COMPOSITIO MATHEMATICA

JEAN COUGNARD

Propriétés galoisiennes des anneaux d'entiers des p-extensions

Compositio Mathematica, tome 33, n° 3 (1976), p. 303-336

<http://www.numdam.org/item?id=CM_1976__33_3_303_0>

COMPOSITIO MATHEMATICA, Vol. 33, Fasc. 3, 1976, pag. 303–336
Noordhoff International Publishing
Printed in the Netherlands

PROPRIÉTÉS GALOISIENNES DES ANNEAUX D'ENTIERS DES p-EXTENSIONS

Jean Cougnard

Table des matières

Introduction

Soient $N/\mathbb{Q}$ une extension galoisienne et G son groupe de Galois. On note O_N la cloture intégrale de Z dans N et $\mathcal{O}$ un ordre maximal de $Q[G]$ contenant $Z[G]$. Le $\mathcal{O}$-module $\mathcal{O}O_N$ est projectif et Jacques Martinet a conjecturé: $\mathcal{O}O_N$ est stablement libre. Lorsque l'extension $N/\mathbb{Q}$ est modérément ramifiée cette conjecture a été vérifiée par A. Fröhlich ([5]).

L'algèbre $Q[G]$ est isomorphe à un produit d'algèbres simples: $Q[G] \cong \Pi_i A_i$ l'ordre maximal se décompose en un produit: $\mathcal{O} \cong \Pi_i \mathcal{O}_i$ où $\mathcal{O}_i$ est un ordre maximal de A_i. Pour que $\mathcal{O}O_N$ soit stablement libre, il faut et il suffit que chacun des $\mathcal{O}_iO_N$ le soit; cela revient à dire que dans les centres k_i des A_i des idéaux I_i sont principaux (principaux et engendrables par un élément totalement positif dans certains cas).

Si G est un p-groupe, les seules places ramifiées dans les extensions k_i/Q sont celles au-dessus de p et elles sont principales (principales et

engendrables par un élément totalement positif si $p = 2$ et si k_i est réel). Dans ce cas, on peut associer à chaque $\mathcal{O}_i O_N$ un idéal J_i de k_i principal (principal et engendrable par un élément totalement positif le cas échéant); cet idéal coïncide avec I_i sauf aux places au-dessus de p ce qui permet d'énoncer:

THÉORÈME: *Lorsque G est un p-groupe, le $\mathcal{O}$-module $\mathcal{O}O_N$ est stablement libre.*

Compte-tenu du résultat de A. Fröhlich rappelé ci-dessus il était alors permis d'espérer que la conjecture de Jacques Martinet soit vérifiée. Il n'en est malheureusement rien, un contre-exemple ayant été construit (J. Cougnard, contre-exemple à une conjecture de Jacques Martinet, Fourth working research symposium on Galois-module structure and L-functions, Durham 1975, à paraître).

Sans les conseils et les encouragements de Jacques Martinet ce travail n'aurait pas vu le jour, qu'il me soit permis de lui exprimer ici ma gratitude.

Chapitre I. RAPPELS

Tous les modules seront supposés être à gauche.

1. Modules sur les ordres maximaux

Soient O_k un anneau de Dedekind de corps des fractions k et V un k-espace vectoriel de dimension finie. Dans tout ce qui suit on supposera que k est un corps de nombres algébriques. Soient X_1 et X_2 deux O_k-réseaux de V, on notera $\chi_{O_k}(X_1, X_2)$ l'invariant relatif de ces réseaux (pour la définition et les propriétés voir [7]).

Soient A une k-algèbre semi-simple de dimension m et $\mathcal{O}$ un ordre maximal de O_k dans A. L'ordre $\mathcal{O}$ contient la clôture intégrale de O_k dans le centre de A; en particulier, $\mathcal{O}$ contient les idempotents du centre. Si on désigne par $\{e_i\}$ la famille des idempotents irréductibles du centre, orthogonaux deux à deux, $A_i = e_i A$ est une algèbre simple, $\mathcal{O}_i = e_i \mathcal{O}$ est un ordre maximal de O_k dans A_i et on a $A = \Pi_{i \in I} A_i$, $\mathcal{O} = \Pi_{i \in I} \mathcal{O}_i$ (cf. [1]).

Un $\mathcal{O}$-module M sans torsion est projectif ([1]), il sera $\mathcal{O}$-stablement libre si et seulement si $M_i = e_i M$ est $\mathcal{O}_i$ stablement libre. Nous supposerons donc dans la suite de ce paragraphe que A est une

k-algèbre simple, soient C son centre et O_C la clôture intégrale de O_k dans C.

Si le module M est de rang r, on sait qu'il existe un idéal à gauche fractionnaire de O tel que $M \simeq \mathcal{O}^{r-1} \oplus I$ ([8]).

On sait définir la norme réduite dans une algèbre centrale simple; cela permet d'associer à un idéal fractionnaire (donc localement libre) I de $\mathcal{O}$ un idéal fractionnaire de O_C noté $N_{\text{red}}(I)$ et défini localement. On démontre aisément:

PROPOSITION I.1: *Lorsque A est une k-algèbre simple de rang t^2 sur son centre C et I un idéal fractionnaire localement libre de $\mathcal{O}$, on a*:

$$N_{\text{red}}(I)^t = \chi_{O_k}(\mathcal{O}, I).$$

Le théorème suivant est essentiellement dû à Eichler:

THÉORÈME I.1: *L'idéal I est $\mathcal{O}$-stablement libre si et seulement si $N_{\text{red}}(I)$ est un idéal principal (principal totalement positif lorsque A est une algèbre de quaternions totalement définie).*

Si A est une k-algèbre centrale simple, on a alors $A \simeq M_t(D)$ où D est un corps gauche de centre k. Soit Λ un ordre maximal de O_k dans D, alors $M_t(\Lambda)$ est un ordre maximal de O_k dans A (cf. [1]). Soit I un idéal à gauche de $M_t(\Lambda)$. On note e_{ij} $(1 \leq i, j \leq t)$ la matrice dont tous les coefficients sont nuls sauf celui de la i-eme ligne, j-ème colonne qui vaut 1. On a une décomposition de I comme O_k-module: $I = \bigoplus_{i=1}^{t} e_{ii}I$. Les $e_{ii}I$ sont des O_k-modules isomorphes, l'isomorphisme de $e_{ll}I$ dans $e_{ii}I$ étant la multiplication à gauche par $e_{i,l}$. On en déduit:

PROPOSITION I.2: *Soit I un idéal à gauche fractionnaire de $M_t(\Lambda)$, avec les notations précédentes on a*:

$$\chi_{O_k}(M_t(\Lambda), I) = \chi_{O_k}(e_{ll}M_t(\Lambda), e_{ll}I)^t.$$

2. Caractères induits et représentations induites

DEFINITION I.1: Soient G un groupe et H un sous-groupe de G, $W \subset V$ deux k-espaces vectoriels tels que H opère sur W et G sur V. Si les conditions suivantes sont réalisées:

(a) W est un sous-module de V considéré comme $k[H]$-module
(b) $V = \bigoplus_{s \in G/H} sW$.

On dit que la représentation V de G est induite par la représentation W de H.

DÉFINITION I.2: Soit φ (resp. ψ) le caractère de H (resp. G) obtenu à partir de W (resp. V) on dit que ψ est le caractère de G induit par le caractère φ de H. On note $\psi = \varphi^*$ ou encore $\psi = \mathrm{Ind}_H^G \varphi$.

Soit T (resp. U) la représentation matricielle de H (resp. de G) fournie par le H-module W (resp. G-module V). On peut expliciter U à l'aide de T de la façon suivante: si T est une représentation de degré r, $[G:H] = t$ et $G = \cup_{i=1}^{t} g_i H$, alors $U(G)$ est une matrice à rt lignes, rt colonnes divisée en t^2 blocs de matrices à r lignes, r colonnes de sorte que dans la i-ème colonne de blocs, j-ème colonne de blocs on trouve $T(g_j^{-1} g g_i)$ où l'on a posé $T(g_j^{-1} g g_i) = 0$ si $g_j^{-1} g g_i \notin H$ et $T(g_j^{-1} g g_i) = T(h)$ si $g_j^{-1} g g_i = h \in H$ (cf. [3]).

Soient $H \subset G$ et A un facteur simple de $\mathbb{Q}[H]$ associé à un caractère absolument irréductible ξ. On suppose que $\mu = \xi^*$ est absolument irréductible et que le facteur simple de $\mathbb{Q}[G]$ associé à μ est isomorphe à $M_r(A)$ (où $r = [G:H]$). On désigne par O_ξ (resp. Λ_μ) l'image de $\mathbb{Z}[H]$ (resp. $\mathbb{Z}[G]$) dans A (resp. $M_r(A)$).

PROPOSITION I.3: *Si $\mathcal{O}$ est un ordre maximal contenant O_ξ, la surjection de $\mathbb{Q}[G]$ sur $M_r(A)$ peut être choisie de sorte que $M_r(\mathcal{O})$ soit un ordre maximal contenant Λ_μ.*

DÉMONSTRATION: Si A est une algèbre de matrices sur son centre k, les images des éléments h de H donnent une représentation matricielle dont le caractère est ξ. Par le procédé du §2, on construit la représentation induite, ce qui nous donne la surjection voulue.

Si $A = M_t(D)$ où D est un corps gauche de dimension n^2 sur son centre k, on choisit une extension algébrique K de k qui soit un corps neutralisant de D. Soit $\rho(h)$ l'image de h dans A, l'image de $1 \otimes \rho(h)$ dans $K \otimes_k M_t(D)$ donne une représentation absolument irréductible de H. On construit la représentation induite ce qui nous donne $\rho(g) \in M_{trn^2}(K)$. Cette construction montre que dans l'injection de $M_r(A)$ dans $K \otimes_k M_r(A)$, $\rho(g)$ est l'image d'un élément de $M_r(\mathcal{O})$.

3. Structure de l'algèbre d'un p-groupe sur le corps des rationnels

Précisons les notations que nous utiliserons pour désigner certains p-groupes.

Soit p un nombre premier. Pour tout entier positif n, on désigne par I_n le groupe cyclique d'ordre p^n.

Pour $p = 2$, $n \geq 2$ soit $J = \{l, \tau\}$ un groupe cyclique d'ordre 2 et A_n une extension de J par I_n. Un relèvement $\bar{\tau}$ de τ opère sur I_n par automorphisme intérieur. On pose $A_n = D_n$ si pour tout a dans I_n $\bar{\tau}a\bar{\tau}^{-1} = a^{-1}$ et si A_n est produit semi-direct de I_n par J. Le groupe D_n est isomorphe au groupe diédral d'ordre 2^{n+1}. On pose $A_n = H_n$ si pour tout a dans I_n on a $\bar{\tau}a\bar{\tau}^{-1} = a^{-1}$ et s'il n'y a pas de relèvement de τ d'ordre 2. Le groupe H_n est isomorphe au groupe quaternionien d'ordre 2^{n+1}.

Pour $p = 2$, $n \geq 3$ on pose $A_n = M_n$ si pour tout a dans I_n $\bar{\tau}a\bar{\tau}^{-1} = a^{-1+2^{n-1}}$ et si A_n s'identifie au produit semi-direct de J par I_n.

Rappelons qu'étant donné le caractère χ d'une représentation ρ d'un groupe G, on note $\operatorname{Ker}\chi$ le noyau de ρ. On peut alors énoncer le théorème suivant dont on trouvera une démonstration dans ([4]).

THÉORÈME I.2: *Soient G un p-groupe et ψ un caractère absolument irréductible de G; il existe un sous-groupe H' de G et un caractère η de H' tels que*:

(a) $\mathbb{Q}(\psi) = \mathbb{Q}(\eta)$

(b) $\psi = \eta^*$

(c) *le quotient de H' par* $\operatorname{Ker}\eta$ *est isomorphe à l'un des groupes I_n, D_n, H_n ou M_n. On dit alors que ψ est du type I_n (resp. D_n, H_n, M_n).*

Donnons quelques indications sur les représentations absolument irréductibles des groupes I_n, D_n, H_n, M_n. On note ζ_n une racine primitive p^n-ième de l'unité et h un générateur de I_n.

Toutes les représentations absolument irréductibles de I_n sont de degré 1. Par construction η est le caractère d'une représentation fidèle de I_n. Le théorème I.2 montre que pour les caractères de type I_n le facteur simple de $\mathbb{Q}[G]$ associé à η^* est $M_{[G:H]}(\mathbb{Q}(\eta))$. La clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}(\eta)$ est $\mathbb{Z}[\eta]$. Avec les notations de la proposition I.3, Λ_ψ est inclus dans $M_{[G:H]}(\mathbb{Z}[\eta])$.

Dans les groupes D_n, H_n, M_n posons $\bar{\tau}a\bar{\tau}^{-1} = a^r$ quel que soit a appartenant au sous-groupe I_n.

Dans les cas des groupes D_n, M_n on obtient des représentations absolument irréductibles et fidèles en envoyant h sur la matrice

$$\begin{vmatrix} 0 & -\zeta_n\,\zeta_n^r \\ 1 & \zeta_n + \zeta_n^r \end{vmatrix} \text{ et } \bar{\tau} \text{ sur } \begin{vmatrix} 1 & \zeta_n + \zeta_n^r \\ 0 & -1 \end{vmatrix}.$$

Les caractères de ces représentations sont à valeurs dans $\mathbb{Q}(\zeta_n + \zeta_n^r)$. Ces représentations étant rationnelles sur ce corps, les facteurs simples des algèbres de groupes associées à leurs caractères sont isomorphes à

$M_2(\mathbb{Q}(\zeta_n + \zeta_n^r))$. On en déduit que si un caractère absolument irréductible ψ d'un 2-groupe est du type D_n ou M_n le facteur simple associé à ψ est $M_{2[G:H']}(\mathbb{Q}(\psi))$.

Dans le cas d'un groupe H_n on obtient une représentation absolument irréductible et fidèle en envoyant:

$$h \text{ sur } \begin{vmatrix} \zeta_n & 0 \\ 0 & \zeta_n^r \end{vmatrix} \text{ et } \bar{\tau} \text{ sur } \begin{vmatrix} 0 & -1 \\ 1 & 0 \end{vmatrix}.$$

Le caractère de cette représentation est à valeurs dans $\mathbb{Q}(\zeta + \zeta^r)$, mais la représentation ne peut être obtenue par des matrices à coefficients dans ce corps. Le facteur simple de $\mathbb{Q}[H_n]$ associé est le corps gauche $\mathbb{H}_n = \mathbb{Q}(s, t)$ de centre $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ où s et t vérifient les relations $s^{2^{n-1}} + 1 = 0$, $t^2 + 1 = 0$, $tst^{-1} = s^{-1}$. Si le caractère absolument irréductible ψ d'un 2-groupe G est du type H_n, le facteur simple qui lui est associé est $M_{[G:H']}(\mathbb{H}_n)$.

