SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

JEAN-JACQUES PAYAN

# Sur le théorème des indices de Brauer-Walter. Application à l'existence d'unités de Minkowski

*Séminaire de théorie des nombres de Grenoble*, tome 5 (1975-1977), exp. n° 2, p. 1-18

<http://www.numdam.org/item?id=STNG_1975-1977__5__A2_0>

Séminaire de Théorie des Nombres
22 avril et 10 juin 1976 et 24 mars 1977
Grenoble



# SUR LE THEOREME DES INDICES DE BRAUER-WALTER. APPLICATION A L'EXISTENCE D'UNITES DE MINKOWSKI.

par

Jean Jacques PAYAN

## I. NOTATIONS ET RAPPELS.

Dans tout ce qui suit, on note $G$ un groupe fini et pour tout sous-groupe $H$ de $G$, on note $1_H^G$ le caractère induit à $G$ par le caractère principal de $H$, $|H|$ l'ordre de $H$ et $\tilde{H}$ la somme des éléments de $H$, $\tilde{H} \in \mathbb{Z}[G]$.

Dans un travail très connu, R. Brauer [1] montre que tout caractère rationnel sur $G$ est combinaison linéaire rationnelle des $1_H^G$ pour $H$ parcourant un système de représentants des classes de conjugaison dans $G$ des sous-groupes cycliques. R. Brauer ayant en vue des résultats concernant les fonctions $\zeta$ prouve que si $H$ est un sous-groupe de $G$ alors

$$1_H^G = \sum_{H'} \lambda_{H'} 1_{H'}^G \tag{1}$$

où $H'$ parcourt l'ensemble des sous-groupes cycliques de $G$ et où $\lambda_{H'} = \frac{1}{[H:H']} \sum_{H''} \mu([H'':H'])$, $H''$ parcourant l'ensemble des sous-groupes, cycliques de $H$ contenant $H'$ et $\mu$ désignant la fonction de Möbius.

On fixe pour la suite une relation de dépendance $\mathbb{Z}$-linéaire entre les $1_H^G$ que l'on écrit

$$\sum_H a_H 1_H^G = 0 \ . \tag{2}$$

Si $G$ possède un élément $\gamma$ d'ordre $2$, on posera $r_1(H)$ (resp. $2r_2(H)$) le nombre de conjugués de $H$ qui contiennent (resp. qui ne contiennent pas) $\gamma$. $r_1(H) + 2r_2(H)$ est évidemment égal à $[G:H]$.

Remarque I.1. (Brauer-Walter) - Avec les notations précédentes $\sum_H a_H = 0$, $\sum_H a_H[G:H] = 0$ et $\sum_H a_H r_1(H) = 0$. Pour s'en convaincre il suffit de prendre la valeur du caractère $\sum_H a_H 1_H^G$ en $e$ élément neutre de $G$, en $\gamma$ et en $\frac{e-\gamma}{2}$.

L'objet de ce travail étant l'étude de la structure du groupe des unités d'une extension galoisienne, on suppose que $G$ est le groupe de Galois d'une extension $K/\mathbb{Q}$. Pour tout sous-groupe $H$ de $G$, on note $K^H$ l'extension intermédiaire fixe par $H$. On note $U_H$ (resp. $V_H$) le groupe des unités (resp. des racines de l'unité) de $K^H$ et on pose $E_H = U_H/V_H$. Par commodité, on notera $U,V,E$ les groupes correspondants de $K$. On notera encore $n(H) = [G:H] = [K^H:\mathbb{Q}]$, $w(H)$ = cardinal de $V_H$, $R(H)$ le régulateur de $K^H$ et $h(H)$ le nombre de classes d'idéaux de $K^H$.

Pour tout sous-groupe $H$ de $G$, $E_H V/V$ est un sous-$\mathbb{Z}$-module d'indice fini de $E^H$, (voir N. Moser [4], pour une étude plus précise), on appellera indice de Hasse de l'extension $K/K^H$, l'indice de $E_H V/V$ dans $E^H$.

DEFINITION I.1. - On appellera invariant de Hasse associé à la relation (2) le produit

$$\prod_H [E^H : E_H V/V]^{a_H}.$$

Pour tout $\mathbb{Z}[G]$-module $M$ et tout sous-groupe $H$ de $G$, on note $M^H$ le sous-$\mathbb{Z}$-module de $M$ formé des éléments de $M$ fixes par l'action des éléments de $H$.

La première étape du travail de Brauer aboutit à la formule suivante

associée à la relation de dépendance $\mathbb{Z}$-linéaire (2)

$$(3) \qquad \prod_H \left(\frac{R(H)h(H)}{w(H)}\right)^{a_H} = 1$$

formule mise en évidence et indépendamment par S.N. Kuroda [3]

$w(H)$ s'écrit évidemment comme le produit de ses p-composantes $w_p(H)$ ordre du groupe des racines de l'unité d'ordre une puissance de $p$ contenue dans $K^H$. Brauer a prouvé que $\prod_H w(H)^{a_H} = \prod_H w_2(H)^{a_H}$ et a donné une formule explicite de cet invariant du corps $K$. La démonstration de C.D. Walter de l'égalité $\prod_H w_p(H)^{a_H} = 1$ si $p$ est différent de $2$ montre bien que la clef est la propriété du groupe de Galois de $\mathbb{Q}(V_p)/\mathbb{Q}$ d'être cyclique pour $p$ impair. On voit en outre facilement que si $K$ ne contient pas les racines primitives huitièmes de l'unité alors $\prod_H w_2(H)^{a_H} = 1$.

## II. RESEAUX, MODULES ET THEOREME DES INDICES.

A tout $\mathbb{Q}[G]$-module $M$ de type fini est associé de manière naturelle un caractère rationnel de $G$, à savoir celui qui est défini à partir de la représentation multiplication des éléments de $M$ par ceux de $G$.

