[\Gamma]$ et $\prod_{\psi\in S} A^{(\psi)}$ sont égales.

Dans la suite de ce paragraphe on identifie les algèbres $\mathbf{Q}[\Gamma]$ et $\prod_{\psi\in S} A^{(\psi)}$; dans cette identification l'algèbre $\mathbf{Z}[\Gamma]$ devient un ordre de $\mathbf{Z}$ dans $\prod_{\psi\in S} A^{(\psi)}$ contenu dans l'ordre $\mathfrak{U} = \prod_{\psi\in S} \mathfrak{U}^{(\psi)}$ où $\mathfrak{U}^{(\psi)}$ désigne le sous-anneau de $A^{(\psi)}$ des éléments de la forme $\sum_{X\in F/F_\psi} a_X u_X$ où a_X appartient à $\mathbf{Z}^{(g_\psi)}$.

c) *Démonstration du théorème 3.2. (i)*

Nous adoptons les notations suivantes : Pour tout caractère irréductible ψ du groupe Γ on désigne par $R^{(\psi)}$ l'anneau des entiers de $\mathbf{Q}(\psi)$ et pour tout idéal premier $\mathfrak{P}$ (resp. P) de $\mathbf{Z}^{(g_\psi)}$ (resp. $R^{(\psi)}$) on note $\mathbf{Z}_{\mathfrak{P}}^{(g_\psi)}$ (resp. $R_P^{(\psi)}$) l'anneau des entiers du complété pour la valuation $\mathfrak{P}$-adique (resp. P-adique) de $\mathbf{Q}^{(g_\psi)}$ (resp. $\mathbf{Q}(\psi)$). Si l est un nombre premier on note $U^1(\mathbf{Z}_l^{(g_\psi)})$ (resp. $U^1(R_l^{(\psi)})$) le produit $\prod_{\mathfrak{P} \in \mathfrak{S}_l} U^1(\mathbf{Z}_{\mathfrak{P}}^{(g_\psi)})$ (resp. $\prod_{P \in S_l} U^1(R_P^{(\psi)})$) où $\mathfrak{S}_l$ (resp. S_l) désigne l'ensemble des idéaux premiers $\mathfrak{P}$ de $\mathbf{Z}^{(g_\psi)}$ (resp. P de $R^{(\psi)}$) au-dessus de l et on identifie $U^1(R_l^{(\psi)})$ à un sous-groupe de $U^1(\mathbf{Z}_l^{(g_\psi)})$. Le produit des normes locales induit un homomorphisme $N_l^{(\psi)}$ de $U^1(\mathbf{Z}_l^{(g_\psi)})$ dans $U^1(R_l^{(\psi)})$. On utilise les trois lemmes suivants dont nous ne faisons qu'indiquer les démonstrations.

LEMME 5.1. – *Pour tout caractère irréductible* ψ *de* Γ *et tout nombre premier* l *qui divise* $|\Gamma|$ *alors* $N_l^{(\psi)}$ *est un homomorphisme surjectif de* $U^1(\mathbf{Z}_l^{(g_\psi)})$ *sur* $U^1(R_l^{(\psi)})$.

Montrons tout d'abord que pour tout idéal premier P de $\mathbf{Q}(\psi)$ au-dessus du diviseur premier l de $|\Gamma|$ l'extension $\mathbf{Q}^{(g_\psi)}$ de $\mathbf{Q}(\psi)$ est modérément ramifiée en P. En effet si l divise m alors l ne divise pas $[F : F_\psi]$ et donc l ne divise pas l'indice de ramification de P dans $\mathbf{Q}^{(g_\psi)}$; si l divise s alors P n'est pas ramifié dans $\mathbf{Q}^{(g_\psi)}$. Soit $\mathfrak{P}$ un idéal premier de $\mathbf{Q}^{(g_\psi)}$ au-dessus de P, on sait ([24], chapitre V) que la norme locale induit un homomorphisme surjectif de $U^1(\mathbf{Z}_{\mathfrak{P}}^{(g_\psi)})$ sur $U^1(R_P^{(\psi)})$; on en déduit que $N_l^{(\psi)}$ est surjectif.

Remarque. – Pour tout caractère irréductible ψ de Γ le corps $\mathbf{Q}^{(g_\psi)}$ est une extension de $\mathbf{Q}(\psi)$ contenue dans $A^{(\psi)}$ dont le degré sur $\mathbf{Q}(\psi)$ est égal à la racine carré du degré de $A^{(\psi)}$ sur $\mathbf{Q}(\psi)$. On sait qu'alors la restriction à $\mathbf{Q}^{(g_\psi)}$ de la norme réduite de $A^{(\psi)}$ est égale à la norme de corps de $\mathbf{Q}^{(g_\psi)}$ sur $\mathbf{Q}(\psi)$.

Si K est un corps de nombres on note $d(K)$ la différente de K. On définit pour tout caractère ψ de S l'idéal bilatère $\mathfrak{F}^{(\psi)}$ de $\mathfrak{U}^{(\psi)}$ par l'égalité : $\mathfrak{F}^{(\psi)} = |\Gamma_\psi|/d(\mathbf{Q}^{(g_\psi)})$ et on note $\mathfrak{F}$ l'idéal bilatère $\prod_{\psi \in S} \mathfrak{F}^{(\psi)}$ de $\mathfrak{U}$.

LEMME 5.2. – *On a l'inclusion suivante* : $\mathfrak{F}\mathfrak{U} \subset \mathbf{Z}[\Gamma]$.

La démonstration de ce lemme est laissée au lecteur.

Pour tout nombre premier l et tout caractère ψ de S notons $l^{e_l(\psi)}$ l'ordre d'un l-sous-groupe de Sylow de Γ_ψ.

LEMME 5.3. – *Pour tout élément* x *de* $U^1(\mathbf{Z}^{(g_\psi)})$ *on a l'inégalité :* $v_{\mathfrak{P}}(x^{l^{e_l(\psi)-1}} - 1) \geqslant v_{\mathfrak{P}}(\mathfrak{F}^{(\psi)})$.