Remarquons que pour les groupes D_n, H_n et M_n, le facteur simple de l'algèbre de groupe associé aux caractères indiqués ci-dessus est de dimension 2^{n-1} sur $\mathbb{Q}$. Comme chacun des trois groupes possède un sous-groupe invariant d'ordre 2, les caractères non conjugués des précédents ne sont pas des caractères fidèles.

Etant donné un caractère absolument irréductible ψ du type D_n (resp. H_n, M_n), on peut appliquer la proposition I.3. On constate que dans les cas D_n, M_n, l'ordre maximal $M_{2[G:H']}(O_{\mathbb{Q}(\chi)})$ contient Λ_ψ. Dans le cas H_n, si $\mathcal{O}$ est un ordre maximal de $\mathbb{H}_n$ contenant s et t, Λ_ψ est inclus dans $M_{[G:H']}(\mathcal{O})$.

Remarquons que dans chacun de ces cas le caractère est induit par un caractère de degré 1 à valeurs dans les racines p^n-ièmes de l'unité.

THÉORÈME I.3: *Soient G un p-groupe et A un facteur simple de $\mathbb{Q}[G]$. Le centre de A est un sous-corps k d'un corps de racines d'ordre p^n de l'unité. Soit Λ la projection de $\mathbb{Z}[G]$ sur A et $\mathcal{O}$ un ordre maximal contenant Λ alors, Λ et $\mathcal{O}$ coïncident localement, sauf éventuellement en p.*

DÉMONSTRATION: La première partie résulte de la discussion précédente. Le discriminant de $\mathcal{O}$ relativement à la trace de A sur $\mathbb{Q}$ divise le discriminant d'un ordre maximal contenant $\mathbb{Z}[G]$, donc divise le discriminant de $\mathbb{Z}[G]$, c'est-à-dire $[G : l]^{[G:l]}$ qui est une puissance de p. Lorsqu'on localise en $(\ell) \neq (p)$, les discriminants de $\mathbb{Z}_\ell[G]$ et $\mathcal{O}_\ell$ sont égaux. L'inclusion $\mathbb{Z}_\ell[G] \subset \mathcal{O}_\ell$ est donc une égalité.

En particulier, Λ_ℓ contient l'anneau des entiers du centre de A_ℓ. En

conséquence, si $\mathfrak{L}$ est une place du centre de A, au-dessus de (ℓ), et si I est un idéal de Λ, on pourra parler de l'invariant $\chi_{O_{k\mathfrak{L}}}(\Lambda_{\mathfrak{L}}, I_{\mathfrak{L}})$.

4. Conséquences pour les anneaux d'entiers

Soient $N/\mathbb{Q}$ une extension galoisienne de groupe de Galois G et O_N la clôture intégrale de $\mathbb{Z}$ dans N. L'anneau O_N possède une structure de $\mathbb{Z}[G]$-module. Soit $\mathcal{O}$ un ordre maximal de $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$ et considérons le $\mathcal{O}$-module $\mathcal{O}O_N = \{z \in N | z = \Sigma_i x_i y_i | x_i \in \mathcal{O},\ y_i \in O_N\}$. On se propose de démontrer que $\mathcal{O}O_N$ est $\mathcal{O}$-stablement libre si G est un p-groupes. L'algèbre $\mathbb{Q}[G]$ est isomorphe à un produit d'algèbres simples A_j de dimension n_j^2 sur leurs centres C_j. On note Λ_j la projection de $\mathbb{Z}[G]$ sur A_j. On a $\mathcal{O} = \Pi_j \mathcal{O}_j$ où $\mathcal{O}_j$ est la projection de $\mathcal{O}$ sur A_j.

Le corps N est un $\mathbb{Q}[G]$-module libre de rang 1; soit θ_0 une base. On peut donc établir un $\mathbb{Q}[G]$ isomorphisme g de $\Pi_j A_j \simeq \mathbb{Q}[G]$ dans N. L'image réciproque de O_N par g est un idéal J de $\mathbb{Z}[G]$, et sa projection sur A_j est un idéal J_j de Λ_j. Posons $I = g^{-1}(\mathcal{O}O_N) = \mathcal{O}J$; on peut écrire $I = \Pi_j I_j$ avec $I_j = \mathcal{O}_j J_j$. Le $\mathcal{O}$-module $\mathcal{O}O_N$ est $\mathcal{O}$-stablement libre si et seulement si chacun des I_j est $\mathcal{O}_j$-stablement libre. D'après la proposition I.1 et le théorème I.1, il revient au même de dire que $\chi_{C_j}(\mathcal{O}_j, I_j)$ est la puissance n_j-ième d'un idéal principal (principal totalement positif si A_j est une algèbre de quaternions totalement définie). Avec ces notations, nous pouvons énoncer les propositions suivantes:

PROPOSITION I.4: *Si G est un p-groupe, p impair, l'idéal $\chi_{C_j}(\mathcal{O}_j, I_j)$ est la puissance n_j-ième d'un idéal principal si et seulement si il existe un idéal principal M_j de C_j tel que pour toute valuation $v_{\mathfrak{L}}$ de C_j avec $\mathfrak{L}$ premier à (p) on ait*:

$$v_{\mathfrak{L}}(\chi_{O_{C_j,\mathfrak{L}}}(\Lambda_{j,\mathfrak{L}}, J_{j,\mathfrak{L}})) = n_j v_{\mathfrak{L}}(M_j).$$

DÉMONSTRATION: Puisque p est impair, $\mathbb{Q}[G]$ ne contient pas de corps de quaternion totalement défini, on n'a donc pas à envisager la condition "totalement positif". Le théorème I.3 montre que pour $\mathfrak{L}$ premier à (p) $\chi_{O_{C_j,\mathfrak{L}}}(\Lambda_{j,\mathfrak{L}}, J_{j,\mathfrak{L}}) = \chi(\mathcal{O}_{j,\mathfrak{L}}, I_{j,\mathfrak{L}})$. La condition de l'énoncé équivaut donc à $\chi_{O_{C_j}}(\mathcal{O}_j, I_j) = M_j^{n_j}(1 - \zeta_{p^n})^x$ ce qui nous permet d'affirmer que la norme réduite de I_j est un idéal principal ce qui démontre la proposition, d'après le théorème I.1.

PROPOSITION I.5: *Si G est un 2-groupe, $\chi_{C_j}(\mathcal{O}_j, I_j)$ est la puissance*

n_j-ième d'un idéal principal (engendré par un élément totalement positif si A_j est une algèbre de quaternions totalement définie) si et seulement si il existe un idéal principal (resp. engendré par un élément totalement positif) M_j de C_j tel que pour toute valuation $v_{\mathfrak{L}}$ de C_j, $\mathfrak{L}$ premier à (2), on ait:

$$v_{\mathfrak{L}}(\chi_{O_{C_j,\mathfrak{L}}}(\Lambda_{j,\mathfrak{L}}, J_{j,\mathfrak{L}})) = v_{\mathfrak{L}}(M_j).$$

DÉMONSTRATION: Le théorème I.3 montre que, pour $\mathfrak{L}$ premier à (2), $v_{\mathfrak{L}}(\chi_{O_{C_j,\mathfrak{L}}}(\Lambda_{j,\mathfrak{L}}, J_{j,\mathfrak{L}})) = v_{\mathfrak{L}}(\chi_{C_j}(\mathcal{O}_j, I_j))$. La condition de l'énoncé peut donc se traduire par:

$$\chi_{O_{C_j}}(\mathcal{O}_j, I_j) = M_j P_j^x$$

où P_j désigne l'unique idéal premier de O_{C_j} au-dessus de (2). D'après le théorème I.2, C_j est un sous-corps du 2^{m_j}-ème corps cyclotomique donc P_j est principal (principal au sens restreint si C_j est totalement réel); il en est donc de même de $\chi_{O_{C_j}}(\mathcal{O}_j, I_j)$; mais la proposition I.1 permet d'écrire $\chi_{O_{C_j}}(\mathcal{O}_j, I_j) = N_{\text{réd}}(I_j)^{n_j}$ où n_j est une puissance de 2. On sait que le nombre de classes de C_j (le nombre de classes au sens restreint si C_j est totalement réel) est impair (cf. [6]) ce qui démontre la proposition I.5.

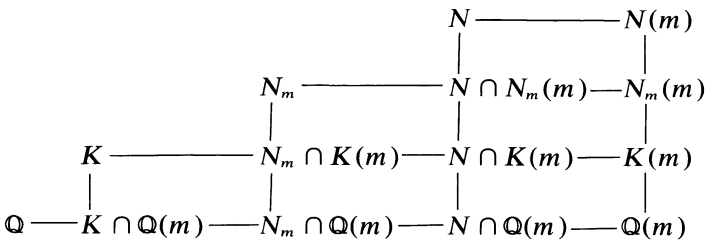
Chapitre II. RÉSOLVANTES DE LAGRANGE

Soit $N/\mathbb{Q}$ une extension galoisienne de groupe de Galois G. On se donne un sous-groupe H d'ordre n et G et un caractère χ de H de degré 1 et d'ordre m.

On note K le sous-corps de N invariant par H, N_m celui invariant par $\operatorname{Ker}\chi$; pour tout diviseur d de m, N_d sera le sous-corps de N_m contenant K et de degré d sur K.

Pour tout entier k et tout corps L, $L(k)$ désignera le corps obtenu en adjoignant à L les racines k-ièmes de l'unité. On note s_i le L-automorphisme de $L(k)$ défini par $s_i(\zeta_k) = \zeta_k^i$ où ζ_k désigne une racine primitive k-ième de l'unité et $(i, k) = 1$.

Dans ce qui suit on adjoindra à N les racines m-ièmes de l'unité. La situation est résumée dans le graphique ci-après:



On note $h_0, h_1, \ldots, h_{m-1}$ un système de représentants des classes de $\mathrm{Gal}(N/K)$ modulo $\mathrm{Gal}(N/N_m)$ et $\bar{h}_0, \bar{h}_1, \ldots, \bar{h}_{m-1}$ leurs images dans $\mathrm{Gal}(N_m/K)$. On convient que $h_0 = id$ et que $\bar{h}_1$ engendre $\mathrm{Gal}(N_m/K)$.

On pose $t = [K \cap \mathbb{Q}(m) : \mathbb{Q}]$ et $t' = [N_m \cap K(m) : K]$. Soient $\sigma_1, \ldots, \sigma_t$ (resp. $\sigma'_1, \ldots, \sigma'_{t'}$) un système de représentants des classes de $\mathrm{Gal}(N(m)/\mathbb{Q})$ modulo $\mathrm{Gal}(N(m)/K \cap \mathbb{Q}(m))$ (resp. de $\mathrm{Gal}(N_m(m)/K)$ modulo $\mathrm{Gal}(N_m(m)/N_m \cap K(m))$. On convient que $\sigma_1 = id$. On désignera par $\bar{\sigma}_1, \ldots, \bar{\sigma}_t$ (resp. $s_{u_1}, \ldots, s_{u_t}$) la restriction de $\sigma_1, \ldots, \sigma_t$ à N (resp. à $\mathbb{Q}(m)$) et par $\bar{h}_{j(k)}$ (resp. s_{v_k}) la restriction de σ'_k à N_m (resp. $K(m)$). Pour tout entier α premier à m, on note α^* l'entier compris entre 1 et m tel que $\alpha\alpha^* \equiv 1 \pmod{m}$.

1. Définition et propriétés élémentaires des résolvantes de Lagrange

DÉFINITION II.1: Soient θ un élément de N et χ' un caractère de degré 1 de H tel que $\ker \chi' \supset \ker \chi$. On appelle résolvante de Lagrange de θ et de χ' l'élément:

$$\langle \theta, \chi' \rangle = \sum_{h \in H} h(\theta)\chi'(h^{-1}).$$

PROPOSITION II.1: *L'élément* $\langle \theta, \chi' \rangle$ *appartient au corps* $N_m(m)$.

DÉMONSTRATION: On a par définition:

$$\langle \theta, \chi' \rangle = \sum_{i=0}^{m-1} \sum_{h' \in \mathrm{Ker}\,\chi} h_i h'(\theta)\chi'(h'^{-1}h_i^{-1})$$

$$= \sum_{i=0}^{m-1} h_i \left(\sum_{h' \in \mathrm{Ker}\,\chi} h'(\theta) \right) \chi'(h_i^{-1}) = \sum_{i=1}^{m} h_i(T_{N/N_m}(\theta))\chi'(h_i^{-1});$$

ce qui démontre la proposition.

Nous utiliserons plusieurs fois par la suite cette expression.

PROPOSITION II.2: *Pour tout $h \in H$ on a* $\langle h\theta, \chi' \rangle = \chi'(h)\langle \theta, \chi' \rangle$.

DÉMONSTRATION: On écrit:

$$\langle h(\theta), \chi' \rangle = \sum_{h' \in H} h'h(\theta)\chi'(h'^{-1}) = \sum_{h' \in H} h'h(\theta)\chi'(h'^{-1}h^{-1})\chi'(h)$$

mais pour h fixé, $h'h$ parcourt H, donc la somme vaut $\chi'(h)\langle \theta, \chi' \rangle$.

Soit σ un $\mathbb{Q}$-automorphisme de N; on note H_σ le groupe $\sigma H \sigma^{-1}$. Pour tout caractère ξ de degré 1 de H, on note ξ_σ le caractère de degré 1 de H_σ défini par $\xi_\sigma(h) = \xi(\sigma^{-1}h\sigma)$. Avec ces notations, nous avons:

PROPOSITION II.3: *Si on fait opérer l'élément σ_i sur la résolvante de Lagrange de θ et χ', on obtient*:

$$\sigma_i(\langle \theta, \chi' \rangle) = \langle \bar{\sigma}_i(\theta), \chi'^{u_i}_{\bar{\sigma}_i} \rangle.$$

DÉMONSTRATION:

$$\sigma_i(\langle \theta, \chi' \rangle) = \sigma_i\left(\sum_{h \in H} h(\theta)\chi'(h^{-1})\right) = \bar{\sigma}_i\left(\sum_{h \in H} h(\theta)\right) s_{u_i}(\chi'(h^{-1}))$$

$$= \sum_{h \in H} \bar{\sigma}_i h \bar{\sigma}_i^{-1}(\bar{\sigma}_i(\theta))\chi'^{u_i}(\bar{\sigma}_i^{-1}\bar{\sigma}_i h^{-1}\bar{\sigma}_i^{-1}\bar{\sigma}_i) = \sum_{h \in H_{\bar{\sigma}_i}} h(\bar{\sigma}_i(\theta))\chi'^{u_i}_{\bar{\sigma}_i}(h^{-1})$$

$$= \langle \bar{\sigma}_i(\theta), \chi'^{u_i}_{\bar{\sigma}_i} \rangle.$$

On suppose que K' est un sous-corps de K tel que N, N_m, K soient galoisiens sur K'. Soit τ' un K'-automorphisme de N, dont la restriction à K est $\bar{\tau}'$; τ' opère par automorphismes intérieurs sur $\mathrm{Gal}(N_m/K)$. On pose $\tau' \bar{h}_i \tau'^{-1} = \bar{h}_i^{\alpha(\tau')}$, où $\alpha(\tau')$ est un entier défini modulo m. On note σ un automorphisme de $N(m)$ dont la restriction à N (resp. à $\mathbb{Q}(m)$) est τ' (resp. s_i).