Soient alors $M$ et $N$ deux $\mathbb{Z}[G]$-modules de type fini et sans $\mathbb{Z}$-torsion, posons $M' = \mathbb{Q} \otimes_{\mathbb{Z}} M$ et $N' = \mathbb{Q} \otimes_{\mathbb{Z}} N$, on appellera caractère associé à $M$ (resp. $N$) le caractère du $\mathbb{Q}[G]$-module $M'$ (resp. $N'$).

Remarque II.1. - Pour que $M$ et $N$ aient le même caractère il faut et il suffit que $M'$ et $N'$ soient $\mathbb{Q}[G]$-isomorphes. Pour que $M$ et $N$ aient le même caractère il faut et il suffit qu'il existe un sous-$\mathbb{Z}[G]$-module de $M$ d'indice fini et isomorphe à $N$.

Soient alors $A$ un anneau principal de corps des fractions $k$, $L$ un $A[G]$-module de type fini sans A-torsion plongé dans $L' = k \otimes_A L$.

Remarque II.2. (C.D. Walter et d'autres) - Soit $e$ un idempotent de $\mathbb{Q}[G]$, alors $eL' \cap L$ est un réseau de $eL'$. Si $H$ est un sous-groupe de $G$, $L^H$ est un réseau de $L'^H$. On passe de la première assertion à la seconde à l'aide de l'idempotent $\frac{\tilde{H}}{\overline{H}}$. On montre que la première est vraie à l'aide d'une k-base de $eL'$.

Supposons que $A$ principal soit un sous-anneau de $\mathbb{Q}$ et donnons-nous un $\mathbb{Q}$-espace vectoriel $X$ de dimension finie et deux A-réseaux $M$ et $N$ de $X$. On appelle indice de $N$ dans $M$ et on note $[M:N]$ la valeur absolue du déterminant d'une matrice de passage d'une A-base de $N$ à une A-base de $M$. Cet indice est un nombre rationnel positif défini au produit près par une unité positive de $A$.

Remarque II.3. - Si $A = \mathbb{Z}$ et $M \supset N$, on retrouve la définition classique de l'indice.

Remarque II.4. - L'indice ainsi défini est lié de manière très simple à la fonction caractéristique des deux réseaux sur un anneau de Didekind (voir par exemple J.P. Serre [7] chapitre III, § 1). Le lecteur intéressé est invité à préciser ce lien, il pourra également le comparer à l'indice-idéal défini par A. Fröhlich.

Enonçons alors le

THEOREME II.1. (C.D. Walter) - *Soient $M$ et $N$ deux $\mathbb{Z}[G]$-modules de type fini sans $\mathbb{Z}$-torsion et $\mathbb{Z}[G]$-isomorphes alors*

$$\prod_H [M^H : N^H]^{a_H} = 1 .$$

Démonstration : Supposons d'abord que $M$ et $N$ sont deux réseaux de $X$. Un $\mathbb{Z}[G]$-isomorphisme de $M$ sur $N$ se prolonge en un $\mathbb{Q}[G]$-automorphisme $\alpha$ de $X$.

Soit $Y$ un $\mathbb{Q}[G]$-module, on définit grâce à $\alpha$ un $\mathbb{Q}[G]$-automorphisme $\alpha(Y)$ de $\mathrm{Hom}_{\mathbb{Q}[G]}(Y,X)$ comme suit : à $f$ de $\mathrm{Hom}_{\mathbb{Q}[G]}(Y,X)$ on fait correspondre $\alpha(Y)(f) = \alpha \circ f$ . Soient alors $Y'$ , $\mathbb{Q}[G]$-isomorphe à $Y$ et $\rho : Y \to Y'$ réalisant cet isomorphisme. Notons $\beta$ l'application de $\mathrm{Hom}_{\mathbb{Q}[G]}[Y',X]$ dans $\mathrm{Hom}_{\mathbb{Q}[G]}[Y,X]$ définie par $\beta(f') = f' \circ \rho$ . On vérifie facilement que $\beta$ est un $\mathbb{Q}$-isomorphisme et l'égalité $\alpha(Y) \circ \beta = \beta \circ \alpha(Y')$ il en résulte $\det \alpha(Y) = \det \alpha(Y') \neq 0$ . En utilisant la remarque II.1 on voit que $\det \alpha(Y)$ permet de définir une application $\det \alpha(\chi)$ sur l'ensemble des caractères de représentations (les "vrais" caractères) à valeurs dans $\mathbb{Q}^*$ . De l'égalité $\mathrm{Hom}_{\mathbb{Q}[G]}(Y_1 \oplus Y_2 , X) = \mathrm{Hom}_{\mathbb{Q}[G]}(Y_1,X) \oplus \mathrm{Hom}_{\mathbb{Q}[G]}(Y_2,X)$ résulte $\det \alpha(\chi_1 + \chi_2) = \det \alpha(\chi_1).\det \alpha(\chi_2)$ , on a donc en étendant par linéarité, le domaine de définition, en remplaçant les déterminants par leurs valeurs absolues pour pouvoir prendre des puissances fractionnaires, un homomorphisme du groupe additif des caractères virtuels rationnels dans $\mathbb{Q}_+^*$ . Il en résulte en particulier

$$\det \alpha(\sum_H a_H 1_H^G) = \prod_H |\det \alpha(1_H^G)|^{a_H} = 1 .$$

Prenons maintenant pour $Y$ le module $\mathbb{Q}[G]e$ où $e$ est un idempotent de $\mathbb{Q}[G]$ et $\chi$ le caractère associé. L'application $\varphi$ qui à $f \in \mathrm{Hom}_{\mathbb{Q}[G]}(Y,X)$ associe $\varphi(f) = f(e)$ envoie $\mathrm{Hom}_{\mathbb{Q}[G]}(Y,X)$ dans $eX$ puisque $f(e) = ef(e)$ . Il est clair que $\varphi$ est un $\mathbb{Q}$-homomorphisme. Soit alors $\psi$ l'application qui à $ex$ de $eX$ associe l'application $f$ de $Y$ dans $X$ définie par $f(y) = yex$ , $f$ est évidemment $\mathbb{Q}$-linéaire, montrons que c'est un $\mathbb{Q}[G]$-homomorphisme de $Y$ dans $X$ . Si $\lambda \in \mathbb{Q}[G]$ et $y \in \mathbb{Q}[G]e$ on voit que $f(\lambda y) = \lambda yex = \lambda f(y)$ . Soit alors $f$ de $\mathrm{Hom}_{\mathbb{Q}[G]}(Y,X)$ , $(\psi \circ \varphi)(f)$ est un élément de $\mathrm{Hom}_{\mathbb{Q}[G]}(Y,X)$ , soit $y$ de $Y$