La démonstration de ce lemme est analogue à celle du lemme 4.3 ; nous ne l'écrivons pas.

Démontrons maintenant le théorème 3.2. (i). On sait par un résultat de Williamson et Harada ([16] et [33]) que $\mathfrak{U}$ est un ordre héréditaire de $\mathbf{Z}$ dans $\prod_{\psi \in S} A^{(\psi)}$. On sait donc ([17]) que tout élément x de $D(\mathbf{Z}[\Gamma])$ possède dans $\operatorname{Hom}^+_{\Omega_{\mathbf{Q}}}(R_\Gamma, U(\overline{\mathbf{Q}}))$ un représentant de la forme $\det(\alpha)$ où α est un élément de $U(\mathfrak{U})$. La proposition 4.2. et la remarque précédente montrent que tout élément x de $\operatorname{Ker} h(\Gamma)$ admet un représentant $\det(\alpha)$ où $\alpha = (\alpha_l)$ est un élément de $U(\mathfrak{U})$ qui vérifie les congruences : $\det_\psi(\alpha_l) \equiv 1 \pmod{\mathfrak{L}}$ pour tout caractère ψ de Γ et tout nombre premier l. Pour démontrer le théorème il suffit de démontrer l'existence, pour tout nombre premier l qui divise $|\Gamma|$, d'un élément a_l de $\mathbf{Z}_l[\Gamma]^*$ tel qu'on ait les égalités : $\det_\psi(\alpha_l)^{l^{e_l(\Gamma)-1}} = \det_\psi(a_l)$ pour tout ψ de S où $e_l(\Gamma)$ est défini par l'égalité : $|\Gamma|_l = l^{e_l(\Gamma)}$.

L'élément $(\det_\psi(\alpha_l))_{\psi \in S}$ définit un élément de $\prod_{\psi \in S} U^1(R_l^{(\psi)})$ et l'on sait par le lemme 5.1. qu'il existe $b_l = (b_l^{(\psi)})_{\psi \in S}$ de $\prod_{\psi \in S} U^1(\mathbf{Z}_l^{(g_\psi)})$ vérifiant :

$$\det_\psi(b_l) = \det_\psi(b_l^{(\psi)}) = N_l^{(\psi)}(b_l^{(\psi)}) = \det_\psi(\alpha_l)$$

pour tout caractère ψ appartenant à S. Or pour tout ψ de S on sait, grâce au lemme 5.3, que $(b_l^{(\psi)})^{l^{e_l(\Gamma)-1}}$ appartient au sous-groupe $1 + (\mathfrak{F}^{(\psi)}\mathfrak{U}^{(\psi)})_l$ de $\mathfrak{U}_l^{(\psi)*}$ et donc $b_l^{l^{e_l(\Gamma)-1}}$ appartient au sous-groupe $1 + (\mathfrak{F}\mathfrak{U})_l$ de $\mathfrak{U}_l^*$; l'élément $b_l^{l^{e_l(\Gamma)-1}}$ appartient à $\mathbf{Z}_l[\Gamma] \cap \mathfrak{U}_l^*$ (lemme 5.2.), c'est-à-dire au groupe $\mathbf{Z}_l[\Gamma]^*$. Nous venons donc de montrer que $\det(\alpha_l)^{l^{e_l(\Gamma)-1}}$ appartient au groupe $\det(\mathbf{Z}_l[\Gamma]^*)$ ce qui achève la démonstration du théorème 3.2. (i).

d) *Démonstration du théorème 3.2. (ii)*

Pour démontrer cette proposition il suffit de montrer que tout élément x de $\operatorname{Ker} h_0(\Gamma)$ possède dans $\operatorname{Hom}^+_{\Omega_{\mathbf{Q}}}(R_\Gamma, U(\overline{\mathbf{Q}}))$ un représentant $\det(\alpha)$ où $\alpha = (\alpha_l)$ est un élément de $U(\mathfrak{U})$ tel qu'on ait : $\det_\psi(\alpha_l) \equiv 1$ (mod. $\mathfrak{L}$) (resp. $= 1$) pour tout nombre premier l et tout caractère ψ de Γ (resp. de degré 1 de Γ).

Nous supposons que le sous-groupe H de Γ est cyclique. Notons Γ' le sous-groupe des commutateurs de Γ et $\Gamma^{(ab)}$ le groupe quotient Γ/Γ'. Puisque Γ/H est un groupe abélien. Γ' est un sous-groupe de H.

LEMME 5.4. – *Si les entiers m et s sont premiers entre eux, alors le groupe $\Gamma^{(ab)}$ est isomorphe à un sous-groupe de Γ.*

La démonstration consiste en la vérification des assertions suivantes :

(i) Soit H'' le centralisateur de F dans H. Alors $[H:H'']$ et $[H'':1]$ sont premiers entre eux.

(ii) Soit U le sous-groupe de H tel que $U \cap H'' = \{1\}$ et $UH'' = H$, alors $\Gamma' \doteq U$.

On en déduit que le groupe $\Gamma^{(ab)}$ est isomorphe au sous-groupe $H''F$ de Γ auquel nous l'identifions et nous considérons $\mathbf{Z}[\Gamma^{(ab)}]$ (resp. $U(\mathbf{Z}[\Gamma^{(ab)}])$) comme une sous-algèbre (resp. un sous-groupe) de $\mathbf{Z}[\Gamma]$ (resp. $U(\mathbf{Z}[\Gamma])$). Tout caractère de degré 1 de Γ est trivial sur le sous-groupe Γ' de Γ et définit par passage au quotient un caractère $\overline{\theta}$ de $\Gamma^{(ab)}$. L'application $(\theta \longrightarrow \overline{\theta})$ définit une bijection de l'ensemble des caractères irréductibles de degré 1 de Γ sur l'ensemble des caractères irréductibles de $\Gamma^{(ab)}$; elle se prolonge en un isomorphisme de $R_\Gamma^{(1)}$ sur $R_\Gamma^{(ab)}$ où $R_\Gamma^{(1)}$ désigne le sous-groupe de R_Γ engendré par les caractères de degré 1. Si ψ est le caractère d'une représentation T de Γ, la restriction de T à $\Gamma^{(ab)}$ définit une représentation de ce groupe qui se décompose en une somme de caractères de degré 1 ; on définit ainsi un homomorphisme $(\psi \longrightarrow \psi')$ de R_Γ sur $R_{\Gamma^{(ab)}}$ (ou $R_\Gamma^{(1)}$).