COROLLAIRE: *Avec les notations ci-dessus,* $\sigma\langle \theta, \chi' \rangle = \langle \tau'\theta, \chi'^{i\alpha(\tau')^*} \rangle$.

DÉMONSTRATION: Il suffit de remarquer qu'ici $\chi'_{\bar{\sigma}} = \chi'^{\alpha(\tau')^*}$.

PROPOSITION II.4: *Soit σ' un K-automorphisme de $N_m(m)$ dont la restriction à $K(m)$ (resp. à N_m) est s_j (resp. h_ℓ). Avec ces notations, on peut écrire*:

$$\sigma'\langle \theta, \chi' \rangle = \chi'^j(h_\ell)\langle \theta, \chi'^j \rangle.$$

DÉMONSTRATION: On a:

$$\sigma'\left(\sum_{h\in H} h(\theta)\chi'(h^{-1})\right) = \sum_{h\in H} h_\ell h(\theta) s_j(\chi'(h^{-1}))$$

$$= \sum_{h\in H} h_\ell h(\theta')\chi'^j(h^{-1}h_\ell^{-1}h_\ell) = \chi'^j(h_\ell)\sum_{h\in H} h(\theta)\chi'^j(h)$$

$$= \chi'^j(h_\ell)\langle\theta, \chi'^j\rangle.$$

COROLLAIRE 1: *Si σ' est un élément* $\mathrm{Gal}(N_m(m)/K(m))$ *on a, avec les notations précédentes*:

$$\sigma'\langle\theta, \chi'\rangle = \chi'(h_\ell)\langle\theta, \chi'\rangle.$$

COROLLAIRE 2: *L'élément $\langle\theta, \chi\rangle^m$ appartient au corps $K(m)$.*

COROLLAIRE 3: *Pour tout élément s_k de* $\mathrm{Gal}(N_m(m)/N_m)$ *on a la relation $s_k\langle\theta, \chi'\rangle = \langle\theta, \chi'^k\rangle$.*

COROLLAIRE 4: *Si s_j est un élément de* $\mathrm{Gal}(K(m)/K)$ *on a*:

$$s_j(\langle\theta, \chi'\rangle^m) = \langle\theta, \chi'^j\rangle^m.$$

DÉMONSTRATION: Soit σ' un K-automorphisme de $N_m(m)$ dont la restriction à $K(m)$ (resp. N_m) est s_j (resp. $\bar{h}_\ell$), alors:

$$s_j(\langle\theta, \chi'\rangle^m) = (\sigma'(\langle\theta, \chi'\rangle))^m = \langle\theta, \chi'^j\rangle^m.$$

COROLLAIRE 5: *Quels que soient les éléments θ et θ' de N tels que $\langle\theta, \chi'\rangle \neq 0$, on a*: $\langle\theta', \chi'\rangle/\langle\theta, \chi'\rangle \in K(m)$.

COROLLAIRE 6: *Quels que soient les caractères χ_1 et χ_2 de degré* 1 *de H, triviaux sur* $\ker\chi$ *et l'élément θ de N tels que $\langle\theta, \chi_1\chi_2\rangle \neq 0$, on a*:

$$\frac{\langle\theta, \chi_1\rangle\langle\theta, \chi_2\rangle}{\langle\theta, \chi_1\chi_2\rangle} \in K(m).$$

En particulier, pour tout entier i, si $\langle\theta, \chi\rangle \neq 0$, $\beta_i(\chi) = \langle\theta, \chi^i\rangle/\langle\theta, \chi\rangle^i \in K(m)$.

PROPOSITION II.5: *Soit $\bar{H}$ le groupe formé des caractères de degré* 1 *de H triviaux sur* $\ker\chi$. *On a la relation*:

$$\sum_{\chi'\in\bar{H}} \langle\theta, \chi'\rangle = mT_{N/N_m}(\theta).$$

DÉMONSTRATION: $\Sigma_{\chi' \in \bar{H}} \langle \theta, \chi' \rangle = \Sigma_{\chi' \in \bar{H}} \Sigma_{h \in \bar{H}} h(\theta) \chi'(h^{-1}) = \Sigma_{h \in H} h(\theta) \Sigma_{\chi' \in \bar{H}} \chi'(h^{-1})$ mais $\Sigma_{\chi' \in H} \chi'(h^{-1}) = 0$ sauf si h appartient à $\operatorname{Ker} \chi$, auquel cas la somme vaut m. Il nous reste donc $\Sigma_{h \in \operatorname{Ker} \chi} mh(\theta) = mT_{N/N_m}(\theta)$.

2. L'application φ

Soit θ_0 un élément de N engendrant une base normale de N/K et une base normale de $N/\mathbb{Q}$.

DÉFINITION II.2: Soit W le $\mathbb{Q}(m)$-espace vectoriel

$$W = K(m) \times \sigma_2(K(m)) \times \cdots \times \sigma_t(K(m)).$$

Les valeurs du caractère χ de H étant des racines m-èmes de l'unité, on en déduit pour le $\mathbb{Q}(m)$-espace vectoriel une structure de $\mathbb{Q}[H]$ module en posant:

$$h \times (a_1, \ldots, a_t) = (\chi(h)a_1, \ldots, \chi(h)a_t).$$

DÉFINITION II.3: On note φ le $\mathbb{Q}$-homomorphisme d'espaces vectoriels de N dans W défini par:

$$\varphi(\theta) = \left(\left(\frac{\langle \theta, \chi \rangle}{\langle \theta_0, \chi \rangle} \right), \ldots, \sigma_i \left(\frac{\langle \theta, \chi^{u_i^*} \rangle}{\langle \theta_0, \chi^{u_i^*} \rangle} \right), \ldots, \sigma_t \left(\frac{\langle \theta, \chi^{u_t^*} \rangle}{\langle \theta_0, \chi^{u_t^*} \rangle} \right) \right).$$

La proposition II.2 a pour conséquence:

PROPOSITION II.6: *L'application φ est un homomorphisme de $\mathbb{Q}[H]$ module.*

PROPOSITION II.7: *L'homomorphisme φ est surjectif.*

DÉMONSTRATION: Soient $x_1, \ldots, x_t$ t éléments de $K(m)$. Cherchons un élément θ de N, tel que $\varphi(\theta) = (x_1, \sigma_2(x_2), \ldots, \sigma_t(x_t))$, ou ce qui revient au même, tel que $\langle \theta, \chi^{u_i^*} \rangle = x_i \langle \theta_0, \chi^{u_i^*} \rangle$. Posons:

$$y = \frac{1}{[N:K]} \sum_{s_j \in \operatorname{Gal}(K(m)/K)} \sum_{\ell=1}^{t} s_j(x_\ell) \langle \theta_0, \chi^{iu_\ell^*} \rangle.$$

Montrons d'abord que cet élément appartient à N. Par construction, et en utilisant la proposition II.1, on voit qu'il appartient à $N_m(m)$. Pour que y appartienne à N il suffit qu'il soit invariant par $\operatorname{Gal}(N_m(m)/N_m)$. On remarque, que d'après le corollaire 3, pour chaque ℓ, on a:

$$\sum_{s_j \in \mathrm{Gal}(K(m)/K)} s_j(x_\ell)\langle \theta_0, \chi^{ju_\ell^*}\rangle = \sum_{j=1}^{t'} \sum_{s_i \in \mathrm{Gal}(N_m(m)/N_m)} s_{v_j} \circ s_i(x_\ell)\langle \theta_0, \chi^{iv_j u_\ell^*}\rangle$$

$$= \sum_{j=1}^{t'} \sum_{s_i \in \mathrm{Gal}(N_m(m)/N_m)} s_i(s_{v_j}(x_\ell)\langle \theta_0, \chi^{v_j u_\ell^*}\rangle)$$

et que cette somme est invariante par $\mathrm{Gal}(N_m(m)/N_m)$. Donc $y \in N_m \subset N$. Notons α l'un des t nombres $1, u_2^*, \ldots, u_t^*$ et calculons $\langle y, \chi^\alpha\rangle$. Pour chaque $h \in H$, on note μ_h un K-automorphisme de $N(m)$ dont la restriction à N est h, on désigne par s_{i_h} la restriction de μ_h à $K(m)$. On aura:

$$\langle y, \chi^\alpha\rangle = \sum_{h \in H} h(y)\chi^\alpha(h^{-1})$$

$$= \sum_{h \in H} \frac{1}{[N:K]} h\left(\sum_{s_j \in \mathrm{Gal}(K(m)/K)} \sum_{\ell=1}^{t} s_j(x_\ell)\langle \theta_0, \chi^{ju_\ell^*}\rangle\right) \chi^\alpha(h^{-1})$$

$$= \frac{1}{[N:K]} \sum_{h \in H} \left[\sum_{s_j \in \mathrm{Gal}(K(m)/K)} \sum_{\ell=1}^{t} \mu_h(s_j(x_\ell))\mu_h(\langle \theta_0, \chi^{ju_\ell^*}\rangle)\right] \chi^\alpha(h^{-1})$$

$$= \frac{1}{[N:K]} \sum_{h \in H} \left[\sum_{s_j \in \mathrm{Gal}(K(m)/K)} \sum_{\ell=1}^{t} s_j s_{i_h}(x_\ell)\langle \theta_0, \chi^{i_h j u_\ell^*}\rangle \chi^{i_h j u_\ell^* - \alpha}(h)\right]$$

mais pour h fixé, s_{ji_h} parcourt $\mathrm{Gal}(K(m)/K)$ quand s_j décrit $\mathrm{Gal}(K(m)/K)$. On peut écrire:

$$\langle y, \chi^\alpha\rangle = \frac{1}{[N:K]} \left[\sum_{s_j \in \mathrm{Gal}(K(m)/K)} \sum_{\ell=1}^{t} s_j(x_\ell)\langle \theta_0, \chi^{ju_\ell^*}\rangle \times \left[\sum_{h \in H} \chi^{ju_\ell^* - \alpha}(h)\right]\right].$$

La deuxième somme entre crochets est nulle sauf si $ju_\ell^* \equiv \alpha \pmod m$, cette éventualité n'a lieu que si $j = 1$, $u_\ell^* = \alpha$, auquel cas la comme vaut $[N:K]$. On a donc l'égalité $\langle y, \chi^\alpha\rangle = x_i\langle \theta_0, \chi^{u_i^*}\rangle$ où i est l'entier pour lequel $\alpha = u_i^*$, ce qui démontre la proposition.

Nous allons maintenant déterminer le noyau de φ. Ecrivons $m = p_1^{a_1} \cdots \times p_d^{a_d}$ et soient N_{m/p_i} les extensions de K telles que $[N_m : N_{m/p_i}] = p_i$.

PROPOSITION II.8: *Le noyau de φ est l'ensemble des θ de N tels que la trace de θ dans l'extension N/N_m puisse s'écrire $T_{N/N_m}(\theta) = \Sigma_{i=1}^{d} x_i$ avec $x_i \in N_{m/p_i}$.*

DÉMONSTRATION: Soit θ tel que $T_{N/N_m}(\theta) \in N_{m/p_i}$ et calculons $\langle \theta, \chi^{u_\ell^*}\rangle$. D'après la proposition III.1 nous avons:

$$\langle \theta, \chi^{u_\ell^*}\rangle = \sum_{i=1}^{m} \bar{h}_i(T_{N/N_m}(\theta))\chi^{u_\ell^*}(h_i^{-1}).$$

Notons $\tau_1, \ldots, \tau_{m/p_i}$ un système de représentants dans $\mathrm{Gal}(N_m/K)$ des classes modulo $\mathrm{Gal}(N_m/N_{m/p_i})$. La somme peut alors s'écrire:

$$\langle \theta, \chi^{u_\ell *} \rangle = \sum_{j=1}^{m/p_i} \sum_{\sigma \in \mathrm{Gal}(N_m/N_{m/p_i})} t_i \sigma(T_{N/N_m}(\theta)) \chi^{u_\ell *}(\sigma^{-1} t_i^{-1})$$
$$= \sum_{i=1}^{m/p_i} \chi^{u_\ell *}(t_i^{-1}) t_i \left(\sum_{\sigma} T_{N/N_m}(\theta) \chi^{u_\ell *}(\sigma^{-1}) \right)$$

comme la dernière somme est nulle, on a démontré l'inclusion dans un sens.

Réciproquement:

si θ est tel que $\varphi(\theta) = 0$, on a $\langle \theta, \chi^{u_\ell *} \rangle = 0$ pour ℓ variant de l à t.

La proposition II.4 montre qu'alors tous les $\langle \theta, \chi^i \rangle$ avec i premier à m sont nuls. On a donc, d'après la proposition II.5:

$$m T_{N/N_m}(\theta) = \sum_{\substack{i=1 \\ (i,m) \neq 1}}^{m} \langle \theta, \chi^i \rangle.$$

Les χ^i étant des caractères de degré 1, le groupe de Galois de $\mathbb{Q}(m)/\mathbb{Q}$ opère sur eux, deux caractères χ^i et χ^j étant conjugués si et seulement si ils ont même ordre. L'ensemble des χ^t $(1 \leq t \leq m,\ (m,t) \neq 1)$ se partage en classes de conjugaisons $C_1, \ldots, C_r$. On peut donc écrire:

$$m T_{N/N_m}(\theta) = \sum_{j=1}^{r} \sum_{\chi^{i_j} \in C_j} \langle \theta, \chi^{i_j} \rangle.$$

Les χ^{i_j} appartenant à une classe C_j fixée sont tels qu'il existe un nombre premier p_j divisant chacun des i_j. Soit $\bar{h}_1$ un générateur de $\mathrm{Gal}(N_m/K)$, l'élément $\bar{h}_1^{m/p_j}$ engendre $\mathrm{Gal}(N_m/N_{m/p_i})$. Soit σ' un K automorphisme de $N_m(m)$ dont la restriction à N_m est $\bar{h}_1^{m/p_j}$ et soit s_v la restriction de σ' à $K(m)$, on a les égalités:

$$\sigma' \left(\sum_{\chi^{i_j} \in C_j} \langle \theta, \chi^{i_j} \rangle \right) = \sum_{\chi^{i_j} \in C_j} \chi^{i_j v}(h_1^{m/p_i}) \langle \theta, \chi^{v i_j} \rangle = \sum_{\chi^{i_j} \in C_j} = \sum_{\chi^{i_j} \in C_j} \langle \theta, \chi^{i_j} \rangle.$$

D'autre part le corollaire 3 à la proposition II.4 montre que $1/m \ \Sigma_{\chi^{i_j} \in C_j} \langle \theta, \chi^{i_j} \rangle$ est invariant par $\mathrm{Gal}(N_m(m)/N_m)$. Cette somme est invariante par $\mathrm{Gal}(N_m(m)/N_m)$ et par σ' donc elle appartient à N_{m/p_j}, ce qui achève la démonstration de cette proposition.