$$(\psi \circ \varphi)(f)(y) = (\psi'(f(e)))(y) = (\psi(ef(e)))(y)$$

en utilisant la définition de $\varphi$ , utilisons celle de $\psi$ , on obtient

$$\psi(ef(e))(y) = yef(e) = f(ye) = f(y)$$

puisque $y \in \mathbb{Q}[G]e$ . Ce qui se traduit par $\psi \circ \varphi = \mathrm{Id}_{\mathrm{Hom}_{\mathbb{Q}[G]}(Y,X)}$ et

$\varphi$ est inversible, c'est un $\mathbb{Q}$-isomorphisme de $\mathrm{Hom}_{\mathbb{Q}[G]}(Y,X)$ sur $eX$ .

Notons alors $\alpha_e$ la restriction de $\alpha$ à $eX$ , on voit sans peine que

$$\varphi \circ \alpha(Y) = \alpha_e \circ \varphi$$

d'où résulte

$$\det \alpha(\chi) = \det \alpha_e \ .$$

Interprétons alors $\det(1_H^G)$ . $1_H^G$ est le caractère associé à $\mathbb{Q}[G]e$ avec $e = \frac{\bar{H}}{|H|}$ , on a donc $\det \alpha(1_H^G) = \det(\alpha_e)$ où $\alpha_e$ est la restriction à $\frac{\tilde{H}}{|H|} X$ de $\alpha$ . On sait, Remarque II.2, que $M^H$ est un réseau de $eX$ , son image par $\alpha_e$ est égale à $N^H$ et $\det(\alpha_e)$ est donc égal au signe près à $[M^H : N^H]$ d'où $[M^H : N^H] = |\det(\alpha_e)| = |\det(1_H^G)|$ et l'énoncé du théorème en découle par substitution.

Reste à voir ce qui se passe si $M$ et $N$ ne sont pas supposés être des réseaux d'un même $X$ . On prend alors $X = \mathbb{Q} \otimes M$ et on fait le calcul avec un sous-réseau $N'$ de $X$ , $\mathbb{Z}[G]$-isomorphe à $N$ . Le résultat établi montre que le produit $\prod_H [M^H : N'^H]^{a_H}$ ne dépend par de l'image isomorphe de $N$ choisie.

En fait, nous avons à portée de la main un résultat plus fort. Rappelons (cf. [5]) que deux $\mathbb{Z}[G]$-modules de type fini $M$ et $N$ sont dits dans le même genre s'ils ont le même caractère et si, en notant $\mathbb{Z}_{(p)}$ le localisé en $p$ premier de $\mathbb{Z}$ , les $\mathbb{Z}_{(p)}[G]$-modules $\mathbb{Z}_{(p)} \otimes M$ et $\mathbb{Z}_{(p)} \otimes N$ sont isomorphes pour tout $p$ .

THEOREME II.2. - <u>Soient</u> $M$ <u>et</u> $N$ <u>deux</u> $\mathbb{Z}[G]$<u>-modules de type fini, sans torsion et dans le même genre alors</u>

$$\prod_H [M^H : N^H]^{a_H} = 1 \ .$$

Démonstration : Remarquons d'abord que toute $\mathbb{Z}$-base de $M$ (resp. $M^H$) est une $\mathbb{Z}_{(p)}$-base de $\mathbb{Z}_{(p)} \otimes M$ (resp. $\mathbb{Z}_{(p)} \otimes M^H$) donc que $[M^H : N^H]$ est un représentant de $[\mathbb{Z}_{(p)} \otimes M^H : \mathbb{Z}_{(p)} \otimes N^H]$ . En reprenant ensuite la démonstration du théorème II.1 de Walter, on voit qu'elle s'applique sans difficulté à des $\mathbb{Z}_{(p)}[G]$-modules à condition d'utiliser la définition de l'indice donnée après la remarque II.2. On en déduit que $\prod_H [\mathbb{Z}_{(p)} \otimes M^H : \mathbb{Z}_{(p)} \otimes N^H]^{a_H}$ est une unité positive de $\mathbb{Z}_{(p)}$ . Ce produit étant égal au produit près par une unité positive de $\mathbb{Z}_{(p)}$ à $\prod_H [M^H : N^H]^{a_H}$ on voit que ce dernier produit est positif et est une unité pour tout $p$ , il est donc égal à $1$ .

## III. RETOUR SUR LA FORMULE DES NOMBRES DE CLASSES, INVARIANTS DE BRAUER ET DE WALTER.

Si $K/\mathbb{Q}$ , de groupe de Galois $G$ , est non réelle, $\gamma$ désignera la restriction à $K$ de la conjugaison complexe.

DEFINITION III.1. - On dira qu'une unité $\varepsilon$ de $K$ est une unité de Minkowski au sens large (resp. restreint) si et seulement si le sous-$\mathbb{Z}[G]$-module de $E$ engendré par $\varepsilon V$ est d'indice fini (resp. égal à $E$).

Remarque III.1. - $E$ est un $\mathbb{Z}[G]$-module de type fini, sans $\mathbb{Z}$-torsion de caractère $1_1^G - 1_G^G$ (resp. $1_C^G - 1_G^G$) si $K/\mathbb{Q}$ réelle (resp. si $K/\mathbb{Q}$ non réelle). Ce n'est qu'une manière de traduire le théorème de Minkowski concernant l'existence d'unités de Minkowski au sens large dans tout corps de nombres galoisien.