Soit x un élément de $\operatorname{Ker} h_0(\Gamma)$. Puisque x appartient à $\operatorname{Ker} h(\Gamma)$ il possède un représentant $\det(\alpha)$ dans $\underset{\Omega_{\mathbf{Q}}}{\overset{+}{\operatorname{Hom}}}(R_\Gamma, U(\overline{\mathbf{Q}}))$ de la forme $\det(\alpha)$ où $\alpha = (\alpha_l)$ est un élément de $U(\mathfrak{U})$ tel que : $\det_\psi(\alpha_l) \equiv 1 \pmod{\mathfrak{L}}$ pour tout nombre premier l et tout caractère ψ de Γ. Puisque x appartient à $D_0(\mathbf{Z}[\Gamma])$, il existe $a \in U(\mathbf{Z}[\Gamma^{(ab)}])$ et $u \in \underset{\Omega_{\mathbf{Q}}}{\overset{+}{\operatorname{Hom}}}(R_{\Gamma^{(ab)}}, O_{\overline{\mathbf{Q}}}^*)$ tel qu'on ait : $\det_\theta(\alpha) = \det_\theta(a)\, u(\theta)$ pour tout caractère θ de $\Gamma^{(ab)}$. L'élément a de $U(\mathbf{Z}[\Gamma^{(ab)}])$ définit un élément a de $U(\mathbf{Z}[\Gamma])$; en outre on définit un élément v de $\underset{\Omega_{\mathbf{Q}}}{\operatorname{Hom}}(R_\Gamma, O_{\overline{\mathbf{Q}}}^*)$ en posant : $v(\psi) = u(\psi')$

pour tout caractère ψ de Γ. Si le caractère ψ est symplectique on sait que ψ' est symplectique, ce qui montre que v appartient au groupe $\overset{+}{\mathrm{Hom}}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \mathrm{O}^*_{\overline{\mathbf{Q}}})$. Soit $\beta = (\beta_l)$ l'élément de $\mathrm{U}(\mathfrak{U})$ tel que : $\det(\beta) = \det(\alpha a^{-1})\, v^{-1}$.

Par définition $\det(\beta)$ est un représentant de x dans $\overset{+}{\mathrm{Hom}}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \mathrm{U}(\overline{\mathbf{Q}}))$. Si θ est un caractère de degré 1, on a $\det_\theta(\beta) = 1$; pour tout caractère ψ de Γ on a la congruence :

$$\det_\psi(\beta_l) \equiv \det_\psi(a_l^{-1})\, v^{-1}(\psi) \pmod{\mathfrak{L}}.$$

Or on a l'égalité :

$$\det_\psi(a_l)\, v(\psi) = \det_{\psi'}(a_l)\, u(\psi'),$$

et donc :

$$\det_{\psi'}(a_l)\, u(\psi') = \det_{\psi'}(\alpha_l).$$

On en déduit les congruences : $\det_\psi(\beta_l) \equiv 1 \pmod{\mathfrak{L}}$ pour tout nombre premier l et tout caractère ψ de Γ ce qui achève la démonstration.

6. Etude d'un exemple.

Une étude plus précise du groupe $\mathrm{D}_0(\mathbf{Z}[\Gamma])$ permet dans certains cas particuliers d'améliorer les résultats du théorème 3.2. Nous allons faire une étude du groupe $\mathrm{D}(\mathbf{Z}[\mathrm{H}_{4m}])$ associé au groupe quaternionien généralisé H_{4m} où m est un nombre entier impair ; nous nous intéressons plus particulièrement au cas où m est égal à la puissance d'un nombre premier l. On utilise une généralisation immédiate de la méthode donnée dans [2]. On note C_{2m} l'unique sous-groupe cyclique d'ordre $2m$ de H_{4m}. L'algèbre $\mathbf{Z}[\mathrm{C}_{2m}]$ est contenue dans $\mathbf{Z}[\mathrm{H}_{4m}]$ et on définit par extension des scalaires un homomorphisme θ de $\mathrm{C}(\mathbf{Z}[\mathrm{C}_{2m}])$ dans $\mathrm{C}(\mathbf{Z}[\mathrm{H}_{4m}])$. En utilisant les descriptions données dans [6] des groupes $\mathrm{C}(\mathbf{Z}[\mathrm{C}_{2m}])$ et $\mathrm{C}(\mathbf{Z}[\mathrm{H}_{4m}])$, l'homomorphisme θ est défini par passage au quotient par l'application : $(f \longrightarrow \tilde{f})$ de $\mathrm{Hom}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_{\mathrm{C}_{2m}}, \mathrm{J}(\overline{\mathbf{Q}}))$ dans $\mathrm{Hom}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_{\mathrm{H}_{4m}}, \mathrm{J}(\overline{\mathbf{Q}}))$ où $\tilde{f}$ est défini par l'égalité : $\tilde{f}(\theta) = f(i^*(\theta))$ pour tout $\theta \in \mathrm{R}_{\mathrm{H}_{4m}}$. i^* désignant l'homomorphisme de $\mathrm{R}_{\mathrm{H}_{4m}}$ dans $\mathrm{R}_{\mathrm{C}_{2m}}$ induit par l'injection canonique i de C_{2m} dans H_{4m}, et où $\mathrm{J}(\overline{\mathbf{Q}})$ désigne le groupe des idèles de $\overline{\mathbf{Q}}$.