Chapitre III. DÉCOMPOSITION DES RÉSOLVANTES DE LAGRANGE EN PRODUIT D'IDÉAUX

Soit $N/\mathbb{Q}$ une extension galoisienne de groupe de Galois G. On se donne un sous-groupe H et G et un caractère χ de degré 1 et d'ordre m de H. On reprend les notations du chapitre précédent; en particulier χ' est un caractère de degré 1 de H tel que $\operatorname{Ker}\chi' \supset \operatorname{Ker}\chi$.

1. Résultats généraux

Soit θ un élément de N pour lequel $\langle\theta,\chi'\rangle$ n'est pas nul. Ecrivons $(\langle\theta,\chi'\rangle^m) = \mathcal{R}(\chi')^m \prod_{i=1}^{m-1} \mathfrak{U}_i(\chi')^i$ où les idéaux $\mathfrak{U}_i(\chi')$ sont des idéaux entiers, premiers deux à deux, non divisibles par des carrés. On constate aisément que cette décomposition est unique.

PROPOSITION III.1: *Les $\mathfrak{U}_i(\chi')$ et la classe de $\mathcal{R}(\chi')$ sont des invariants de l'extension N/K et du caractère χ'.*

DÉMONSTRATION: Remplaçons θ par un élément θ', on a:

$$\langle\theta',\chi'\rangle^m = \frac{\langle\theta',\chi'\rangle^m}{\langle\theta,\chi'\rangle^m}\langle\theta,\chi'\rangle^m;$$

mais d'après le corollaire 5 à la proposition II.4 l'élément $\langle\theta',\chi'\rangle/\langle\theta,\chi'\rangle$ appartient à $K(m)$. On peut donc écrire:

$$\langle\theta',\chi'\rangle^m = \left(\frac{\langle\theta',\chi'\rangle}{\langle\theta,\chi'\rangle}\mathcal{R}(\chi')\right)^m \prod_{i=1}^{m-1}\mathfrak{U}_i(\chi')^i = \mathcal{R}'(\chi')^m \prod_{i=1}^{m-1}\mathfrak{U}_i'(\chi')^i.$$

L'unicité de la décomposition nous donne le résultat.

Le nombre θ étant choisi, on note $(\langle\theta,\chi'\rangle^m) = \alpha(\chi')$. La décomposition indiquée ci-dessus se transforme en:

$$\alpha(\chi') = \mathcal{R}(\chi')^m \prod_{\substack{d\mid m\\ d\neq 1}} \left(\prod_{\substack{i=1\\(i,d)=1}}^{d} \mathfrak{U}_{i,d}(\chi')^i\right)^{m/d}.$$

NOTATION: Pour tout entier i, et tout diviseur d de m, on note $[i]_d$ le reste de la division de i par d. Rappelons que pour j premier à m, j^* désigne l'entier défini par les conditions $jj^* \equiv 1 \bmod m$ et $1 \leq j^* < m$.

PROPOSITION III.2: *Pour tout entier j premier avec m, on a*:

$$\mathfrak{U}_{[ij]_d,d}(\chi'^j) = \mathfrak{U}_{i,d}(\chi').$$

DÉMONSTRATION: Le corollaire 6 à la proposition II.4 montre qu'il existe un élément $\beta_j(\chi')$ de $K(m)$ tel que $\alpha(\chi') = \beta_j(\chi')^m \alpha(\chi')^j$; ceci nous donne pour la décomposition en idéaux:

$$\mathcal{R}(\chi'^j)^m \prod_{\substack{d|m \\ d\neq 1}} \left(\prod_{\substack{i=1 \\ (i,d)=1}}^{d} \mathfrak{U}_{i,d}(\chi'^j)^i \right)^{m/d} = (\beta_j(\chi)\mathcal{R}(\chi'^j))^m \prod_{\substack{d|m \\ d\neq 1}} \left(\prod_{\substack{i=1 \\ (i,d)=1}}^{d} \mathfrak{U}_{i,d}(\chi')^{ij} \right)^{m/d}$$

$$= \left[\beta_j(\chi')\mathcal{R}(\chi')^j \prod_{\substack{d|m \\ d\neq 1}} \left(\prod_{\substack{i=1 \\ (i,d)=1}}^{d} \mathfrak{U}_{i,d}(\chi')^{(ij-[ij]_d)/d} \right) \right]^m \prod_{\substack{d|m \\ d\neq 1}} \left(\prod_{\substack{i=1 \\ (i,d)=1}}^{d} \mathfrak{U}_{i,j}(\chi')^{[ij]_d} \right)^{m/d}.$$

La proposition se déduit de l'unicité de la décomposition.

COROLLAIRE 1: *On a la relation*: $\mathfrak{U}_{[ij^*]_d,d}(\chi') = \mathfrak{U}_{i,d}(\chi'^j)$.

DÉMONSTRATION: Il suffit dans la relation de la proposition précédente de remplacer j par j^* et χ' par χ'^j.

On voit en particulier:

COROLLAIRE 2: *Si j est congru à 1 modulo d, on a*: $\mathfrak{U}_{i,d}(\chi'^j) = \mathfrak{U}_{i,d}(\chi')$.

PROPOSITION III.3: *En désignant par s_j $((j,m)=1)$ le K-automorphisme de $K(m)$ élevant toute racine m-ième de l'unité à la puissance j, on a*:

$$s_j(\mathfrak{U}_{i,d}(\chi')) = \mathfrak{U}_{[ij^*]_d,d}(\chi').$$

DÉMONSTRATION: Le corollaire 4 à la proposition II.4 montre que l'on a $s_j(\alpha(\chi')) = \alpha(\chi'^j)$, ce qui donne dans la décomposition:

$$s_j(\mathcal{R}(\chi')^m) \prod_{\substack{d|m \\ d\neq 1}} \left(s_j\left(\prod_{\substack{i=1 \\ (i,d)=1}}^{d} \mathfrak{U}_{i,d}(\chi')^i \right) \right)^{m/d} = \mathcal{R}(\chi'^j)^m \prod_{\substack{d|m \\ d\neq 1}} \left(\prod_{\substack{i=1 \\ (i,d)=1}}^{d} \mathfrak{U}_{i,d}(\chi'^j) \right)^{m/d}.$$

L'unicité de la décomposition montre que l'on a $s_j(\mathfrak{U}_{i,d}(\chi')) = \mathfrak{U}_{i,d}(\chi'^j)$ il suffit alors d'appliquer le corollaire 1 à la proposition IV.2.

COROLLAIRE: *Soit s_j un K-automorphisme de $K(m)$. On suppose que la restriction de s_j à $\mathbb{Q}(m)$ laisse invariant le corps $\mathbb{Q}(d)$. Alors, l'idéal $\mathfrak{U}_{i,d}(\chi')$ est invariant par le groupe de Galois de l'extension $K(m)/K(d)$.*

DÉMONSTRATION: L'hypothèse montre que j est congru à 1 modulo d. Le résultat est alors une conséquence du corollaire 2 à la proposition III.2.

2. Idéaux essentiels

On trouvera les démonstrations des quelques résultats non démontrés dans ([2]).

DÉFINITION III.1: Soit n un entier impair ou divisible par 4. Un idéal I de $\mathbb{Q}(n)$ est dit essentiel si:

(a) I est principal,

(b) pour tout i premier à n il existe un idéal principal M_i tel que

$$\frac{s_i(I)}{I^i} = M_i^n.$$

On constate aisément que les idéaux essentiels forment un sous-groupe du groupe des idéaux fractionnaires de $\mathbb{Q}(n)$.

Le lemme suivant est une conséquence immédiate de la définition.

LEMME III.1: *Si I est un idéal principal de $\mathbb{Q}(n)$, I^n est un idéal essentiel.*

Ce lemme admet une réciproque ([2]):

LEMME: III.2: *Si la puissance n-ième d'un idéal est un idéal essentiel, cet idéal est principal.*

LEMME III.3: *L'idéal $\Pi_{s_i \in \mathrm{Gal}(\mathbb{Q}(n)/\mathbb{Q})} s_i(I)^j$ avec $j \equiv ai^* \pmod n$ $1 \leq j \leq n-1$, a fixé, est un idéal essentiel, quel que soit l'idéal fractionnaire I de $\mathbb{Q}(n)$.*

LEMME III.4: *Si n' divise n et si I' est un idéal essentiel de $\mathbb{Q}(n')$ alors l'idéal I de $\mathbb{Q}(n)$ engendré par $I'^{n/n'}$ est essentiel.*

DÉMONSTRATION: Soit s_i un $\mathbb{Q}$-automorphisme de $\mathbb{Q}(n)$ on a:

$$\frac{s_i(I)}{I^i} = \left[\frac{s_i(I')}{I'^i}\right]^{n/n'} = [M_i'^{n'} O_{\mathbb{Q}(n)}]^{n/n'},$$

qui est bien la puissance n-ième d'un idéal principal.

On se propose de démontrer qu'un certain nombre d'idéaux sont des idéaux essentiels. On suppose que m vérifie les conditions de la définition III.1.

PROPOSITION III.4: *L'idéal $I = \Pi_{\ell=1}^{t} N_{\sigma_\ell(K(m))/\mathbb{Q}(m)}(\sigma_\ell(\langle \theta_0, \chi^{u_\ell^*} \rangle^m))$ est un idéal essentiel.*

Nous allons d'abord écrire cet idéal sous une autre forme en tenant compte du résultat suivant:

LEMME III.5: *On a l'égalité*:

$$N_{\sigma_\ell(K(m))/\mathbb{Q}(m)}(\sigma_\ell\langle\theta_0, \chi^{u_\ell^*}\rangle^m)) = s_{u_\ell} N_{K(m)/\mathbb{Q}(m)}(\langle\theta_0, \chi^{u_\ell^*}\rangle^m).$$

DÉMONSTRATION: Soient $\nu_1, \ldots, \nu_k$ un système de représentants des classes de $\mathrm{Gal}(N(m))/\mathbb{Q}(m)$ modulo $\mathrm{Gal}(N(m)/K(m))$; pour $x \in K(m)$, on a:

$$N_{\sigma_\ell(K(m))/\mathbb{Q}(m)}(\sigma_\ell(x)) = \prod_{i=1}^{k} \sigma_\ell \nu_i \sigma_\ell^{-1}(\sigma_\ell(x))$$

$$= \sigma_\ell \prod_{i=1} \nu_i(x) = \sigma_\ell N_{K(m)/\mathbb{Q}(m)}(x)$$

mais la restriction de σ_ℓ à $\mathbb{Q}(m)$ est s_{u_ℓ}, d'où le lemme.

On aura également besoin du lemme suivant:

LEMME III.6: *Si s_v est un K-automorphisme de $K(m)$, on a*:

$$s_v \circ N_{K(m)/\mathbb{Q}(m)} = N_{K(m)/\mathbb{Q}(m)} \circ s_v.$$

DÉMONSTRATION: Soit σ'_v un automorphisme de $N(m)$ dont la restriction à $K(m)$ est s_v. L'automorphisme σ'_v laisse globalement invariant $K(m)$ et appartient donc au normalisateur de $\mathrm{Gal}(N(m)/K(m))$ dans $\mathrm{Gal}(N(m)/\mathbb{Q})$. Les $\sigma'_v \nu_i \sigma'^{-1}_v$ forment donc un système de représentants des classes de $\mathrm{Gal}(N(m)/\mathbb{Q}(m))$ modulo $\mathrm{Gal}(N(m)/K(m))$. On en déduit pour x appartenant à $K(m)$:

$$s_v \circ N_{K(m)/\mathbb{Q}(m)}(x) = \sigma'_v \circ N_{K(m)/\mathbb{Q}(m)}(x) = \prod_{i=1}^{k} \sigma'_v \nu_i(x)$$

$$= \prod_{i=1}^{k} \sigma'_v \nu_i \sigma'^{-1}_v \sigma'_v(x) = N_{K(m)/\mathbb{Q}(m)}(\sigma'_v(x)) = N_{K(m)/\mathbb{Q}(m)}(s_v(x)).$$

Remarquons enfin qu'avec les notations du chapitre II tout $\mathbb{Q}$-automorphisme de $\mathbb{Q}(m)$ s'écrit de façon unique $s_{u_i} \circ s_v$ où $s_v \in \mathrm{Gal}(\mathbb{Q}(m)/K \cap \mathbb{Q}(m))$.

DÉMONSTRATION DE LA PROPOSITION III.4: Il suffit de démontrer que $s_i(I)/I^i$ est la puissance m-ième d'un idéal principal lorsque s_i appartient à $\mathrm{Gal}(\mathbb{Q}(m)/K \cap \mathbb{Q}(m))$ ou bien lorsque s_i est l'un des s_{u_ℓ}.

Si $s_i \in \mathrm{Gal}(\mathbb{Q}(m)/K \cap \mathbb{Q}(m))$, on a, d'après le lemme III.6 et le corollaire 4 à la proposition II.4:

$$s_i N_{K(m)/\mathbb{Q}(m)}(\langle\theta_0, \chi\rangle^m) = N_{K(m)/\mathbb{Q}(m)}(\langle\theta_0, \chi^i\rangle^m)$$

ce qui donne, d'après le corollaire 6 de la proposition II.4:

$$\frac{s_i(N_{K(m)/\mathbb{Q}(m)}\langle\theta_0, \chi\rangle^m)}{(N_{K(m)/\mathbb{Q}(m)}\langle\theta, \chi\rangle^m)^i} = \left[N_{K(m)/\mathbb{Q}(m)}\left(\frac{\langle\theta_0, \chi^i\rangle}{\langle\theta_0, \chi\rangle^i}\right)\right]^m$$

on a donc bien dans ce cas $s_i(I)/I^i$ qui est la puissance m-ième d'un idéal principal.