On sait même qu'il existe des unités réelles de Minkowski au sens large. Le $\mathbb{Z}[G]$-module $E$ admet alors un sous-$\mathbb{Z}[G]$-module d'indice fini $\mathbb{Z}[G]$-isomorphe à

$$\mathfrak{L} = \mathbb{Z}[G]/\mathbb{Z}\tilde{G} \quad \text{si} \quad K/\mathbb{Q} \quad \text{rélle}$$

$$\mathfrak{L} = \mathbb{Z}[G]\tilde{C}/\mathbb{Z}\tilde{G} \quad \text{si} \quad K/\mathbb{Q} \quad \text{non réelle.}$$

C.D. Walter a introduit le module dual de $\mathfrak{L}$ à savoir $\mathfrak{L}^*$ défini à l'aide de la suite exacte

$$0 \longrightarrow \mathfrak{L}^* \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0 \quad \text{si} \quad K/Q \quad \text{réelle}$$

$$0 \longrightarrow \mathfrak{L}^* \longrightarrow \mathbb{Z}[G]\tilde{C} \longrightarrow \mathbb{Z} \longrightarrow 0 \quad \text{sinon}$$

l'homomorphisme sur $\mathbb{Z}$ consistant à associer à un élément de $\mathbb{Z}[G]$ (resp. $\mathbb{Z}[G]\tilde{C}$) la somme (resp. demi-somme) de ses coefficients.

$\mathfrak{L}^*$ est l'idéal d'augmentation $I_G$ de $\mathbb{Z}[G]$ dans le cas réel, dans le cas imaginaire on a facilement $\mathfrak{L}^* = I_G\tilde{C}$ .

DEFINITION III.2. - <u>On appelle invariant de Brauer (resp. de Walter) associé à la relation (2) le produit</u> $\prod_H [E^H : \mathfrak{L}^H]^{a_H}$ (resp. $\prod_H [E^H : \mathfrak{L}^{*H}]^{a_H}$) .

<u>Remarque III.2.</u> (Brauer) - Pour que $K/\mathbb{Q}$ admette une unité de Minkowski au sens restreint, réelle, il faut que l'Invariant de Brauer soit égal à 1 .

Notons dans ce qui suit $\bar{\eta}$ l'image d'un $\eta$ de $U^H$ par la projection canonique sur $U^H/V^H$ et $\hat{\alpha}$ l'image d'un $\alpha$ de $\mathbb{Z}[G]$ par la projection canonique sur $\mathbb{Z}[G]/\mathbb{Z}\tilde{G}$ , on définit alors les applications

$$\lambda : E \longrightarrow \mathbb{C} \otimes_{\mathbb{Z}} \mathfrak{L}$$

$$\lambda^* : E \longrightarrow \mathbb{C} \otimes_{\mathbb{Z}} \mathfrak{L}^*$$

par

$$\lambda(\bar{\epsilon}) = \sum_{\sigma \in G} (\log|\sigma^{-1}\epsilon|)\hat{\sigma}$$

$$\lambda^*(\bar{\epsilon}) = \sum_{\sigma \in G} (\log|\sigma^{-1}\epsilon|)\sigma$$

la valeur absolue étant celle qui est associée au plongement de $K$ dans $\mathbb{C}$ pour lequel le sous-corps réel maximal de $K$ est l'extension intermédiaire de $K/\mathbb{Q}$ qui appartient à $C$ .

Remarque III.3. (C.D. Walter) - $\lambda$ et $\lambda^*$ sont des $\mathbb{Z}[G]$-homomorphismes injectifs. On le vérifie en utilisant le théorème de Dirichlet, celui-ci indique que $E$ et ses images par $\lambda$ et $\lambda^*$ ont le même $\mathbb{Z}$-rang.

Pour tout sous-groupe $H$ de $G$ , on notera dans la suite $\delta(H)$ l'invariant de $K^H$ défini comme suit :

- si tous les conjugués de $K^H$ sont imaginaires $\delta(H) = 2$
- si un conjugué au moins de $K^H$ est réel, $\delta(H) = 1$ .

Il est clair que $\delta(H) = 1$ équivaut à l'existence d'un $\sigma$ dans $G$ tel que $\sigma^{-1}\gamma\sigma \in H$ , cette dernière condition signifiant que $H\sigma_o C$ est une classe à gauche modulo $C$ .

La propriété suivante précise les relations entre régulateurs et unités :

PROPRIETE III.1. (C.D. Walter) - Soit $H$ un sous-groupe de $G$ . Alors

$$[\mathfrak{L}^H : \lambda(\overline{U^H})] = [G:H]2^{-r_2(H)}R(H)$$

$$[\mathfrak{L}^{*H} : \lambda^*(\overline{U^H})] = (H)2^{-r_2(H)}R(H) .$$

Démonstration : On fixe un $\sigma_o$ dans $G$ tel que $H\sigma_o C = H\sigma_o$ si $\delta(H) = 1$ . Dans tous les cas on a $\delta(H) = \dfrac{|H\sigma_o C|}{|H|}$ .