a) *Résultats*

On adopte les notations suivantes : $K^{(d)}$ est la sous-extension réelle maximale de $\mathbf{Q}^{(d)}$ et on note $R^{(d)}$ son anneau d'entiers. On a un isomorphisme de $\mathbf{Z}$-algèbre de $\mathbf{Z}[C_{2m}]$ dans $\prod_{d|m} (\mathbf{Z}^{(d)} \times \mathbf{Z}^{(d)})$ et on identifie $\mathbf{Z}[C_{2m}]$ avec son image dans $\prod_{d|m} (\mathbf{Z}^{(d)} \times \mathbf{Z}^{(d)})$. On désigne par Λ_{2m} le sous-anneau $\mathbf{Z}[C_{2m}] \cap \prod_{d|m} (R^{(d)} \times R^{(d)})$ de $\prod_{d|m} (\mathbf{Z}^{(d)} \times \mathbf{Z}^{(d)})$; c'est un ordre de $\mathbf{Z}$ dans la $\mathbf{Q}$-algèbre $\prod_{d|m} (K^{(d)} \times K^{(d)})$ contenu dans $\prod_{d|m} (R^{(d)} \times R^{(d)})$ qui est l'unique ordre maximal de cette algèbre. On note $D(\Lambda_{2m})$ le noyau de l'homomorphisme induit par l'extension des scalaires de $C(\Lambda_{2m})$ sur $\prod_{d|m} (C(R^{(d)}) \times C(R^{(d)}))$. Pour tout diviseur premier l de m on note e_l le plus grand entier n tel que l^n divise m.

THEOREME 6.1. –

(i) *Le conoyau de l'homomorphisme induit par extension des scalaires de* $D(\mathbf{Z}[C_{2m}])$ *dans* $D(\mathbf{Z}[H_{4m}])$ *est un 2-groupe élémentaire dont l'ordre est égal à* $2^{\sum_{l|m} e_l}$.

(ii) *Il existe un homomorphisme surjectif de* $D(\mathbf{Z}[H_{4m}])$ *dans* $D(\Lambda_{2m})$ *dont le noyau est un 2-groupe élémentaire.*

On dit que H est un l'-groupe lorsque l est un nombre premier qui ne divise pas $|H|$.

COROLLAIRE 6.1. – *Le groupe* $D(\mathbf{Z}[H_{4l^n}])$ *est somme directe d'un 2-groupe élémentaire dont l'ordre est égal à* 2^n *et d'un 2'-groupe isomorphe à* $D(\Lambda_{2l^n})$. *En outre lorsque* l *est un nombre premier régulier et que l'ordre de 2 modulo* l *est pair, alors* $D(\Lambda_{2l^n})$ *est un* l'*-groupe isomorphe au groupe :* $\prod_{1 \leq i \leq n} ((R^{(l^i)}/2)^* / \mathrm{Im}.\, R^{(l^i)*})$.

Remarque. – Le résultat du corollaire 6.1. complète un résultat de Wilson ([32]) et de Fröhlich ([9]).

COROLLAIRE 6.2. – *Si* N *est une extension galoisienne modérément ramifiée d'un corps de nombres* K *dont le groupe de Galois est isomorphe au groupe quaternionien* H_{4l^n} *où* l *est un nombre premier impair et régulier tel que l'ordre de 2 modulo* l *soit pair, alors dans* $D(\mathbf{Z}[G(N/K)])$ *on a l'égalité :* $U_{N/K} = t^+(W_{N/K})$.

Le groupe H_{4l^n} est engendré par ω et σ qui vérifient les égalités $\omega^{l^n} = 1 = \sigma^4$ et $\sigma\omega\sigma^{-1} = \omega^{-1}$. Pour tout entier i, $1 \leqslant i \leqslant n$, on note ϵ_{l^i} une racine primitive l^i-ème de l'unité et on désigne par θ_i le caractère de degré 1 de C_{2l^n} défini par : $\theta_i(\omega) = \epsilon_{l^i}$ et $\theta_i(\sigma^2) = -1$. Notons θ^* le caractère de H_{4l^n} induit par le caractère θ de C_{2l^n}. L'ensemble $\{\theta_i^*, 1 \leqslant i \leqslant n\}$ est un système de représentants des orbites de l'ensemble des caractères symplectiques irréductibles de H_{4l^n} sur lequel opère $\Omega_{\mathbf{Q}}$. Si N est une extension galoisienne de $\mathbf{Q}$ dont le groupe de Galois est H_{4l^n} à chaque i, $1 \leqslant i \leqslant n$, on associe la valeur ± 1 de la constante $W(\theta_i^*, N/\mathbf{Q})$ qu'on note $W_i(N)$. Le corollaire 6.1. montre que la 2-composante de $D(\mathbf{Z}[H_{4l^n}])$ est un 2-groupe élémentaire d'ordre 2^n qu'on identifie au produit de n copies du groupe multiplicatif $\{\pm 1\}$. Si a est un entier non divisible par l on note $\left(\frac{a}{l}\right)$ le symbole de Legendre.

COROLLAIRE 6.3. – *Si* N *est une extension galoisienne modérément ramifiée de* $\mathbf{Q}$ *dont le groupe de Galois est isomorphe au groupe quaternionien* H_{4l^n} *où* l *est un nombre premier impair, alors* :

(i) *on a l'égalité* :

$$U_{N/\mathbf{Q},2} = \left\{ \left(\frac{W_i(N)}{l}\right),\ 1 \leqslant i \leqslant n \right\} ;$$

(ii) *si* l *est régulier et si l'ordre de* 2 *modulo* l *est pair, on a l'égalité* :

$$U_{N/\mathbf{Q}} = \left\{ \left(\frac{W_i(N)}{l}\right),\ 1 \leqslant i \leqslant n \right\} .$$

Remarque 1. – Si l'unique sous-extension quadratique de N est imaginaire on sait ([14] ou [10]) que $W_i(N) = 1$, $1 \leqslant i \leqslant n$; on en déduit que $U_{N/\mathbf{Q},2} = 1$ et même que O_N est un $\mathbf{Z}[G(N/\mathbf{Q})]$-module stablement libre sous les hypothèses du corollaire 6.3. (ii).