Si $s_i = s_{u_j}$ avec $1 \leq j \leq t$, on écrit $s_{u_j} \circ s_{u_i} = s_{u_{k(i,j)}} \circ s_{\ell(i,j)}$ ou $s_{\ell(i,j)}$ appartient à $\mathrm{Gal}(\mathbb{Q}(m)/K \cap \mathbb{Q}(m))$, ce qui donne la relation $\ell(i,j)u_i^* \equiv u_{k(i,j)}^* u_j \pmod m$. On en déduit:

$$s_{u_j} \prod_{i=1}^{t} s_{u_i}(N_{K(m)/\mathbb{Q}(m)}(\langle\theta_0, \chi^{u_i^*}\rangle^m))$$

$$= \prod_{i=1}^{t} s_{u_{k(i,j)}} \circ s_{\ell(i,j)}(N_{K(m)/\mathbb{Q}(m)}(\langle\theta_0, \chi^{u_i^*}\rangle^m))$$

ce qui, d'après la démonstration précédente, est égal à:

$$\prod_{i=1}^{t} s_{u_{k(i,j)}} N_{K(m)/\mathbb{Q}(m)}(\langle\theta_0, \chi^{\ell(i,j)u_i^*}\rangle^m).$$

On peut donc mettre l'expression $s_{u_j}(I)/I^{u_j}$ sous la forme:

$$\prod_{i=1}^{t} s_{u_{k(i,j)}} N_{K(m)/\mathbb{Q}(m)}\left(\frac{\langle\theta_0, \chi^{\ell(i,j)u_i^*}\rangle^m}{\langle\theta_0, \chi^{u_k^*(i,j)}\rangle^{u_j m}}\right)$$

que l'on écrit:

$$\left[\prod_{i=1}^{t} s_{u_{k(i,j)}} N_{K(m)/\mathbb{Q}(m)}\left(\frac{\langle\theta_0, \chi^{\ell(i,j)u_i^*}\rangle}{\langle\theta_0, \chi^{u_k^*(i,j)}\rangle^{u_j}}\right)\right]^m$$

grâce au corollaire 6 à la proposition II.4.

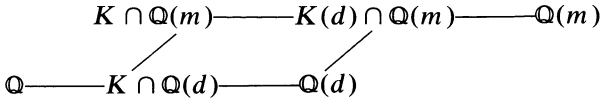
On peut également énoncer la proposition suivante:

PROPOSITION III.5: *Soit d un diviseur de m impair ou congru à 0 modulo 4. Supposons les idéaux $\mathfrak{U}_{i,d}(\chi)$ premiers à m. Alors l'idéal*

$$I_d = \prod_{\ell=1}^{t} s_{u_\ell}\left[\prod_{\substack{i=1 \\ (i,d)=1}}^{d} N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}_{i,d}(\chi^{u_\ell^*})^i)\right]^{m/d}$$

est un idéal essentiel de $\mathbb{Q}(m)$.

DÉMONSTRATION: Le nombre d étant un diviseur de m, on peut considérer les corps $\mathbb{Q}(d)$, $K \cap \mathbb{Q}(d)$, $(K \cap \mathbb{Q}(m))(d) = K(d) \cap \mathbb{Q}(m)$ indiqués dans le schéma ci-dessous:



Soit $s_{u'_j}$ (resp. $s_{u''_n}$) un système de représentants de $\mathrm{Gal}(\mathbb{Q}(m)/\mathbb{Q})$ (resp. $\mathrm{Gal}(\mathbb{Q}(m)/K\cap\mathbb{Q}(d))$ modulo $\mathrm{Gal}(\mathbb{Q}(m)/K\cap\mathbb{Q}(d))$ (resp. $\mathrm{Gal}(\mathbb{Q}(m)/K\cap\mathbb{Q}(m))$.

Les $\mathbb{Q}$-automorphismes s_{u_ℓ} du chapitre précédent s'écrivent sous la forme $s_{u_\ell} = s_{u'_{j(\ell)}} \circ s_{u''_{n(\ell)}} \circ s_{t(\ell)}$ où $s_{t(\ell)} \in \mathrm{Gal}(\mathbb{Q}(m)/K\cap\mathbb{Q}(m))$ et on a l'égalité:

$$u^*_\ell = [u'^*_{j(\ell)}\, u''^*_{n(\ell)}\, t(\ell)^*]_m.$$

Le lemme III.6 et le corollaire à la proposition III.3 montrent que les idéaux $N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}_{i,d}(\chi^{u_\ell^*}))$ sont de la forme $\mathfrak{b}_{i,d}(\chi^{u_\ell^*})\mathbb{Z}[\zeta_m]$ où $\mathfrak{b}_{i,d}(\chi^{u_\ell^*})$ est un idéal de $K(d)\cap\mathbb{Q}(m)$; en effet, ces idéaux sont invariants dans l'extension $\mathbb{Q}(m)/\mathbb{Q}(m)\cap K(d)$ et premiers à m, donc non ramifiés dans cette extension.

Etudions donc:

$$\prod_{\ell=1}^{t} s_{u_\ell}\Bigg[\prod_{\substack{i=1\\(i,d)=1}}^{d} \mathfrak{b}_{i,d}(\chi^{u_\ell^*})^i\Bigg]$$

$$= \prod_{s_{u'_j}}\prod_{s_{u''_n}}\prod_{\ell=1}^{t} s_{u'_{j(\ell)}} \circ s_{u''_{n(\ell)}} \circ s_{t(\ell)}\Bigg[\prod_{\substack{i=1\\(i,d)=1}}^{d} \mathfrak{b}_{i,d}(\chi^{\,u'^*_{j(\ell)}u''^*_{n(\ell)}t(\ell)^*_f})^i\Bigg]$$

ce qui, d'après le lemme III.6 et la proposition III.3, peut s'écrire sous la forme:

$$\prod_{s_{u'_j}}\prod_{s_{u''_n}} s_{u'_{j(\ell)}} \circ s_{u''_{n(\ell)}}\Bigg(\prod_{\substack{i=1\\(i,d)=1}}^{d} \mathfrak{b}_{i,d}(\chi^{\,u'^*_{j(\ell)}u''^*_{n(\ell)}})^i\Bigg).$$

Toujours en utilisant le lemme III.6 et la proposition III.3 on voit que $\mathrm{Gal}(\mathbb{Q}(m)/K\cap\mathbb{Q}(m))$ opère sur les $\mathfrak{b}_{i,d}(\chi)$ par $s_j(\mathfrak{b}_{i,d}(\chi)) = \mathfrak{b}_{[i,j^*]_d,d}(\chi)$, que les $\mathfrak{b}_{[u_j^*]_d,d}(\chi)$ forment un système de représentants des orbites et que l'on obtient chaque élément d'une orbite, une fois et une seule, en faisant opérer sur le représentant les s_i, système représentants des classes de $\mathrm{Gal}(\mathbb{Q}(m)/K\cap\mathbb{Q}(m))$ modulo $\mathrm{Gal}(\mathbb{Q}(m)/K(d)\cap\mathbb{Q}(m))$. On peut donc écrire:

$$\prod_{s_{u'_j}}\prod_{s_{u''_n}} s_{u'_j} \circ s_{u''_n}\Bigg(\prod_{\substack{i=1\\(i,d)=1}}^{d} \mathfrak{b}_{i,d}(\chi^{\,u_j'^*u_n''^*})^i\Bigg)$$

$$= \prod_{s_{u_j}}\prod_{s_{u''_n}} s_{u'_j} \circ s_{u''_n}\Bigg[\prod_{k=1}^{[K\cap\mathbb{Q}(d):\mathbb{Q}]} \prod s_i\,(\mathfrak{b}_{[u_k'^*]_d}\ (\chi^{\,u_j'^*u_n''^*})^{[u_k'^*i^*]_d})\Bigg].$$

Du fait de la disjonction linéaire sur $K \cap \mathbb{Q}(d)$ de $\mathbb{Q}(d)$ et $K \cap \mathbb{Q}(m)$ on peut choisir les $s_{u_n''}$ avec $u_n'' \equiv 1 \pmod{d}$, le corollaire 2 à la proposition III.2 permet alors d'écrire l'expression:

$$\prod_{s_{u_j'}} \prod_{s_{u_n''}} s_{u_j'} \circ s_{u_n''} \left(\prod_{k=1}^{[K\cap\mathbb{Q}(d):\mathbb{Q}]} \prod_{s_i} \mathfrak{b}_{[u_k'^* u']_d,d}(\chi)^{[u_k'^* i^*]_d} \right).$$

Cet idéal est donc engendré dans $\mathbb{Q}(m) \cap K(d)$ par l'idéal

$$\prod_{s_{u_j'}} \prod_{s_i} \prod_{k=1}^{[K\cap\mathbb{Q}(d):\mathbb{Q}]} s_{u_j'} \circ s_i \left(N_{K(d)\cap\mathbb{Q}(m)/\mathbb{Q}(d)} (\mathfrak{b}_{[u_k'^* u_j']_d,d}(\chi))^{[u_k'^* i^*]_d} \right)$$

mais $[u_k'^* u_j']_d = [[u_r'^*]_d \alpha^*(k,j)]_d$ avec

$s_{\alpha(k,j)} \in \mathrm{Gal}(\mathbb{Q}(m)/K \cap \mathbb{Q}(d))$, on a:

$$\prod_{s_i} s_i \circ N_{K(d)\cap\mathbb{Q}(m)/\mathbb{Q}(d)} \left(\mathfrak{b}_{[u_r'^* \alpha(k,j)^*]_d}(\chi)^{[u_k'^* i^*]_d} \right)$$

$$= \prod_{s_i} s_i \circ N_{K(d)\cap\mathbb{Q}(m)/\mathbb{Q}(d)} (\mathfrak{b}_{[u_r'^*]_d}(\chi)^{[u_r'^* u_j'^* i^*]_d}).$$

L'idéal peut donc s'écrire:

$$\prod_{u_r'} \prod_{s_{u_j}} \prod_{s_i} s_{u_j'} \circ s_i (N_{K(d)\cap\mathbb{Q}(m)/\mathbb{Q}(d)} \mathfrak{b}_{[u_r'^*]_d}(\chi)^{[u_r'^* u_j'^* i^*]_d})$$

mais d'après le lemme III.3 le produit

$$\prod_{s_{u_j}} \prod_{s_i} s_{u_j'} \circ s_i \left(N_{K(d)\cap\mathbb{Q}(m)/\mathbb{Q}(d)} \mathfrak{b}_{[u_r'^*]_d}(\chi)^{[u_r'^* u_j'^* i^*]_d} \right)$$

est un idéal essentiel de $\mathbb{Q}(d)$. On achève la démonstration en utilisant le lemme III.4 et le fait que les idéaux essentiels forment un sous-groupe du groupe des idéaux.

COROLLAIRE 1: *Si $m = p^n$, l'énoncé de la proposition précédente reste vrai, sans imposer de condition sur les $\mathfrak{U}_{i,d}(\chi)$.*

DÉMONSTRATION: Supposons que $\mathfrak{U}_{i,d}(\chi')$ ne soit pas premier à p. On peut écrire d'une façon unique: $\mathfrak{U}_{i,d}(\chi') = \mathfrak{U}'_{i,d}(\chi')\mathfrak{U}''_{i,d}(\chi')$ où l'idéal $\mathfrak{U}'_{i,d}(\chi')$ est premier à p tandis que les idéaux premiers divisant $\mathfrak{U}''_{i,d}(\chi')$ sont des diviseurs de p. L'unicité de la décomposition implique $\mathfrak{U}'_{[ij^*]_d,d}(\chi') = \mathfrak{U}'_{i,d}(\chi'^j)$ pour $(j,m) = 1$ et $s_j(\mathfrak{U}'_{i,d}(\chi')) = \mathfrak{U}'_{[ij^*]_d,d}(\chi')$, on a les mêmes relations pour $\mathfrak{U}''_{i,d}(\chi')$.

On écrit $N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}_{i,d}(\chi)) = N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}'_{i,d}(\chi)) N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}''_{i,d}(\chi))$ ce qui donne

$$\prod_{\ell=1}^{t} s_{u_\ell}\left[\prod_{\substack{i=1\\(i,d)=1}}^{d} N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}_{i,d}(\chi^{u_\ell^*}))^i\right]^{m/d}$$

$$=\prod_{\ell=1}^{t} s_{u_\ell}\left[\prod_{\substack{i=1\\(i,d)=1}}^{d} N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}'_{i,d}(\chi^{u_\ell^*}))^i\right]^{m/d}$$

$$\times\prod_{\ell=1}^{t} s_{u_\ell}\left[\prod_{\substack{i=1\\(i,d)=1}}^{d} N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}''_{i,d}(\chi^{u_\ell^*}))^i\right]^{m/d}.$$

Le premier produit se transforme comme dans la proposition précédente, on obtient un idéal essentiel. Considérons le second produit. On utilise les notations $s_{u'_\ell}$, $s_{u''_n}$, s_i définies dans la démonstration de la proposition III.5 on obtient:

$$\prod_{u'_j}\prod_{u''_n} s_{u'_j}\circ s_{u''_n}\left[\prod_{i=1}^{d} N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}''_{i,d}(\chi^{u_j'^* u_n''^* i^*}))\right]^{m/d}$$

$$=\prod_{u'_j} s_{u'_j}\left[\prod_{\substack{i=1\\(i,d)=1}}^{d} N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}''_{i,d}(\chi^{u'_j})^i)\right]^{m/d[K\cap\mathbb{Q}(m):K\cap\mathbb{Q}(d)]}$$

$$=\prod_{u'_j} s_{u'_j}\left[\prod_{k=1}^{[K\cap\mathbb{Q}(d):\mathbb{Q})]}\prod_{s_i} s_i(N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}''_{[u_k'^* i^*]_d,d}(\chi^{u'_j}))^{[u_k'^* i^*]_d})\right]^{[K\cap\mathbb{Q}(m):K\cap\mathbb{Q}(d)]m/d}.$$

Soit en transformant comme dans la proposition III.5

$$\left[\prod_{u'_r}\prod_{u'_j}\prod_{i} s_{u'_j}\circ s_i(N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}''_{[u_r'^* u_j'^* i^*]_d,d}(\chi))^{[u_r'^* u_j'^* i^*]_d}\right]^{[K\cap\mathbb{Q}(m):K\cap\mathbb{Q}(d)]m/d},$$

en posant $N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}''_{[u_r'^* i^*]_d,d}(\chi)) = (1-\zeta_m)^{f(r,d)}$, on obtient:

$$\sum_{u'_r}\left(\sum_{u'_j}\sum_{i}[u_r'^* u_j'^* i^*]_d\right)\frac{m}{d}[K\cap\mathbb{Q}(m):K\cap\mathbb{Q}(d)]f(r,d)$$