Remarquons d'abord que les éléments

$$\tilde{H}\sigma_i\tilde{C} - \frac{|H\sigma C|}{|H\sigma_o C|}\tilde{H}\sigma_o\tilde{C}$$

où $\sigma_i$ parcourt un système complet $S$ de représentants des doubles classes $H\backslash G/C$ ($H\sigma_o C$ étant représentée par $\sigma_o$) est une $\mathbb{Z}$-base de $\mathfrak{L}^{*H}$. Soit alors $\epsilon \in U^H$, $\lambda^*(\bar{\epsilon}) = \sum_{\sigma\in G} (\log|\sigma^{-1}\epsilon|)\sigma$, $\epsilon$ est fixe par les éléments de $H$, on peut donc sommer sur les classes à gauche modulo $H$. Si on multiplie $\sigma$ à droite par $\gamma$, on a

$$|(\sigma\gamma)^{-1}\epsilon| = |\gamma(\sigma^{-1}\epsilon)| = |\sigma^{-1}\epsilon|$$

et on est conduit à sommer sur les doubles classes et à écrire :

$$\lambda^*(\bar{\epsilon}) = \sum_{\sigma_i\in S} (\log|\sigma_i^{-1}\epsilon|)\tilde{H\sigma_i C} .$$

Remarquons alors que

$$\sum_{\sigma_i\in S} \log|\sigma_i^{-1}\epsilon| \frac{|H\sigma_i C|}{|H\sigma_o C|} \tilde{H\sigma_o C} = 0 .$$

Cela résulte de l'égalité $\sum_{\sigma_j\in S'} \log|\sigma_j^{-1}\epsilon| = 0$ où $S'$ est un système complet de représentants des classes à gauche de $G$ modulo $H$. En effet $\sum_{\sigma_j\in S'} \log|\sigma_j^{-1}\epsilon| = \log|N_{K^H/\mathbb{Q}}\epsilon|$.

Cette remarque entraîne

$$\lambda^*(\bar{\epsilon}) = \sum_{\sigma_i\in S} \left(\log|\sigma_i^{-1}\epsilon|\right)\left(\tilde{H\sigma_i C} - \frac{|H\sigma_i C|}{|H\sigma_o C|} \tilde{H\sigma_o C}\right) .$$

Ainsi sont mises en évidence des $\mathbb{Z}$-bases de $\mathfrak{L}^{*H}$ et $\lambda^*(\overline{U^H})$ : l'une est formée des éléments

$$\theta_i = \tilde{H\sigma_i C} - \frac{|H\sigma_i C|}{|H\sigma_o C|} \tilde{H\sigma_o C}$$

pour $\sigma_i$ parcourant $S - \{\sigma_o\}$, l'autre des $\sum_{\sigma_i\in S-\{\sigma_o\}} \log|\sigma_i^{-1}\epsilon_j|\theta_i$ où $\epsilon_j$ parcourt un système d'unités fondamentales de $K^N$. On calcule alors sans difficulté l'indice des deux $\mathbb{Z}$-réseaux $\mathfrak{L}^{*H}$ et $\lambda^*(\overline{U^H})$ de $\mathbb{C}\otimes_{\mathbb{Z}}\mathfrak{L}^*$, c'est un nombre réel égal à

$$[\mathfrak{L}^{*H} : \lambda^*(\overline{U^H})] = \delta(H)2^{-r_2(H)}R(H) .$$

Reste à démontrer la première assertion. On remarque d'abord que les

$\widehat{\tilde{H}\sigma_i\tilde{C}}$ , où $\sigma_i$ parcourt $S - \{\sigma_o\}$ , est une $\mathbb{Z}$-base de $\mathfrak{L}^H$ , cela se voit en remarquant que $\mathfrak{L}^H$ est formé des éléments de $\mathbb{Z}[G]/\mathbb{Z}\tilde{G}$ invariants à droite par la multiplication par $\gamma$ et à gauche par la multiplication par les éléments de $H$ . On passe de $\lambda^*(\bar{\epsilon})$ à $\lambda(\bar{\epsilon})$ en ajoutant un $\wedge$ sur les $\sigma$ dans l'équation définissant $\lambda^*(\bar{\epsilon})$ .

Il en résulte :

$$[\mathfrak{L}^H : \lambda(\overline{U^H})] = \delta(H)2^{-r_2(H)}R(H)\,|\det A|$$

où $A = (a_{i,j})$ est la matrice de passage de la base

$$\left\{\tilde{H}\sigma_i\tilde{C} - \frac{|H\sigma_i C|}{|H\sigma_o C|}\tilde{H}\sigma_o\tilde{C}\right\}_{\sigma_i \in S-\{\sigma_o\}}$$

à la base

$$\{\tilde{H}\sigma_i\tilde{C}\}_{\sigma_i \in S-\{\sigma_o\}}$$

d'où

$$a_{i,j} = \delta_{i,j} + \frac{|H\sigma_i C|}{|H\sigma_o C|} .$$

Comme les doubles classes forment une partition de $G$ on a $\sum_i a_{i,j} = \frac{[G:H]}{\delta(H)}$ qui exprime que la somme des éléments de chaque colonne de $A$ est constante et égale à $\frac{[G:H]}{\delta(H)}$ . Posons $\nu_i = \frac{|H\sigma_i C|}{|H\sigma_o C|}$ , on peut écrire

$$A = \begin{pmatrix} 1+\nu_1 & \nu_1 & \cdots\cdots & \nu_1 \\ \nu_2 & 1+\nu_2 & \cdots\cdots & \nu_2 \\ \vdots & \vdots & & \vdots \\ \nu_r & \nu_r & & 1+\nu_r \end{pmatrix}$$

d'où par un calcul classique

$$\det A = \frac{[G:H]}{\delta(H)}$$

et la première assertion.

Remplaçons alors dans la formule (3) de Brauer-Kuroda $R(H)$ par son expression tirée de la propriété III.1, on obtient :

$$\overline{\prod_H} h(H)^{a_H} = \left(\overline{\prod_H} (w_2(H)[G:H])^{a_H}\right) \times 2^{-\sum_H a_H r_2(H)} \times \overline{\prod_H} [\mathfrak{L}^H : \lambda(U^H)]^{-a_H} .$$

La remarque I.1 montre que $\sum_H a_H = \sum_H a_H r_2(H) = 0$, le deuxième membre se réduit donc à $\overline{\prod_H} \left(\frac{w_2(H)}{|H|} \frac{1}{[\mathfrak{L}^H : \lambda(U^H)]}\right)^{a_H}$. Soit alors $L$ un sous-$\mathbb{Z}[G]$-module de $E$ isomorphe à $\mathfrak{L}$. $\lambda$ étant un $\mathbb{Z}[G]$-homomorphisme injectif de $E$ dans $\mathbb{C} \otimes \mathfrak{L}$, $\lambda(L^H) = \lambda(L)^H$, en outre

$$[\mathfrak{L}^H : \lambda(U^H)] = [\mathfrak{L}^H : (\lambda L)^H][(\lambda L)^H : \lambda(U^H)] .$$