Remarque 2. – Lorsque $\left(\frac{2}{l}\right) = -1$ l'ordre de 2 modulo l est pair ; inversement si $l \equiv 1$ (mod. 4) et si l'ordre de 2 modulo 1 est pair, alors $\left(\frac{2}{l}\right) = -1$. Le corollaire 3 nous donne les résultats simples suivants :

Si N est une extension modérément ramifiée de $\mathbf{Q}$ dont le groupe de Galois est isomorphe à H_{4l^n} où l est un nombre premier et régulier lorsque $n > 1$:

(i) si $l \equiv 1 \pmod{4}$ et $l \not\equiv 1 \pmod{8}$ alors O_N est un $\mathbf{Z}[H_{4l^n}]$-module stablement libre.

(ii) si $l \equiv -1 \pmod{4}$ et $l \not\equiv -1 \pmod{8}$ alors O_N est un $\mathbf{Z}[H_{4l^n}]$ module stablement libre si et seulement si $W_i(N) = 1$ pour tout entier i tel que $1 \leqslant i \leqslant n$.

b) *Démonstrations des résultats*

Le théorème 6.1. est une généralisation immédiate des théorèmes 1 et 2 de [2]. Les corollaires 2 et 3 sont des conséquences du corollaire 1 et du théorème 3 de [9]. Démontrons maintenant le corollaire 1. Etudions pour cela le noyau $D(\Lambda_{2l^n})$ de l'homomorphisme φ induit par l'extension des scalaires de $C(\Lambda_{2l^n})$ sur $\prod_{0\leqslant i\leqslant n} (C(R^{(l^i)}) \times C(R^{(l^i)}))$ où $R^{(l^0)}$ désigne par convention l'anneau $\mathbf{Z}$ des entiers relatifs. Notons C_2 le groupe à deux éléments et considérons l'anneau $\prod_{0\leqslant i\leqslant n} R^{(l^i)}[C_2]$; c'est un ordre de $\mathbf{Z}$ dans $\prod_{0\leqslant i\leqslant n} (K^{(l^i)} \times K^{(l^i)})$ qui vérifie :

$$\Lambda_{2l^n} \subset \prod_{0\leqslant i\leqslant n} R^{(l^i)}[C_2] \subset \prod_{0\leqslant i\leqslant n} (R^{(l^i)} \times R^{(l^i)}) .$$

L'homomorphisme φ se décompose en un produit d'homomorphismes g et f induits par extension des scalaires :

$$f : C(\Lambda_{2l^n}) \longrightarrow \prod_{0\leqslant i\leqslant n} C(R^{(l^i)}[C_2])$$

$$g : \prod_{0\leqslant i\leqslant n} C(R^{(l^i)}[C_2]) \longrightarrow \prod_{0\leqslant i\leqslant n} (C(R^{(l^i)}) \times C(R^{(l^i)})) .$$

On a donc l'égalité numérique :

$$|D(\Lambda_{2l^n})| = |\mathrm{Ker}\, f|\ |\mathrm{Ker}\, g| .$$

Si $\mathfrak{U}$ et $\mathfrak{M}$ sont deux ordres de $\mathbf{Z}$ dans une algèbre commutative tels que $\mathfrak{U} \subset \mathfrak{M}$, Serre a montré ([26]) l'isomorphisme suivant

$$\mathrm{Ker}\,[C(\mathfrak{U}) \longrightarrow C(\mathfrak{M})] \simeq (\mathfrak{M}/\overline{F})^*/(\mathfrak{U}/F)^*\, \mathrm{Im}\,.\,\mathfrak{M}^* \qquad (1)$$

où F (resp. $\overline{F}$) désigne un idéal de $\mathfrak{U}$, conducteur de $\mathfrak{M}$ dans $\mathfrak{U}$ (resp. l'idéal engendré par F dans $\mathfrak{M}$). Nous allons en utilisant cet isomorphisme déterminer séparément les groupes $\mathrm{Ker}\, g$ et $\mathrm{Ker}\, f$.

Calcul de Ker g :

Pour tout entier i, $1 \leqslant i \leqslant n$, on note g_i l'homomorphisme induit par l'extension des scalaires de $C(R^{(l^i)}[C_2])$ sur $C(R^{(l^i)}) \times C(R^{(l^i)})$. L'isomorphisme (1) nous donne l'isomorphisme de groupe :

$$\operatorname{Ker} g_i \simeq (R^{(l^i)}/2)^*/\operatorname{Im} R^{(l^i)*}.$$

On en déduit que Ker g est un $2'$-groupe isomorphe au produit direct de groupes :

$$\prod_{1 \leqslant i \leqslant n} ((R^{(l^i)}/2)^*/\operatorname{Im} R^{(l^i)*}).$$

Calcul de Ker f :

Pour tout entier i, $1 \leqslant i \leqslant n$, on note L_i l'unique idéal premier de $R^{(l^i)}$ au-dessus de l et, pour tout $\alpha_i \geqslant 0$, $\overline{L_i^{\alpha_i}}$ l'idéal bilatère de $R^{(l^i)}[C_2]$ engendré par $L_i^{\alpha_i}$. Il existe un conducteur de $\prod_{0 \leqslant i \leqslant n} R^{(l^i)}[C_2]$ dans Λ_{2l^n} de la forme : $\prod_{0 \leqslant i \leqslant n} \overline{L_i^{\alpha_i}}$ où α_i est un entier > 0 qu'on ne précise pas. Le groupe $(R^{(l^i)}[C_2]/\overline{L_i^{\alpha_i}})^*$ est isomorphe au groupe $(R^{(l^i)}/L_i^{\alpha_i})^* \times (R^{(l^i)}/L_i^{\alpha_i})^*$. Le groupe $(R^{(l^i)}/L_i^{\alpha_i})^*$ est somme directe d'un l-groupe et d'un groupe cyclique d'ordre $(l-1)$; la l-composante de ce groupe étant triviale si $\alpha_i = 1$. L'application $R^{(l^i)}[C_2]^* \longrightarrow (R^{(l^i)}/L_i)^* \times (R^{(l^i)}/L_i)^*$ est surjective. En utilisant l'isomorphisme (1) on en déduit que le groupe Ker f est un l-groupe qui est réduit à l'élément neutre si $n = 1$ ce qui démontre la première partie du corollaire 1.