$(1-\zeta_m)$

si $d\neq 2$, on a:

$$\sum_{u'_j}\sum_{i}[u_r'^* u_j'^* i^*]_d = d\frac{\varphi(d)}{2}\equiv 0\ (\text{modulo } d)$$

donc la somme est divisible par m, le corollaire est alors conséquence du lemme III.1. Pour $d=2$, on doit étudier $\Pi_{\ell=1}^{t} s_{u_\ell}(N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}_1(\chi^{u_\ell^*})))^{2^{n-1}}$ on décompose $\mathfrak{U}_1(\chi^{u_\ell^*})$ de la même façon que précédemment et on a:

$$\prod_{\ell=1}^{t} s_{u_\ell}(N_{K(m)/\mathbb{Q}(m)}\mathfrak{U}'_1(\chi'^{u_\ell^*}))^{2^{n-1}}\prod_{\ell=1}^{t} s_{u_\ell}(N_{K(m)/\mathbb{Q}(m)}\mathfrak{U}''_1(\chi^{u_\ell^*}))^{2^{n-1}}$$

comme dans la proposition III.5 on voit que $N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}_1'(\chi^{u_\ell^*}))$ est de la forme $\mathfrak{b}'(\chi^{u_\ell^*})\mathbb{Z}[\zeta_{2^n}]$ où $\mathfrak{b}'(\chi'^{u_\ell^*})$ est un idéal de $K \cap \mathbb{Q}(m)$. Le corollaire 2 à la proposition III.2 montre que quel que soit ℓ, $\mathfrak{b}'(\chi^{u_\ell^*}) = \mathfrak{b}'(\chi)$, de même $\mathfrak{U}_1''(\chi^{u_\ell^*}) = \mathfrak{U}_1''(\chi)$. En posant $N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}_1''(\chi)) = (1-\zeta_{2^n})^{f(2)}$, l'idéal étudié se transforme en:

$$[N_{K\cap\mathbb{Q}(m)/\mathbb{Q}}(b'(\chi))(1-\zeta_{2^n})^{tf(2)}]^{2^{n-1}}.$$

Cet idéal vérifie les conditions de la définition III.1, donc il est essentiel.

COROLLAIRE 2: *Si* $m = p^n$, *l'idéal* $\prod_{\ell=1}^{t} s_{u_\ell}(N_{K(m)/\mathbb{Q}(m)}(\mathcal{R}(\chi^{u_\ell^*}))$ *est un idéal principal.*

DÉMONSTRATION: Si $m = 2$, le résultat est trivial, sinon on a la relation:

$$\prod_{\ell=1}^{t} s_{u_\ell}(N_{K(m)/\mathbb{Q}(m)}(\mathcal{R}(\chi^{u_\ell^*})))^m$$

$$= \prod_{\ell=1}^{t} s_{u_\ell}(N_{K(m)/\mathbb{Q}(m)}\langle\theta, \chi^{u_\ell^*}\rangle^m) \prod_{\ell=1}^{t} s_{u_\ell}$$

$$\left[\prod_{\substack{d|m \\ d\neq 1}} \left(\prod_{\substack{i=1 \\ (i,d)=1}}^{d} N_{K(m)/\mathbb{Q}(m)}(\mathfrak{U}_{i,d}(\chi^{u_\ell^*})^i)\right)\right]^{-m/d}.$$

La proposition III.4, la proposition III.5 et le corollaire 1 à la proposition III.5 montrent que le membre de droite de l'égalité est un idéal essentiel. Il suffit donc d'appliquer le lemme III.2 pour démontrer ce corollaire.

3. Congruences vérifiés par les résolvantes de Lagrange

Reprenons les notations du chapitre II. On se donne une extension galoisienne $N/\mathbb{Q}$ de groupe de Galois G, un sous-groupe H d'ordre n de G et un caractère χ de degré 1 et d'ordre m de H, à valeurs dans le corps $\mathbb{Q}(m)$. Soient K le sous-corps de G invariant par H et $\sigma_1, \ldots, \sigma_t$ un système de représentants des classes de $\mathrm{Gal}(N(m)/\mathbb{Q})$ modulo $\mathrm{Gal}(N(m)/\mathbb{Q}(m) \cap K)$ avec $\sigma_1 = 1$. On définit un $\mathbb{Q}$-homomorphisme φ de N dans le $\mathbb{Q}(m)$-espace vectoriel $W = K(m) \times \sigma_2(K(m)) \times \cdots \times \sigma_t(K(m))$ en posant

$$\varphi(\theta) = \left(\frac{\langle\theta, \chi\rangle}{\langle\theta_0, \chi\rangle}, \ldots, \sigma_t \frac{\langle\theta, \chi^{u_t^*}\rangle}{\langle\theta_0, \chi^{u_t^*}\rangle}\right).$$

Rappelons que la restriction de σ_i à $\mathbb{Q}(m)$ est notée s_{u_i}, $u_i \bmod m$.

On a vu (démonstration de la proposition II.6) qu'étant donnés $x_1, \ldots, x_t$, t éléments de $K(m)$, il existe un élément y tel que $\varphi(y) = (x_1, \sigma_2(x_2), \ldots, \sigma_t(x_t))$. On peut en particulier choisir:

$$y = \frac{1}{[N:K]} \sum_{s_i \in \mathrm{Gal}(K(m)/K)} \sum_{\ell=1}^{t} s_i(x_\ell)\langle \theta_0, x^{iu_\ell^*}\rangle.$$

DÉFINITION III.2: *On note M le $\mathbb{Z}[\zeta_m]$-réseau de W défini par*:

$$M = \mathcal{R}(\chi)^{-1} \times \sigma_2(\mathcal{R}(\chi^{u_2^*})^{-1}) \times \cdots \times \sigma_t(\mathcal{R}(\chi^{u_t^*})^{-1}).$$

PROPOSITION III.6: *On a la double inclusion* $[N:K]M \subset \varphi(O_N) \subset M$.

DÉMONSTRATION: Soit θ un élément de O_N, $\langle \theta, \chi\rangle$ est un entier algébrique. On a la relation $\langle \theta, \chi\rangle = [\langle \theta, \chi\rangle/\langle \theta_0, \chi\rangle]\langle \theta_0, \chi\rangle$ et le quotient $\langle \theta, \chi\rangle/\langle \theta_0, \chi\rangle$ appartient à $K(m)$. En élévant à la puissance m et en utilisant la décomposition en idéaux:

$$\langle \theta, \chi\rangle^m = \left(\mathcal{R}(\chi)\frac{\langle \theta, \chi\rangle}{\langle \theta_0, \chi\rangle}\right)^m \prod_{\substack{d \mid m \\ d \neq 1}} \left(\prod_{\substack{i=1 \\ (i,d)=1}}^{d} \mathfrak{U}_{i,d}(\chi)^i \right)^{m/d},$$

le produit des $\mathfrak{U}_{i,d}(\chi)^{im/d}$ n'étant pas divisible par une puissance m-ième et $\langle \theta, \chi\rangle^m$ étant entier, on en déduit que $[\langle \theta, \chi\rangle/\langle \theta_0, \chi\rangle]\mathcal{R}(\chi)$ est un idéal entier. Donc, $[\langle \theta, \chi\rangle/\langle \theta_0, \chi\rangle] \in \mathcal{R}(\chi)^{-1}$, d'où l'inclusion de droite.

Soient maintenant $x_1, \ldots, x_t$, n éléments de $K(m)$, tels que n_i appartienne à $[N:K]\mathcal{R}(\chi^{u_i^*})^{-1}$. La proposition II.4 montre que $[N:K]s_i(x_\ell)\langle \theta_0, \chi^{iu_\ell^*}\rangle$ est un entier, donc l'élément y tel que $\varphi(y) = (x_1, \sigma_\ell(x_\ell), \ldots, \sigma_\ell(x_t))$ dont on a rappelé la construction est un entier de N, d'où l'inclusion de gauche.

Chapitre IV. INVARIANTS ATTACHÉS AUX EXTENSIONS

1. Résultats généraux

Soient $N/\mathbb{Q}$ une extension galoisienne de groupe de Galois G, H un sous-groupe de G et χ un caractère de H de degré 1 et d'ordre m à valeurs dans le corps $\mathbb{Q}(m)$. On reprend les notations du chapitre II. On construit le $\mathbb{Q}$-homomorphisme d'espaces vectoriels φ de N dans $W = \bigoplus_{i=1}^{t}(\sigma_i(K(m))$; W est muni d'une structure de $\mathbb{Q}[H]$-module et φ est un homomorphisme de $\mathbb{Q}[H]$-modules.

DÉFINITION IV.1: Soit G' un sous-groupe de G contenant H tel que: quel que soit $\theta \in \operatorname{Ker} \varphi$ et quel que soit $g \in G'$ on ait $g(\theta) \in \operatorname{Ker} \varphi$. On note $\eta = \operatorname{Ind}_H^{G'}(\chi)$.

NOTATIONS: Soient $\mu_1, \ldots, \mu_\ell$ (resp. $\nu_1, \ldots, \nu_k$) un système de représentants des classes à droite de G' (resp. G) modulo H (resp. G'). Soit θ_0 un élément de N engendrant une base normale de N/K et de $N/\mathbb{Q}$.

PROPOSITION IV.1: *Les éléments* $\varphi(\mu_i^{-1}\nu_j^{-1}\theta_0)$ $(1 \leq i \leq \ell;\ 1 \leq j \leq k)$ *forment une* $\mathbb{Q}(m)$*-base de* W.

DÉMONSTRATION: Les éléments $\mu_i^{-1}\nu_j^{-1}$ forment un système de représentants des classes à gauche de G modulo H. Pour tout élément g de G il existe donc un unique couple (i, j) et un unique élément $h \in H$ tels que $g = h\mu_i^{-1}\nu_j^{-1}$. Or, l'application φ est surjective (proposition II.6) et θ_0 engendre une base normale de $N/\mathbb{Q}$. Les éléments $\varphi(h\mu_i^{-1}\nu_j^{-1}\theta_0) = \chi(h)\varphi(\mu_i^{-1}\nu_j^{-1}\theta_0)$ forment donc un système de générateurs de W comme $\mathbb{Q}$-espace vectoriel; il s'ensuit que les $\varphi(\mu_i^{-1}\nu_j^{-1}\theta_0)$ forment un système de générateurs de W comme $\mathbb{Q}(m)$-espace vectoriel, et l'égalité $\dim_{\mathbb{Q}(m)} W = [G : H]$ entraîne le résultat.

DÉFINITION IV.2: Soit $V = \bigoplus_{j=1}^{k} V_j$ un $\mathbb{Q}(\eta)$-espace vectoriel où chacun des V_j est une copie de W. On note f l'application de N dans V définie par:

$$f(\theta) = (\varphi(\nu_1^{-1}\theta), \ldots, \varphi(\nu_j^{-1}\theta), \ldots, \varphi(\nu_k^{-1}\theta)).$$

PROPOSITION IV.2: *Le noyau de* f *est un* $\mathbb{Q}[G]$*-module.*

DÉMONSTRATION: Soient θ un élément de $\operatorname{Ker} f$ et g un élément de G. Puisque $f(\theta) = 0$ on a $\varphi(\nu_j^{-1}\theta) = 0$ $(j = 1, \ldots, k)$. Comme les ν_j^{-1} forment un système de représentants des classes à gauche de G modulo G', il existe un indice $s(i, g)$ et un élément $h'(i, g)$ tels que $\nu_i^{-1}g = h'(i, g)\nu_{s(i,g)}^{-1}$. Par conséquent, $\varphi(\nu_i^{-1}g\theta) = \varphi(h'_{(i,g)}\nu_{s(i,g)}^{-1}(\theta)) = 0$. On en déduit immédiatement que $g\theta$ appartient au noyau de f.

On peut donc, par transport de structure, faire opérer G sur $f(N)$ en posant $g * f(\theta) = f(g\theta)$. Nous allons étudier cette opération dans les différents cas.

2. Application aux p-extensions galoisiennes

Dans ce paragraphe nous utiliserons les notations du chapitre I, §3. Soit $N/\mathbb{Q}$ une p-extension galoisienne de groupe de Galois G. On désigne par ψ un caractère absolument irréductible de G du type I_n (resp. D_n, M_n, H_n).

D'après le théorème I.2, il existe un sous-groupe H' de G et un caractère η de H' tel que $\psi = \mathrm{Ind}_{H'}^{G}(\eta)$ et $\mathbb{Q}(\psi) = \mathbb{Q}(\eta)$. Le quotient de H' par $\mathrm{Ker}\,\eta$ est isomorphe à I_n (resp. D_n, M_n, H_n).

Dans chacun des cas, il existe un sous-groupe H de H' et un caractère χ de degré 1 de H tels que $\eta = \mathrm{Ind}_{H}^{H'}(\chi)$. Le caractère χ est à valeurs dans $\mathbb{Q}(m)$ avec $m = p^n$. Rappelons que K (resp. N_m) est le sous-corps de N invariant par H (resp. $\mathrm{Ker}\,\eta = \mathrm{Ker}\,\chi$), et que $N_{p^{n-1}}$ est le sous-corps de N_m contenant K tel que $[N_{p^{n-1}}:K] = p^{n-1}$.

On construit les résolvantes de Lagrange relatives aux éléments θ de N et au caractère χ de H. On considère alors l'espace vectoriel W de la définition II.2 et l'application φ de N dans W de la définition II.3.

PROPOSITION IV.3: *Le* $\mathbb{Q}[H]$*-module* $\mathrm{Ker}\,\varphi$ *est invariant par* H'.

DÉMONSTRATION: Les corps N_m et K sont galoisiens sur K'. Il s'ensuit que $N_{p^{n-1}}$ est galoisien sur K'; par conséquent, l'ensemble des éléments θ de N tels que $T_{N/N_m}(\theta)$ appartient à $N_{p^{n-1}}$ est stable par H', et d'après la proposition II.7, cet ensemble est précisément $\mathrm{Ker}\,\varphi$.

Nous considérons l'application f du paragraphe précédent construite en prenant G' égal à H'.

Si ψ est du type I_n, on a $H' = H$. Si ψ est du type D_n (resp. M_n, H_n), il existe un K'-automorphisme τ de N dont la restriction à D_n (resp. M_n, H_n) est l'automorphisme $\bar{\tau}$ du §3 du chapitre I. Les représentants $\mu_1, \ldots, \mu_\ell$ de la définition IV.1 seront donc 1 et τ. On note h_1 un K-automorphisme de N dont la restriction à N_m est un générateur de $\mathrm{Gal}\,(N_m/K)$ et on pose $\zeta = \chi(h_1)$.