Le théorème des indices de Walter montre que

$$\overline{\prod_H} [\mathfrak{L}^H : (\lambda L)^H]^{a_H} = 1$$

d'où

$$\overline{\prod_H} [\mathfrak{L}^H : \lambda(U^H)][\lambda(U^H) : (\lambda L^H)]^{a_H} = 1$$

d'où

$$\overline{\prod_H} h(H)^{a_H} = \overline{\prod_H} \left(\frac{w_2(H)}{|H|} [U^H : L^H]\right)^{a_H} .$$

Notons $\mathfrak{B}$ l'invariant de Brauer : $\mathfrak{B} = \overline{\prod_H} [E^H : L^H]^{a_H}$,

$\mathfrak{H}$ l'invariant de Hasse : $\mathfrak{H} = \overline{\prod_H} [E^H : U^H]$,

la relation entre les nombres de classes associée à la relation de dépendance linéaire entre les caractères s'écrit sous la forme suivante mise en évidence par Brauer :

$$\mathfrak{H} \overline{\prod_H} h(H)^{a_H} = \mathfrak{B} \overline{\prod_H} \left(\frac{w_2(H)}{|H|}\right)^{a_H} . \tag{4}$$

La deuxième assertion de la propriété III.1 et l'utilisation du sous-$\mathbb{Z}[G]$-module $L^*$ de $E$, isomorphe à $\mathfrak{L}^*$ nous conduit à la formule suivante où $\mathfrak{w}$ désigne l'invariant de Walter :

$$\mathfrak{H} \overline{\prod_H} h(H)^{a_H} = \mathfrak{w} . \overline{\prod_H} (w_2(H)\delta(H))^{a_H} .$$

On a vu que si $E$ est $\mathbb{Z}[G]$-isomorphe à $\mathfrak{L}$ alors $\mathfrak{B} = 1$. N. Moser a prouvé dans [4] que $E$ est isomorphe à $\mathfrak{L}$ si et seulement si il existe une unité de Minkowski au sens restreint. Dans le même tra-

vail, elle montre que si $K/\mathbb{Q}$ est imaginaire il peut y avoir unité de Minkowski au sens restreint avec $\mathcal{B} \neq 1$ . Ce qui implique l'existence de $\mathbb{Z}[G]$-modules de caractère $1_C^G - 1_G^G$ non isomorphes à $\mathfrak{L}$ . C'est l'objet de ce qui suit.

## IV. UTILISATION DU THEOREME DE WALTER COMME TEST D'ISOMORPHIE.

On s'intéresse d'abord à la question suivante : pour quels $G$ les modules $\mathfrak{L}$ et $\mathfrak{L}^*$ sont-ils isomorphes ? Donnons une première réponse partielle dans le cas réel.

PROPRIETE IV.1. - Les modules $\mathbb{Z}[G]/\mathbb{Z}\tilde{G}$ et $I_G$ sont $\mathbb{Z}[G]$-isomorphes si et seulement si $G$ est cyclique.

Démonstration : si $G$ est cyclique et engendré par $G$ , $I_G = \mathbb{Z}[G](\sigma - 1)$ et d'après [4] proposition I.3, $I_G$ est $\mathbb{Z}[G]$-isomorphe à $\mathbb{Z}[G]/\mathbb{Z}\tilde{G}$ . Supposons alors $G$ non cyclique, nous allons exhiber une relation du type (2) pour laquelle

$$\prod_H [I_G^H : (\mathbb{Z}[G]/\mathbb{Z}\tilde{G})^H]^{a_H} \neq 1$$

on aura prouvé que $I_G$ et $\mathbb{Z}[G]/\mathbb{Z}\tilde{G}$ sont non-$\mathbb{Z}[G]$-isomorphes et même qu'ils ne sont pas dans le même genre. Pour un tel $G$ ou bien il existe $p$ tel que les p-groupes de Sylow soient non cycliques, ou bien pour tout $p$ les p-groupes de Sylow de $G$ sont cycliques. Ces derniers groupes sont décrits dans [2] p. 111. Ils sont engendrés par deux éléments $a,b$ avec les relations $a^m = b^n = 1$ , $b^{-1}ab = a^s$ où $m,n,s$ sont les entiers naturels plus grands que 1 vérifiant $(s-1)n$ et $m$ sont premiers entre eux.

Premier cas : Tous les p-groupes de Sylow sont cycliques. Un calcul facile utilisant la formule (1) donne

$$1_G^G = \frac{1}{m}\sum_{i=0}^{m-1} 1_{g_i}^G + \frac{1}{n} 1_H^G - \frac{1}{n} 1_1^G$$

où les $g_i$ , $i=0,\ldots,m-1$ sont les sous-groupes conjugués de $g_o = \langle b\rangle$ et où $H$ désigne le sous-groupe dérivé de $G$ .