Montrons la seconde partie du corollaire 1. Nous allons montrer que Ker g est un l'-groupe lorsque l'ordre de 2 modulo l est pair et que, si l'entier n est égal à 1 ou si l est régulier, le groupe Ker f est réduit à l'élément neutre. Pour tout entier i, $1 \leqslant i \leqslant n$, notons t_i (resp. s_i) l'ordre de 2 modulo l^i (resp. $[\mathbf{Q}^{(l^i)} : \mathbf{Q}]/t_i$).

Si l'ordre de 2 modulo l est pair, l'entier t_i est pair et l'ordre du groupe $(R^{(l^i)}/2)^*$ est égal à $(2^{t_i/2} - 1)^{s_i}$. Le groupe Ker g_i est un l'-groupe pour tout i, $1 \leqslant i \leqslant n$, et donc Ker g est un l'-groupe.

L'application f se décompose de la manière suivante :

$$C(\Lambda_{2l^n}) \xrightarrow{f_n} C(\Lambda_{2l^{n-1}}) \times C(R^{(l^n)}[C_2]) \longrightarrow \ldots \xrightarrow{f_1} C(\mathbf{Z}[C_2]) \prod_{1 \leqslant i \leqslant n} C(R^{(l^i)}[C_2]).$$

Montrons que pour tout i, $1 \leqslant i \leqslant n$, le groupe $\operatorname{Ker} f_i$ est réduit à l'élément neutre. Nous utilisons pour cela les résultats de Keating ([20]).

Nous donnons un rapide aperçu de la démonstration de l'égalité : $\operatorname{Ker} f_n = \{1\}$. Il existe un conducteur F_n de $\Lambda_{2l^{n-1}} \times R^{(l^n)}[C_2]$ dans Λ_{2l^n} de la forme : $F_n = F_{n-1} \times \overline{L}_n^{(l^{n-1}+1)/2}$. On peut définir un homomorphisme surjectif de groupe de

$$(\Lambda_{2l^{n-1}}/F_{n-1})^* \times (R^{(l^n)}[C_2]/\overline{L}_n^{(l^{n-1}+1)/2})^*$$

sur $(R^{(l^n)}[C_2]/\overline{L}_n^{(l^{n-1}+1)/2})^*$ dont le noyau est le groupe : $(\Lambda_{2l^n}/F_n)^*$. En utilisant (1) on obtient l'isomorphisme :

$$(R^{(l^n)}[C_2]/\overline{L}_n^{(l^{n-1}+1)/2})^*/\operatorname{Im}(R^{(l^n)}[C_2]^*) \simeq \operatorname{Ker} f_n .$$

Lorsque l est un nombre premier régulier, Keating a montré ([20]) que quel que soit l'élément x de $R^{(l^n)}$ congru à 1 modulo L_n il existe une unité u de $R^{(l^n)}$ telle que xu^{-1} soit congru à 1 modulo $L_n^{(l^{n-1}+1)/2}$. En outre lorsque l'ordre de 2 modulo l est pair l'entier $(2^{t_n/2} - 1)$ n'est pas divisible par l et tout élément de $R^{(l^n)}$ vérifie la congruence : $x^{(2^{t_n/2}-1)} \equiv 1 \pmod{2}$; on peut alors choisir l'unité u précédente congrue à 1 modulo 2. Le groupe $\operatorname{Ker} f_n$ est donc réduit à $\{1\}$. Pour tout entier i, $1 \leqslant i \leqslant n$, l'homomorphisme f_i est un isomorphisme et donc f est un isomorphisme. On a donc démontré que lorsque l est régulier et que l'ordre de 2 modulo l est pair le groupe $\operatorname{Ker} f$ est réduit à l'élément neutre.

Appendice I.

Soit Γ un groupe fini. On désigne par $\mathfrak{M}$ un ordre maximal de $\mathbf{Z}$ dans $\mathbf{Q}[\Gamma]$ contenant $\mathbf{Z}[\Gamma]$ et par F le conducteur central ([19]) de $\mathfrak{M}$ dans $\mathbf{Z}[\Gamma]$. Si $\mathfrak{U}$ est un ordre de $\mathbf{Z}$ dans $\mathbf{Q}[\Gamma]$ contenant $\mathbf{Z}[\Gamma]$ on note $D_{\mathfrak{U}}(\mathbf{Z}[\Gamma])$ le noyau de l'homomorphisme induit par l'extension des scalaires de $C(\mathbf{Z}[\Gamma])$ sur le groupe projectif $C(\mathfrak{U})$ associé à $\mathfrak{U}$. On sait ([6]) que $D_{\mathfrak{U}}(\mathbf{Z}[\Gamma])$ est isomorphe au groupe :

$$(\operatorname{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, O_{\overline{\mathbf{Q}}}^*) . \det U(\mathfrak{U}))/(\operatorname{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, O_{\overline{\mathbf{Q}}}^*) . \det U(\mathbf{Z}[\Gamma])) . \qquad (2)$$

A tout nombre premier l on sait associer ([6]) un homomorphisme $r_{l,\Gamma}$ de $\operatorname{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, U(\overline{\mathbf{Q}}))$ sur $\operatorname{Hom}_{\Omega_{\mathbf{Q}}}(\operatorname{Ker} d_{l,\Gamma}, V_l)$ tel que l'image par $r_{l,\Gamma}$ de $\det U(\mathbf{Z}[\Gamma])$ soit réduite à l'élément neutre. On définit ([6]) par passage au quotient un homomorphisme, noté $h_l(\Gamma)$, de $D(\mathbf{Z}[\Gamma])$ sur le groupe $E_l(\Gamma)$ défini par l'égalité :

$$E_l(\Gamma) = \operatorname*{Hom}_{\Omega_{\mathbf{Q}}} (\operatorname{Ker} d_{l,\Gamma}\,, V_l)/r_{l,\Gamma} (\operatorname*{\overset{+}{Hom}}_{\Omega_{\mathbf{Q}}} (R_\Gamma\,, O^*_{\overline{\mathbf{Q}}}))\,.$$