Puisque $\mathrm{Ker}\,\varphi$ est invariant par H' et que l'application φ est surjective, on peut faire opérer H' sur W en posant pour tout élément μ de H' et tout élément $\varphi(\theta)$ de W : $\mu * \varphi(\theta) = \varphi(\mu\theta)$.

Nous allons nous intéresser à cette opération lorsque $H'/\mathrm{Ker}\,\eta$ est isomorphe à l'un des groupes D_n, M_n, H_n.

DÉFINITION IV.3: On désigne par R_i le sous-$\mathbb{Q}(\eta)$-espace vectoriel de W engendré par

$$\varphi(\nu_i^{-1}\theta_0),.\varphi(\tau\nu_i^{-1}\theta_0),\ \zeta\varphi(\nu_i^{-1}\theta_0),\ \zeta\varphi(\tau\nu_i^{-1}\theta_0).$$

On constate aisément que ce système de générateurs est une base de R_i sur $\mathbb{Q}(\eta)$.

PROPOSITION IV.4: *Le $\mathbb{Q}(\eta)$-espace vectoriel R_i est un sous-$\mathbb{Q}[H']$-module de W.*

DÉMONSTRATION: Soit ℓ un entier. Considérons le produit d'un générateur de R_i par $(\zeta+\zeta^r)^\ell$ (pour la définition de r, cf. ch. I, §3). Pour démontrer la proposition, il suffit de vérifier qu'en faisant opérer h et τ sur cet élément, on obtient un élément de R_i. Cela résulte des identités suivantes qui sont conséquences de la proposition II.2:

$$h*(\zeta+\zeta^r)^\ell\varphi(\nu_i^{-1}\theta_0)=h*\varphi((h+h^r)^\ell\nu_i^{-1}\theta_0)=\varphi(h(h+h^r)^\ell\nu_i^{-1}\theta_0)$$
$$=(\zeta+\zeta^r)^\ell\zeta\varphi(\nu_i^{-1}\theta_0),$$
$$h*(\zeta+\zeta^r)^\ell\varphi(\tau\nu_i^{-1}\theta_0)=(\zeta+\zeta^r)^\ell\zeta\varphi(\tau\nu_i^{-1}\theta_0),$$
$$h*(\zeta+\zeta^r)^\ell\zeta\varphi(\nu_i^{-1}\theta_0)=(\zeta+\zeta^r)^{\ell+1}\zeta\varphi(\nu_i^{-1}\theta_0)-\zeta^{r+1}(\zeta+\zeta^r)^\ell\varphi(\nu_i^{-1}\theta_0),$$
$$h*(\zeta+\zeta^r)^\ell\zeta\varphi(\tau\nu_i^{-1}\theta_0)=(\zeta+\zeta^r)^{\ell+1}\zeta\varphi(\tau\nu_i^{-1}\theta_0)-\zeta^{r+1}(\zeta+\zeta^r)^\ell\varphi(\tau\nu_i^{-1}\theta_0),$$
$$\tau*(\zeta+\zeta^r)^\ell\varphi(\nu_i^{-1}\theta_0)=(\zeta+\zeta^r)^\ell\varphi(\tau\nu_i^{-1}\theta_0),$$
$$\tau*(\zeta+\zeta^r)^\ell\varphi(\tau\nu_i^{-1}\theta_0)=(\zeta+\zeta^r)^\ell\chi(\tau^2)\varphi(\nu_i^{-1}\theta_0),$$
$$\tau*(\zeta+\zeta^r)^\ell\zeta\varphi(\nu_i^{-1}\theta_0)=(\zeta+\zeta^r)^{\ell+1}\varphi(\tau\nu_i^{-1}\theta_0)-(\zeta+\zeta^r)^\ell\zeta\varphi(\tau\nu_i^{-1}\theta_0),$$
$$\tau*(\zeta+\zeta^r)^\ell\zeta\varphi(\tau\nu_i^{-1}\theta_0)$$
$$=(\zeta+\zeta^r)^{\ell+1}\chi(\tau^2)\varphi(\nu_i^{-1}\theta_0)-\chi(\tau^2)(\zeta+\zeta^r)^\ell\zeta\varphi(\nu_i^{-1}\theta_0),$$

en remarquant que $\zeta^{r+1}=\zeta\zeta^r$ appartient à $\mathbb{Q}(\eta)$.

Rappelons que $\mathbb{H}_n$ est le corps gauche défini au paragraphe 3 du chapitre I. En remarquant que $\mathbb{H}_n$ est isomorphe au quotient de $\mathbb{Q}[H_n]$ par l'idéal bilatère engendré par $(\bar{h}^{2^n}+1)$, la proposition IV.4 nous donne:

COROLLAIRE: *Si $H'/\mathrm{Ker}\,\eta$ est isomorphe à H_n, le $\mathbb{Q}[H']$-module R_i est un $\mathbb{H}_n$-module de rang* 1 *ayant pour base $\varphi(\nu_i^{-1}\theta_0)$.*

Pour interpréter la proposition IV.4 dans les cas D_n et M_n, choisissons une nouvelle base de R_i:

$$u_{i,1}=\frac{1}{(\zeta-\zeta^r)^2}[(\zeta^2+\zeta^{2r})\varphi(\nu_i^{-1}\theta_0)+(\zeta+\zeta^r)\zeta\varphi(\nu_i^{-1}\theta_0)-2\zeta^{1+r}\varphi(\tau\nu_i^{-1}\theta_0)$$
$$+(\zeta+\zeta^r)\zeta\varphi(\tau\nu_i^{-1}\theta_0)]$$
$$u_{i,2}=\frac{1}{(\zeta-\zeta^r)^2}[-(\zeta+\zeta^r)\varphi(\nu_i^{-1}\theta_0)+2\zeta\varphi(\nu_i^{-1}\theta_0)+(\zeta+\zeta^r)\varphi(\tau\nu_i^{-1}\theta_0)$$
$$-2\zeta\varphi(\tau\nu_i^{-1}\theta_0)]$$

$$u_{i,3} = \frac{1}{(\zeta - \zeta^r)^2}[\zeta^{1+r}(\zeta + \zeta^r)\varphi(\nu_i^{-1}\theta_0) - 2\zeta^{1+r}\zeta\varphi(\nu_i^{-1}\theta_0) - \zeta^{1+r}(\zeta + \zeta^r)\varphi(\tau\nu_i^{-1}\theta_0) - (\zeta^2 + \zeta^{2r})\zeta\varphi(\tau\nu_i^{-1}\theta_0)]$$

$$u_{i,4} = \frac{1}{(\zeta - \zeta^r)^2}[-2\zeta^{1+r}\varphi(\nu_i^{-1}\theta_0) + (\zeta + \zeta^r)\zeta\varphi(\nu_i^{-1}\theta_0) + 2\zeta^{1+r}\varphi(\tau\nu_i^{-1}\theta_0) - (\zeta + \zeta^r)\zeta\varphi(\tau\nu_i^{-1}\theta_0)].$$

Si on note $a_{i,j}$ la matrice carrée d'ordre 2 dont les coefficients sont nuls, sauf celui de la i-ème ligne, j-ème colonne qui vaut 1, on fait opérer $M_2(\mathbb{Q}(\eta))$ sur R_i par:

$$a_{1,1} \circ u_{i,1} = u_{i,1}; \quad a_{1,1} \circ u_{i,2} = u_{i,2}; \quad a_{1,1} \circ u_{i,3} = 0; \quad a_{1,1} \circ u_{i,4} = 0$$
$$a_{1,2} \circ u_{i,1} = 0; \quad a_{1,2} \circ u_{i,2} = 0; \quad a_{1,2} \circ u_{i,3} = u_{i,1}; \quad a_{1,2} \circ u_{i,4} = u_{i,2}$$
$$a_{1,3} \circ u_{i,1} = u_{i,3}; \quad a_{1,3} \circ u_{i,2} = u_{i,4}; \quad a_{1,3} \circ u_{i,3} = 0; \quad a_{1,3} \circ u_{i,4} = 0$$
$$a_{1,4} \circ u_{i,1} = 0; \quad a_{1,4} \circ u_{i,2} = 0; \quad a_{1,4} \circ u_{i,3} = u_{i,3}; \quad a_{1,4} \circ u_{i,4} = u_{i,4}.$$

Avec ces conventions R_i est un $M_2(\mathbb{Q}(\eta))$-module de rang 1 ayant pour base $u_{i,1} + u_{i,4} = \varphi(\nu_i^{-1}\theta_0)$. Pour tout élément h' de H', on note $\rho(h')$ l'image de h' dans le facteur simple de $\mathbb{Q}[H']$ associé à η. On constate que:

$$\rho(h) \circ (u_{i,1} + u_{i,4}) = h * (u_{i,1} + u_{i,4})$$
$$\rho(\tau) \circ (u_{i,1} + u_{i,4}) = \tau * (u_{i,1} + u_{i,4}).$$

Ces différents résultats montrent que l'opération de $\mathbb{Q}[H']$ sur W est en fait celle du facteur de $\mathbb{Q}[H']$ associé au caractère η.

Nous avons vu que si ψ est du type I_n (resp. D_n, M_n, H_n) le facteur simple de $\mathbb{Q}[G]$ associé à ψ est $M_{[G:H']}(\mathbb{Q}(\eta))$ (resp. $M_{2[G:H']}(\mathbb{Q}(\eta))$, $M_{2[G:H']}(\mathbb{Q}(\eta))$, $M_{[G:H']}(\mathbb{H}_n)$). La dimension de ce facteur simple est égale à celle de V considéré comme $\mathbb{Q}(\eta)$-espace vectoriel. Nous allons faire opérer ce facteur simple sur V. Nous en déduirons que V est égal à $f(N)$ et que l'opération de G sur $f(N)$ se fait par l'intermédiaire de l'algèbre simple associée à ψ.

Donnons-nous une base du $\mathbb{Q}(\eta)$-espace vectoriel V de la façon suivante:

(a) si ψ est du type I_n, on prend pour $\mathbb{Q}(\zeta)$-base de V les $v_{i,j}$ où $v_{i,j}$ est l'élément de V dont la composante sur V_k est nulle sauf pour $k = i$ où elle vaut $\varphi(\nu_j^{-1}\theta_0)$;

(b) si ψ est du type D_n ou M_n, on prend pour $\mathbb{Q}(\eta)$-base de V les éléments $v_{2i-\epsilon_1,2j-\epsilon_2}$ (ϵ_1, ϵ_2 valant 0 ou 1, i et j compris entre 1 et k) où $v_{2i-\epsilon_1,2j-\epsilon_2}$ est l'élément de V dont la composante sur V_k est nulle sauf

pour $k = i$ où elle vaut:

$$(v_{2i-1,2j-1})_i = u_{j,1}; \qquad (v_{2i-1,2j})_i = u_{j,2};$$
$$(v_{2i,2j-1})_i = u_{j,3}; \qquad (v_{2i,2j})_i = u_{j,4};$$

(c) si ψ est du type H_n, on prend pour base du $\mathbb{Q}(\eta)$-espace vectoriel V les éléments $v_{2i-\epsilon_1,2j-\epsilon_2}$ (ϵ_1, ϵ_2 valant 0 ou 1, $1 \leq i, j \leq k$) où $v_{2i-\epsilon_1,2j-\epsilon_2}$ est l'élément de V dont la composante sur V_k est nulle sauf pour $k = i$ où elle vaut:

$$(v_{2i-1,2j-1})_i = \varphi(\nu_j^{-1}\theta_0); \quad (v_{2i-1,2j})_i = \varphi(\tau\nu_j^{-1}\theta_0); \quad (v_{2i,2j-1})_i = \zeta\varphi(\nu_j^{-1}\theta_0);$$
$$(v_{2i,2j})_i = \zeta\varphi(\tau\nu_j^{-1}\theta_0).$$

L'opération du facteur simple de $\mathbb{Q}[G]$ associé à ψ se fait de la façon suivante:

(a) lorsque ψ est du type I_n, D_n ou M_n, on désigne par $e_{k,\ell}$ la matrice dont tous les coefficients sont nuls sauf celui qui se trouve à la k-ième ligne, ℓ-ième colonne et qui vaut 1 ($1 \leq k$, $\ell \leq [G:H']$ dans le cas I_n, $1 \leq k$, $\ell \leq 2[G:H']$ dans les deux autres cas), et on pose:

$$e_{k,\ell} \circ v_{i,j} = \delta_{\ell,i} \cdot v_{k,j}$$

où $\delta_{\ell,i}$ est le symbole de Kronecker.

(b) lorsque ψ est du type H_n, on définit $e_{k,\ell}$ comme précédemment avec $1 \leq k$, $\ell \leq [G:H']$ et on pose:

$$e_{k,\ell} \circ v_{2i-\epsilon_1,2j-\epsilon_2} = \delta_{\ell,2} v_{2k-\epsilon_1,2j-\epsilon_2}.$$

Cela suffit à définir une opération de $M_{[G:H']}(\mathbb{H}_n)$ sur V puisque l'on sait faire opérer les éléments de $\mathbb{H}_n$ sur $v_{2k-\epsilon_1,2j-\epsilon_2}$.

Soit $\rho'(g)$ l'image de g dans le facteur de $\mathbb{Q}[G]$ associé à ψ.

THÉORÈME IV.1:

(1) *Quels que soient* $g \in G$ *et* $\theta \in N$, *on a*:

$$g * f(\theta) = \rho'(g) \circ f(\theta).$$

(2) *On a l'égalité*: $V = f(N)$.

DÉMONSTRATION:

(1) Il suffit de démontrer la relation pour $\theta = \theta_0$. En effet, si $g * f(\theta_0) = \rho'(g) \circ f(\theta_0)$ on aura $g * f(g'\theta_0) = f(gg'\theta_0) = \rho'(g) \circ \rho'(g') \circ f(\theta_0) = \rho'(g) \circ [\rho'(g') * f(\theta_0)] = \rho'(g) \circ f(g'\theta_0)$. La relation sera alors démontrée

puisque tout élément θ est une combinaison linéaire à coefficients dans $\mathbb{Q}$ des $g'\theta_0$.