La relation s'écrit alors :

$$(2') \qquad mn 1_G^G - n\sum_{i=0}^{m-1} 1_{g_i}^G - m 1_H^G + m 1_1^G = 0 \ .$$

Deuxième cas : $G$ admet un p-sous-groupe de Sylow non cyclique $S$ . $S$ étant non cyclique, il existe $T$ distingué dans $S$ tel que $S/T \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ . Ecrivons la relation (1) en prenant $G = H = S/T$ . On obtient, en notant $H_i$ , $i=1,\ldots,p+1$ les sous-groupes d'ordre $p$ de $S/T$ :

$$1_{S/T}^{S/T} = \frac{1}{p}\sum_{i=1}^{p+1} 1_{H_i}^{S/T} - \frac{1}{p} 1_1^{S/T}$$

et on a la relation de dépendance $\mathbb{Z}$-linéaire

$$p\, 1_{S/T}^{S/T} - \sum_{i=1}^{p+1} 1_{H_i}^{S/T} + 1_1^{S/T} = 0 \ .$$

Comme l'a indiqué C.D. Walter dans [8 ] lemme 3.1.2, cette relation implique la relation suivante obtenue en prenant les images réciproques par la projection canonique de $S$ sur $S/T$ des sous-groupes de $S/T$ qui interviennent :

$$p\, 1_S^S - \sum_{i=1}^{p+1} 1_{H_i'}^S + 1_T^S = 0$$

où les $H_i'$ sont les images réciproques des $H_i$ . En prenant les caractères induits à $G$ tout entier on a enfin

$$(2'') \qquad p\, 1_S^G - \sum_{i=1}^{p+1} 1_{H_i'}^S + 1_T^G = 0 \ .$$

Remarquons alors que la Propriété III.1 entraîne :

$$\overline{\prod_H} [\mathfrak{L}^{*H} : \mathfrak{L}^H]^{a_H} = \overline{\prod_H} \left(\frac{\delta(H)}{[G:H]}\right)^{a_H}$$

dans le cas envisagé ici $\mathfrak{L} = \mathbb{Z}[G]/\mathbb{Z}\tilde{G}$ , $\delta(H) = 1$ , pour tout $H$ , d'autre part $\sum_H a_H = 0$ entraîne $\overline{\prod_H} \frac{1}{|G|^{a_H}} = 1$ d'où

$$\overline{\prod_H} [\mathfrak{L}^{*H} : \mathfrak{L}^H] = \overline{\prod_H} |H|^{a_H} .$$

Dans le premier cas la relation (2') donne $\overline{\prod_H} [\mathfrak{L}^{*H} : \mathfrak{L}^H] = m^{m(n-1)}$ qui diffère de 1 . Dans le deuxième cas la relation (2") donne $\overline{\prod_H} [\mathfrak{L}^{*H} : \mathfrak{L}^H]^{a_H} = p^{p-1} \neq 1$ .

Le cas imaginaire est plus compliqué. Nous commencerons par une remarque :

Remarque IV.1. - Si $G = CH$ avec $H$ distingué, alors $\mathfrak{L}^* = I_G\tilde{C} = I_H\tilde{C}$ et $\mathfrak{L}^*$ est monogène si et seulement si $I_H\tilde{C}$ est $\mathbb{Z}[G]$-monogène. Si $I_H$ est $\mathbb{Z}[H]$-monogène, ce qui équivaut, on vient de le voir, à $H$ cyclique, alors $\mathfrak{L}^*$ est $\mathbb{Z}[G]$-monogène. Mais $I_H\tilde{C}$ peut être $\mathbb{Z}[G]$-monogène sans que $I_H$ soit $\mathbb{Z}[H]$-monogène. On le voit sur le groupe $G$ produit semi-direct de $H$ par $C$ où $H$ est défini par les générateurs $\sigma$ et $\tau$ et les relations $\sigma^p = \tau^p = 1$ , $\sigma\tau = \tau\sigma$ et l'opération de $\gamma$ sur $H$ étant définie par $\gamma\sigma\gamma^{-1} = \tau$ . $I_H\tilde{C}$ est engendré par $(\sigma-1)\tilde{C}$ et $(\tau-1)\tilde{C}$ , mais $\gamma(\sigma-1)\tilde{C} = (\tau-1)\tilde{C}$ donc $I_H\tilde{C}$ admet comme $\mathbb{Z}[G]$-générateur $(\sigma-1)\tilde{C}$ .

Examinons enfin le problème suivant suggéré par les résultats de N. Moser dans le cas dièdral imaginaire : $G$ admettant un sous-groupe $C$ d'ordre 2 , existe-t-il un idéal à gauche $\mathfrak{a}$ de $\mathbb{Z}[G]$ contenant $\tilde{C}$ tel que $\mathbb{Z}[G]/\mathfrak{a}$ ait pour caractère $1_C^G - 1_G^G$ ? Cela revient à chercher s'il peut exister une unité de Minkowski au sens large de norme égale à 1 sur le sous-corps réel maximal.

PROPRIETE IV.2. (démontrée avec l'aide de J.M. Fontaine) - Pour qu'il existe $\mathfrak{a}$ idéal à gauche de $\mathbb{Z}[G]$ avec $\tilde{C} \in \mathfrak{a}$ et $\mathbb{Z}[G]/\mathfrak{a}$ a pour caractère $1_C^G - 1_G^G$ , il faut et il suffit que $G = CH$ avec $H$ abélien distingué d'ordre impair sur lequel $\gamma$ opère par $\gamma\sigma\gamma = \sigma^{-1}$ pour tout $\sigma$ de $H$ .

Démonstration : Supposons que $\mathfrak{a}$ existe avec les propriétés $\tilde{C} \in \mathfrak{a}$ et $\mathbb{Z}[G]/\mathfrak{a}$ de caractère $1_C^G - 1_G^G$. De $\mathbb{Q}[G] = \mathbb{Q}[G](1+\gamma) + \mathbb{Q}[G](1-\gamma)$ résulte $\mathbb{Q}[G]\tilde{C} \subset \mathbb{Q} \otimes_{\mathbb{Z}} \mathfrak{a}$. On pose $|G| = 2m$, l'assertion sur le caractère de $\mathbb{Z}[G]/\mathfrak{a}$ montre que $\dim_{\mathbb{Q}} \mathbb{Q} \otimes_{\mathbb{Z}} \mathfrak{a} = m+1$. Comme $\mathbb{Q}[G]$ est semi-simple, on en déduit que le caractère de $\mathfrak{a}$ est égal à la somme du caractère de $\mathbb{Q}[G]\tilde{C}$, c'est-à-dire $1_C^G$, et d'un caractère de degré 1 qu'on note $\eta$. $\mathbb{Z}[G]/\mathfrak{a}$ a donc comme caractère le caractère de $\mathbb{Z}[G]$ moins celui de $\mathfrak{a}$ soit : $1_1^G - 1_C^G - \eta$ d'où la condition nécessaire :