Dans l'anneau des entiers du centre l'idéal F se décompose, pour tout nombre premier l, en un produit $F(l)\,F'(l)$ où $F(l)$ (resp. $F'(l)$) est un idéal entier du centre égal à un produit de puissance d'idéaux maximaux du centre au-dessus de l (resp. premier avec l). Si $\mathfrak{A}$ est un idéal d'un anneau commutatif A, on note $\operatorname{rad}(\mathfrak{A})$ l'intersection des idéaux maximaux de A contenant $\mathfrak{A}$.

PROPOSITION. —

(i) *Pour tout nombre premier* l *on a l'égalité :*

$$\operatorname{Ker} h_l(\Gamma) = D_{\Lambda(l)}(\mathbf{Z}[\Gamma])$$

où $\Lambda(l)$ *est l'ordre de* $\mathbf{Z}$ *dans* $\mathbf{Q}[\Gamma]$ *défini par l'égalité* :

$$\Lambda(l) = \mathbf{Z}[\Gamma] + \operatorname{rad}(F(l))\ \mathfrak{M}\,.$$

(ii) *On a l'égalité* :

$$\operatorname{Ker} h(\Gamma) = D_\Lambda(\mathbf{Z}[\Gamma])$$

où Λ *est l'ordre de* $\mathbf{Z}$ *dans* $\mathbf{Q}[\Gamma]$ *défini par l'égalité* :

$$\Lambda = \bigcap_l \Lambda(l) = \mathbf{Z}[\Gamma] + \operatorname{rad}(F)\ \mathfrak{M}\,.$$

Soit N une extension galoisienne modérément ramifiée d'un corps de nombres K dont le groupe de Galois est noté Γ. On sait que le produit ΛO_N est un sous-Λ-module localement libre de N isomorphe à $\Lambda \underset{\mathbf{Z}[\Gamma]}{\otimes} O_N$. L'élément $U_{N/K}$ de $D(\mathbf{Z}[\Gamma])$ défini par O_N se décompose en un produit $t^+(W_{N/K})\,.\,V_{N/K}$ où $V_{N/K}$ appartient à $\operatorname{Ker} h(\Gamma)$ sous-groupe de $\bigcap_l \operatorname{Ker} h_l(\Gamma)$. La proposition précédente nous fournit l'interprétation suivante du théorème 6.2 ([3]).

COROLLAIRE. — *On a l'isomorphisme de* Λ*-module suivant :* $\Lambda O_N \oplus \Lambda O_N \cong \Lambda \oplus \Lambda$. *En outre, si pour tout caractère symplectique* θ *de* Γ *on a* $W(\theta\,, N/K) = 1$, *alors* ΛO_N *est un* Λ*-module stablement libre et même libre lorsque* $\mathbf{Q}[\Gamma]$ *satisfait la condition d'Eichler ou lorsque* $[K : \mathbf{Q}]$ *est supérieur ou égal à 2.*

Démontrons la proposition. Pour tout nombre premier l' égal à l (resp. différent de l) on a l'égalité : $\Lambda(l)_{l'} = \Lambda_{l'}$ (resp. $\mathfrak{M}_{l'}$).

En utilisant l'isomorphisme (2) et l'égalité :

$$\operatorname{Ker} r'_{l,\Gamma} = \det(\mathbf{Z}_l[\Gamma]^*) \,.\, \det{}^{(1)}(\mathfrak{M}_l^*)\,,$$

qu'on a déduite de la proposition 4.1., on remarque qu'il suffit de démontrer le lemme suivant :

LEMME. – *Pour tout nombre premier* l *on a l'égalité :* $\operatorname{Ker} r'_{l,\Gamma} = \det(\Lambda_l^*)$.

Si l ne divise pas $|\Gamma|$ on a les égalités immédiates suivantes : $\operatorname{Ker} r'_{l,\Gamma} = \det(\mathfrak{M}_l^*) = \det(\Lambda_l^*)$. On suppose maintenant que l divise $|\Gamma|$ et on adopte les notations du paragraphe 4 (proposition 4.3.). Tout élément α de Λ_l^* s'écrit sous la forme $\alpha = a + u$ avec a (resp. u) élément de $\mathbf{Z}_l[\Gamma]$ (resp. $(\operatorname{rad}(F) \,.\, \mathfrak{M})_l$). Pour tout i, $1 \leqslant i \leqslant m$, on a les congruences : $\det_{\theta_i}(\alpha) \equiv \det_{\theta_i}(a) \pmod{P}$. On en déduit que pour tout i, $1 \leqslant i \leqslant m$, $\det_{\theta_i}(a)$ appartient à R_i^* donc a appartient à $\mathbf{Z}_l[\Gamma] \cap \mathfrak{M}_l^* = \mathbf{Z}_l[\Gamma]^*$. On a ainsi montré l'inclusion : $\det(\Lambda_l^*) \subset \det(\mathbf{Z}_l[\Gamma]^*) \,.\, \det^{(1)}(\mathfrak{M}_l^*)$. Inversement, on démontre par une méthode analogue à celle de la proposition 1.3. l'inclusion : $\det^{(1)}(\mathfrak{M}_l^*) \subset \det(1 + (\operatorname{rad}(F) \,.\, \mathfrak{M})_l)$, ce qui achève la démonstration du lemme et de la proposition.

Appendice II.