Considérons donc $g * f(\theta_0) = f(g\theta_0)$. Par définition de f, l'élément $f(g\theta_0)$ de V est k-uple:

$$(\varphi(\nu_1^{-1}g\theta_0), \varphi(\nu_2^{-1}g\theta_0), \ldots, \varphi(\nu_k^{-1}g\theta_0)).$$

Pour chaque élément g de G et chaque indice i, il existe un élément $h'(g,i)$ de H' et un indice $\ell(g,i)$ tels que:

$$\nu_i^{-1}g = h'(g,i)\nu_{\ell(g,i)}^{-1}, \quad \text{d'où:}$$

$$\begin{aligned} g * f(\theta_0) &= (\varphi(h'(g,1)\nu_{\ell(g,1)}^{-1}\theta_0); \ldots; \varphi(h'(g,i)\nu_{\ell(g,i)}^{-1}\theta_0); \\ &\qquad \ldots; \varphi(h'(g,k)\nu_{\ell(g,k)}^{-1}\theta_0)) \\ &= (h'(g,1) * \varphi(\nu_{\ell(g,1)}^{-1}\theta_0); \ldots; h'(g,i) * \varphi(\nu_{\ell(g,i)}^{-1}\theta_0); \\ &\qquad \ldots; h'(g,k) * \varphi(\nu_{\ell(g,k)}^{-1}\theta_0)) \\ &= (h'(g,1) \circ \varphi(\nu_{\ell(g,1)}^{-1}\theta_0); \ldots; h'(g,i) \circ \varphi(\nu_{\ell(g,i)}^{-1}\theta_0); \\ &\qquad \ldots; h'(g,k) \circ \varphi(\nu_{\ell(g,k)}^{-1}\theta_0)). \end{aligned}$$

La construction de la représentation induite donnée au paragraphe 2 du premier chapitre montre que l'expression ci-dessus est égale à $\rho'(g) \circ f(\theta_0)$.

(2) Puisque le facteur simple associé à ψ est formé des combinaisons linéaires à coefficients dans $\mathbb{Q}$ des éléments $\rho'(g)$, on en déduit immédiatement l'égalité $V = f(N)$.

3. Définition de l'invariant associé à un caractère absolument irréductible ψ

Dans chacun des cas précédents, soient A_ψ le facteur simple de $\mathbb{Q}[G]$ associé à ψ et i l'injection de A_ψ dans $\mathbb{Q}[G]$. Le choix de l'élément θ_0 du chapitre II définit un $\mathbb{Q}[G]$-isomorphisme entre $\mathbb{Q}[G]$ et N. On a donc une suite de $\mathbb{Q}[G]$-homomorphismes:

$$A_\psi \xrightarrow{i} \mathbb{Q}[G] \to N \xrightarrow{f} V$$

dont le composé est un isomorphisme de A_ψ-modules. Si $\mathcal{O}$ est un ordre maximal de $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$, l'image réciproque de $\mathcal{O}O_N$ est un idéal fractionnaire $I_\psi(N)$ de l'ordre maximal $\mathcal{O}_\psi = i(A_\psi) \cap \mathcal{O}$. Si A_ψ est de dimension n^2 sur son centre C_ψ, on aura, d'après la

proposition I.1:

$$N_{\mathrm{red}}(I_\psi(N))^n = \chi_{O_{C_\psi}}(\mathcal{O}_\psi, I_\psi(N)) = \chi_{O_{C_\psi}}(\mathcal{O}_\psi f(\mathbb{Z}[G]\theta_0), \mathcal{O}_\psi f(O_N)).$$

DÉFINITION IV.4: L'idéal $\chi_{O_{C_\psi}}(\mathcal{O}_\psi f(\mathbb{Z}[G]\theta_0), \mathcal{O}_\psi f(O_N))$ est l'invariant de l'extension $N/\mathbb{Q}$ associé au caractère ψ.

Chapitre V. CALCUL DES INVARIANTS

Nous démontrons dans ce chapitre le théorème énoncé dans l'introduction.

Nous le rappelons ci-dessous:

THÉORÈME V.1: *Soit $N/\mathbb{Q}$ une extension galoisienne dont le groupe de Galois G est un p-groupe, et $\mathcal{O}$ un ordre maximal de $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$. Le $\mathcal{O}$-module $\mathcal{O}O_N$ est stablement libre.*

REMARQUE: On vérifie aisément que ce résultat est indépendant de l'ordre maximal choisi contenant $\mathbb{Z}[G]$ ($\mathcal{O}_1$ et $\mathcal{O}_2$ étant deux tels ordres, on sait que $\mathcal{O}_1O_N$ et $\mathcal{O}_2O_N$ coïncident pour toutes les places $\mathfrak{P}$ du centre premières à p).

Soient ψ un caractère absolument irréductible de G, et A_ψ le facteur simple de $\mathbb{Q}[G]$ associé à ψ. On désigne par C_ψ le centre de A_ψ. Le caractère ψ est induit par un caractère χ de degré 1 d'un sous-groupe H de G. On peut donc faire la construction du chapitre précédent. On a vu que le théorème résulterait du calcul de:

$$\chi_{O_{C_\psi}}(\mathcal{O}_\psi f(\mathbb{Z}[G]\theta_0), \mathcal{O}_\psi f(O_N)).$$

Soient G un p-groupe et χ un caractère de degré 1 et d'ordre $m = p^n$ de H. Si $m = 2$, le centre de l'algèbre A_ψ est $\mathbb{Q}$. Les normes réduites des idéaux de A_ψ sont donc principales. Nous supposerons par conséquent dans la suite de ce paragraphe m impair ou $m \equiv 0 \pmod 4$.

Reprenons les notations du chapitre précédent. Le lemme suivant résulte immédiatement des définitions du chapitre IV, §2.

LEMME V.1: *On a les relations*:

$$e_{11} \circ V = V_1 = W \qquad \text{dans les cas } I_n \text{ et } H_n$$
$$(e_{11} + e_{22}) \circ V = V_1 = W \qquad \text{dans les cas } D_n \text{ et } M_n.$$

LEMME V.2: *Le $\mathbb{Z}[\zeta_m]$-module M est un module libre.*

DÉMONSTRATION: Le $\mathbb{Z}[\zeta_m]$-module M a été défini au chapitre III, §3:

$$M = \bigoplus_{i=1}^{t} \sigma_i(\mathcal{R}(\chi^{u_i^*})^{-1}).$$

Considérons également le $\mathbb{Z}[\zeta_m]$-module $\bigoplus_{i=1}^{t} O_{\sigma_i(K(m))}$ et calculons l'invariant relatif de ces deux réseaux de W:

$$\chi_{\mathbb{Z}[\zeta_m]}\left(\bigoplus_{i=1}^{t} O_{\sigma_i(K(m))}, \bigoplus_{i=1}^{t} \sigma_i(\mathcal{R}(\chi^{u_i^*})^{-1}\right) = \prod_{i=1}^{t} \chi_{\mathbb{Z}[\zeta_m]}(O_{\sigma_i(K(m))}, \sigma_i(\mathcal{R}(\chi^{u_i^*})^{-1}))$$

ce qui vaut d'après les résultats bien connus sur les invariants relatifs ([7])

$$\prod_{i=1}^{t} N_{\sigma_i(K(m))/\mathbb{Q}(m)}(\sigma_i(\mathcal{R}(\chi^{u_i^*})^{-1})).$$

D'après le lemme III.5, cette expression est égale à:

$$\prod_{i=1}^{t} s_{u_i}(N_{K(m)/\mathbb{Q}(m)}(\mathcal{R}(\chi^{u_i^*})^{-1})),$$

et le corollaire 2 à la proposition III.5 montre que cet idéal est principal. On peut donc affirmer que M est $\mathbb{Z}[\zeta_m]$-libre si et seulement si $\bigoplus_{i=1}^{t} O_{\sigma_i(K(m))}$ l'est.

Soit L un $O_{K\cap\mathbb{Q}(m)}$-réseau libre de K. On note L' le $\mathbb{Z}[\zeta_m]$-réseau de $K(m)$ engendré par L. On désigne par L'_i le réseau $\sigma_i(L')$. Soit $\mathcal{U}$ un idéal de $O_{K\cap\mathbb{Q}(m)}$ tel que $cl(\mathcal{U}) = cl(O_K)$. On a évidemment $cl(\sigma_i\mathcal{U}) = cl(O_{\sigma_i(K)})$ et $\prod_{i=1}^{t} cl(\sigma_i\mathcal{U})$ est la classe principale puisque engendrée par $N_{K\cap\mathbb{Q}(m)/\mathbb{Q}}(\mathcal{U})$. Si on note Δ_i le discriminant relativement à la trace dans $K/\mathbb{Q}(m)\cap K$ et Δ'_i le discriminant relativement à la trace dans $\sigma_i(K(m))/\mathbb{Q}(m)$, il existe un entier $e(i)$ tel que:

$$\frac{\Delta'_i(O_{\sigma_i(K(m))})}{\Delta'_i(L'_i)} = \frac{\Delta_i(O_{\sigma_i(K)})}{\Delta_i(L)}(1-\zeta_m)^{e(i)}.$$

Ceci nous montre que la classe de $O_{\sigma_i(K(m))}$ comme $\mathbb{Z}[\zeta_m]$ est celle de $\sigma_i\mathcal{U}\mathbb{Z}[\zeta_m]$. On en déduit immédiatement que $\bigoplus_{i=1}^{t} O_{\sigma_i(K(m))}$ est un $\mathbb{Z}[\zeta_m]$-module libre, d'où le lemme.

COROLLAIRE: *$\varphi(O_N)$ est un $\mathbb{Z}[\zeta_m]$-module libre.*

DÉMONSTRATION: On a vu dans la proposition III.6 la double inclusion $[N:K]M \subset \varphi(O_N) \subset M$. Comme $[N:K]$ est une puissance de p et que l'unique idéal premier au-dessus de p dans $\mathbb{Z}[\zeta_m]$ est principal, M et $\varphi(O_N)$ sont isomorphes.

Démonstration du théorème

Soient $e_{k,\ell}$ les matrices définies au paragraphe 2 du chapitre IV. La propositon I.3 montre que l'on peut choisir $\mathcal{O}_\psi$ de telle sorte qu'il contienne les $e_{k,\ell}$. Supposons que A_ψ soit une algèbre de matrices de dimension b^2 sur un corps gauche de centre C_ψ. La proposition I.2 nous permet d'écrire:
si ψ est du type I_n ou H_n:

$$\chi_{O_{C_\psi}}(\mathcal{O}_\psi f(\mathbb{Z}[G]\theta_0), \mathcal{O}_\psi f(O_N)) = \chi_{O_{C_\psi}}(e_{11} \circ \mathcal{O}_\psi f(\mathbb{Z}[G]\theta_0, e_{11} \circ \mathcal{O}_\psi f(O_N))^b$$

si ψ est du type D_n ou M_n:

$$\chi_{O_{C_\psi}}(\mathcal{O}_\psi f(\mathbb{Z}[G]\theta_0), \mathcal{O}_\psi f(O_N)) = \chi_{O_{C_\psi}}((e_{11}+e_{22}) \circ \mathcal{O}_\psi f(\mathbb{Z}[G]\theta_0), (e_{11}+e_{22}) \circ \mathcal{O}_\psi f(O_N)^{b/2}.$$

Considérons un idéal premier (ℓ) de $\mathbb{Z}$ différent de (p). On a:

$$\mathbb{Z}_\ell[G] \simeq \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{O}.$$

On en déduit pour la valuation $v_{\mathfrak{L}}$ associée à une place $\mathfrak{L}$ de C_ψ au-dessus de (ℓ):
si ψ est du type I_n, H_n:

$$v_{\mathfrak{L}}(\chi_{O_{C_\psi}}(e_{11} \circ \mathcal{O}_\psi f(\mathbb{Z}[G]\theta_0), e_{11} \circ \mathcal{O}_\psi f(O_N))) = v_{\mathfrak{L}}(\chi_{O_{C_\psi}}(e_{11} \circ f(\mathbb{Z}[G]\theta_0), e_{11} \circ f(O_N))$$

ce qui d'après le lemme 1 est égal à $v_{\mathfrak{L}}(\chi_{O_{C_\psi}}(\varphi(\mathbb{Z}[G]\theta_0), \varphi(O_N))$.
Si ψ est du type D_n ou M_n

$$v_{\mathfrak{L}}(\chi_{O_{C_\psi}}((e_{11}+e_{22}) \circ \mathcal{O}_\psi f(\mathbb{Z}[G]\theta_0), (e_{11}+e_{22}) \circ \mathcal{O}_\psi f(O_N))) = v_{\mathfrak{L}}(\chi_{O_{C_\psi}}((e_{11}+e_{22}) \circ f(\mathbb{Z}[G]\theta_0), (e_{11}+e_{22}) \circ f(O_N)))$$

ce qui d'après le lemme 1 vaut:

$$v_{\mathfrak{L}}(x_{O_{C_\psi}}(\varphi(\mathbb{Z}[G]\theta_0), \varphi(O_N))).$$

Si ψ est du type I_n, $O_{C_\psi} = \mathbb{Z}[\zeta_m]$. Or, $\varphi(\mathbb{Z}[G]\theta_0)$ est un module libre. Le théorème résulte dans ce cas du lemme 2 et des propositions I.4 et I.5.

Dans les cas D_n, M_n, H_n, l'idéal:

$$\chi_{\mathbb{Z}[\chi_m]}(\varphi(\mathbb{Z}[G]\theta_0), \varphi(O_N))$$

est également principal.

Ceci nous montre que $\chi_{O_{C\psi}}(\varphi(\mathbb{Z}[G]\theta_0, \varphi(O_N))$ est principal. On peut donc appliquer la proposition I.5 et le théorème est démontré.

BIBLIOGRAPHIE

[1] M. AUSLANDER and O. GOLDMAN: Maximal orders. *Trans. Amer. Math. Soc. 97* (1960) 1–24.

[2] A. CHATELET: Idéaux principaux dans les corps circulaires. *Colloque du C.N.R.S., algébre et théorie des nombres*, Paris (1949) 103–106.

[3] C. CURTIS and I. REINER: *Representation theory of finite groups and associative algebras.* Interscience Publishers (1962).

[4] J.-M. FONTAINE: Sur la décomposition des algèbres de groupes. *Ann. Sc. de l'E.N.S., 4e série, t. 4* (1971) 121–180.

[5] A. FRÖHLICH: Arithmetic and Galois Module Structure for tame extensions (à paraître).

[6] H. HASSE: *Uber die Klassenzahl abelsher Zahlkörper.* Berlin, Akademie Verlag (1952).

[7] J.-P. SERRE: *Corps locaux*, (Hermann, 1968).

[8] R.-G. SWAN: Induced representations and projective modules. *Ann. of Math. 71* (1960) 552–578.

(Oblatum 14–IV–1976)

Laboratoire de Mathématiques
et d'Informatique dépendant de
l'Université de Bordeaux I
associé au C.N.R.S.