$$1_1^G = 2(1_C^G - 1_G^G) + \eta + 1_G^G$$

au premier membre figure le caractère de la représentation régulière et au second une somme de "vrais" caractères. Le caractère de la représentation régulière s'écrit classiquement $\sum d_i \psi_i$ où les $\psi_i$ sont les caractères absolument irréductibles de $G$ et $d_i$ le degré de $\psi_i$. $1_C^G - 1_G^G$ étant le caractère d'une représentation est somme à coefficients entiers positifs ou nuls des $\psi_i$, soit $1_C^G - 1_G^G = \sum \lambda_i \psi_i$. L'unicité de la décomposition en somme de caractères absolument irréductibles entraîne que $G$ admet deux caractères absolument irréductibles de degré 1 et que les autres sont de degré pair. Le groupe $G'$ dérivé de $G$ est donc d'indice 2 et en égalant les degrés des deux membres on obtient :

$$2m = 1 + 1 + \sum d_{i'}^2 \quad ,$$

les $d_{i'}$ étant pairs, $m$ est nécessairement impair, c'est l'ordre de $G'$.

Soit alors $x \in G - G'$, $\eta$ étant non trivial, $\eta(x) = -1$, d'autre part $1_G^G(x) = 1$ et $1_1^G(x) = 0$ l'égalité entre caractères entraîne $1_C^G(x) = 1$. Revenons à la définition de $1_C^G$, soit $h_i$ un système complet de représentants des classes à gauche de $G/C$, on sait (voir par exemple [6] chap. 3) que $1_C^G(x) = \sum_{h_i^{-1}xh_i \in C} 1_C^C(h_i^{-1}xh_i)$, il existe donc un $h_i$ et un seul tel que $h_i^{-1}xh_i \in C$, en outre $h_i^{-1}xh_i \neq 1$ sinon $x$ serait l'élément unité. Pour ce $h_i$ on a donc $h_i^{-1}xh_i = \gamma$. Cela signifie que $\gamma$ et les éléments de $G - G'$ sont dans la même classe de conjugaison de $G$, le cardinal de celle-ci est donc au moins égal à $m$,

comme c'est un diviseur strict de $|G|$ on en déduit que $G-G'$ est une classe de conjugaison contenant $\gamma$ . Il en résulte $G = CG'$ . Un élément de $G - G'$ s'écrit $\gamma h$ avec $h$ dans $G'$ , étant conjugué de $\gamma$ , il est d'ordre 2 d'où $\gamma h \gamma = h^{-1}$ . Comme $h \to \gamma h \gamma$ est un automorphisme de $G'$ , ce groupe est nécessairement abélien.

Supposons réciproquement $G = CH$ avec $H$ abélien d'ordre impair et $\gamma \sigma \gamma = \sigma^{-1}$ pour tout $\sigma$ de $H$ . On voit que $\mathfrak{a} = \mathbb{Z}[G]\tilde{C} + \mathbb{Z}\tilde{G}$ est un idéal à gauche de $\mathbb{Z}[G]$ de caractère $1_C^G + \eta$ où $\eta$ est le caractère de degré 1 autre que $1_G^G$ . Notons encore $\eta$ le caractère irréductible de degré 1 non trivial sur $G-H$ . Vérifions l'égalité $1_1^G = 2(1_C^G - 1_G^G) + \eta + 1_G^G$ , on compare les valeurs des deux membres :

si $x = e$ , $1_1^G(e) = 2m$ , $1_C^G(e) = m$ , $1_G^G(e) = \eta(e) = 1$

si $x \in G'-e$ , $1_1^G(x) = 0$ , $1_C^G(x) = 0$ , $1_G^G(x) = 1 = \eta(x)$

si $x \in G-G'$ , $1_1^G(x) = 0$ , $1_C^G(x) = 1$ , $1_G^G(x) = 1$ et $\eta(x) = -1$ .

Pour tout $x$ dans $G$ les deux membres sont égaux, il y a donc bien égalité des caractères. Le caractère de $\mathbb{Z}[G]/\mathfrak{a}$ étant $1_1^G - 1_C^G - \eta$ l'égalité précédente montre que $\mathbb{Z}[G]/\mathfrak{a}$ a pour caractère $1_C^G - 1_G^G$ d'où la propriété.

Remarque IV.2. - $K/\mathbb{Q}$ imaginaire de groupe de Galois $G$ , il existe une unité de Minkowski au sens large de norme 1 sur le sous-corps réel maximal de $K$ si et seulement si $G = CG'$ , $G'$ abélien d'ordre impair sur lequel $\gamma$ opère par retournement.

BIBLIOGRAPHIE

[1] R. BRAUER - "Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoischen Körpers". Math. Nachr. 4 (1951) pp. 158-174.

[2] W. FEIT - "Characters of finite groups". Benjamin, Inc. New-York. Amsterdam 1967.

[3] S.N. KURODA - "Über die Klassenzahlen algebraischer Zahlkörper". Nagorpa Math. J. 1 (1950) pp. 1-10.

[4] N. MOSER - "Unités et nombre de classes d'une extension galoisienne diédrale de $\mathbb{Q}$ ". Sém. Th. des Nombres, Univ. de Grenoble 1974, et à paraître Math. Sem. der Univ. Hamburg.

[5] I. REINER - "A survey of integral representation theory". Amer. Math. Soc. Bull. 76 (1970) pp. 159-227.

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

[7] J.P. SERRE - "Corps locaux". Hermann, Paris 1962.

[8] C.D. WALTER - "Class number relations". A paraître Acta Arithmetica.

-:-:-:-

Laboratoire de Mathématiques Pures - Institut Fourier
dépendant de l'Université Scientifique et Médicale de Grenoble
associé au C.N.R.S.
B.P. 116
38402 ST MARTIN D'HERES (France)