On sait (lettre de Fröhlich à Martinet) que M. Taylor a récemment démontré une généralisation du théorème de Hilbert et Speiser sous la forme suivante si N/K est une extension abélienne de corps de nombres dont le discriminant D est premier avec le degré n, alors O_N est un $\mathbf{Z}[G(N/K)]$-module libre (note : l'hypothèse $(D, n) = 1$ est plus restrictive que la simple hypothèse de ramification modérée mais cette restriction n'est sans doute que provisoire).

Etant donnée une extension galoisienne N/K, de groupe de Galois Γ, dont le degré est premier avec le discriminant, l'application du résultat ci-dessus conduit à des améliorations de certains résultats de cet article. On peut par exemple montrer qu'on a l'égalité : $U_{N/K}^{A(\Gamma)} = 1$ où $A(\Gamma)$ désigne l'exposant d'Artin de Γ qui divise $[N : K]$ (cf. théorème 3.1.). Cette égalité et le théorème 3.2. permettent, en particulier, de démontrer la conjecture de Fröhlich lorsque Γ est un groupe diédral D_{2m} ou quaternionien H_{4m} où m est un nombre entier impair.

BIBLIOGRAPHIE

[1] Ph. CASSOU-NOGUES, Classes d'idéaux de l'algèbre d'un groupe abélien et applications, *Mémoire de la S.M.F.*, n° 37 (1974).

[2] Ph. CASSOU-NOGUES, Groupe des classes de l'algèbre d'un groupe métacyclique, *J. of Algebra,* 1 (1976).

[3] Ph. CASSOU-NOGUES, Structure galoisienne des anneaux d'entiers, à paraître in *Proc. London Math. Soc.*

[4] Ph. CASSOU-NOGUES, Quelques théorèmes de base normale, Journées Arithmétiques de Caen (1976), *Astérisque,* 41-42 (1977), 183-189.

[4a] Ph. CASSOU-NOGUES, Théorèmes de base normale, Séminaire de Théorie des Nombres, Bordeaux, exposé n° 27 (1976-1977) (à paraître).

[5] A. FRÖHLICH, Galois module structure, Durham symposium in Algebraic Number Fields, A. Fröhlich éd. Academic Press, (1977), 133-191.

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

[7] A. FRÖHLICH, Galois module structure and Artin L-functions, *Proc. int. congress of Mathematicians Vancouver* (1974), 1 (1975), 351-356.

[8] A. FRÖHLICH, A normal integral basis theorem, *J. of Algebra,* vol. 39 (1976), n° 1.

[9] A. FRÖHLICH, Module invariants and root numbers for quaternion fields of degree $4l^r$, *Proc. Camb. Phil. Soc.*, 76 (1974), 393-399.

[10] A. FRÖHLICH, Artin root numbers, conductors and representations for generalised quaternion groups, *Proc. London Math. Soc.*, 28 (1974).

[11] A. FRÖHLICH, E. KEATING, S.M.J. WILSON, The class-group of quaternion and dihedral 2-groups, *Mathematika,* vol 21 (1974), n° 41.

[12] J.M. FONTAINE, Sur la décomposition des algèbres de groupes, *Ann. Sc. de l'E.N.S.*, 4^e série, 4 (1971), 121-180.

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

[14] J. GECHTER, Artin root numbers for real characters, *Trans. Amer. Math. Soc.,* (1976), 35-38.

[15] M. HALL, The theory of groups. The Macmillan Company, New-York (1959).

[16] M. HARADA, Some criteria of hereditarity of crossed products, *Osaka J. Math.,* 1 (1964), 69-80.

[17] M. HARADA, Hereditary orders, *Trans. Amer. Math. Soc.,* 107 (1963), 273-290.

[18] D. HILBERT, Die theorie der algebraishen Zahlkörper, *Jahresbericht D. Math. Ver.,* (1897).

[19] H. JACOBINSKI, On extensions of lattices, *Michigan Math. J.,* 13 (1966), 471-475.

[20] M.E. KEATING, Class group of metacyclic group of order $p^r q$, *Mathematika,* vol. 21 (1974), n° 41.

[21] J. MARTINET, Modules sur l'algèbre du groupe quaternionien, *Ann. Sc. de l'E.N.S.,* 4e série, 4, (1971), 299-308.

[22] I. REINER, Maximal orders, Academic Press, London (1975).

[23] D.S. RIM, Module over finite groups, *Ann of Maths,* vol. 69 (1959), 700-713.

[24] J.P. SERRE, Corps locaux, 2e édition, Hermann, Paris (1968).

[25] J.P. SERRE, Représentation linéaire des groupes finis, 2e édition, Hermann, (1971).

[26] J.P. SERRE, Modules projectifs et espaces fibrés à fibre vectorielle, Séminaire Dubreuil (1957-1958), p. 1-17.

[27] M. TAYLOR, Galois module structure of the ring of integers of l-extensions, Thesis of P.H.D., London (1977).

[28] S. ULLOM, The exponent of class group, *J. of Algebra,* vol. 29 (1974), 124-132.

[29] T. YAMADA, On the group algebras of metabelian groups over algebraic number fields I, *Osaka J. Math.,* vol. 6 (1969), 211-228.

[30] T. YAMADA, On the group algebras of metabelian groups over algebraic number fields II, *J. Fac. Sci. Univ. Tokio,* 16 (1969), 83-90.

[31] T. YAMADA, On the group algebras of metacyclic groups over algebraic number fields, *J. Fac. Sci. Univ. Tokio,* 15 (1968), 179-199.

[32] S.M.J. WILSON, Reduced norms in the K-theory of orders, *Proc. London Math. Soc.*.

[33] S. WILLIAMSON, Crossed products and hereditary orders, *Nagoya Math., J.,* 23 (1963), 103-120.

[34] C.W. CURTIS, I. REINER, Representation theory of finite groups and associative algebras, *Interscience,* New-York (1962).

Manuscrit reçu le 28 juin 1977
Proposé par J. Martinet.

Philippe CASSOU-NOGUES,
U.E.R. de Mathématiques
et d'Informatique de
l'Université de Bordeaux I
351, cours de la Libération
33405 – Talence Cedex.