JEAN-JACQUES PAYAN

Sur un article de Brauer concernant les nombres de classes d'une extension galoisienne de corps de nombres et de certains corps intermédiaires

Séminaire de théorie des nombres de Grenoble, tome 3 (1973-1974), exp. nº 8, p. 1-6
<http://www.numdam.org/item?id=STNG_1973-1974__3__A8_0>

Séminaire de Théorie des Nombres
6 juin 1974
Grenoble

SUR UN ARTICLE DE BRAUER CONCERNANT LES NOMBRES DE CLASSES D'UNE EXTENSION GALOISIENNE DE CORPS DE NOMBRES ET DE CERTAINS CORPS INTERMEDIAIRES [1]

par Jean Jacques PAYAN

Rappels.

On sait que si k désigne un corps de nombres, K une extension galoisienne finie de k de groupe de Galois G et L une extension intermédiaire quelconque, on a les relations suivantes : [2]

a) $L(s,1,K/k) = \zeta_k(s)$.

b) $L(s,\chi_1+\chi_L,K/k) = L(s,\chi_1,K/k)\cdot L(s,\chi_2,K/k)$.

c) χ étant un caractère de $\mathrm{Gal}\ K/L$, on note χ^* le caractère induit sur G alors $L(s,\chi_1+\chi_2,K/k) = L(s,\chi^*,K/k)$.

On sait d'après un résultat d'Artin [5] que tout caractère χ s'écrit sous la forme $\chi = \sum_{i\in I} \lambda_i \chi_i^*$ où les χ_i sont des caractères de sous-groupes cycliques et les λ_i des rationnels.

Dans le cas où χ est à valeurs rationnelles, le résultat suivant est plus précis.

THEOREME 1 (Brauer). Soit G un groupe fini, pour tout sous-groupe H de G, on note χ_H le caractère de G induit par le caractère trivial de H. Soit Φ un caractère sur G à valeurs rationnelles alors

$$\Phi = \sum_{\substack{H \text{ sous-groupe} \\ \text{cyclique de } G}} C_H \chi_H$$

avec

$$C_H = \frac{\text{Card } H}{\text{Card } G} \sum_{H'} \mu([H':H]) \Phi(z')$$

où H' parcourt les sous-groupes cycliques de G qui contiennent H, où μ est la fonction de Möbius et où z' est un générateur de H'.

Démonstration : $\Phi(z')$ ne dépend pas du générateur z' choisi dans H', en effet si $z'_1 = z'^m$ avec $(m, \text{Card } H') = 1$, on aura $\Phi(z') = \epsilon_1 + \ldots + \epsilon_d$ où les ϵ_i sont des racines Card H'-ièmes de l'unité. On a $\Phi(z'_1) = \epsilon_1^m + \ldots + \epsilon_d^m$ c'est l'image de $\Phi(z') \in \mathbb{Q}$ par un élément du groupe de Galois du corps des racines Card H'-ièmes de l'unité donc $\Phi(z'_1) = \Phi(z')$.

Considérons alors le caractère $\psi = \sum_{\substack{H \text{ cyclique} \\ \text{ss groupe de } C}} C_H \chi_H$ où C_H a la valeur définie dans l'énoncé.

Pour tout sous-groupe H, de G, on note $\mathfrak{N}(H_1)$ son normalisateur. Soit α un élément de G, $\chi_H(\alpha) = \sum_{g \in G/H} \overline{\chi}_{0,H}(g^{-1}\alpha g)$ où $\chi_{0,H}$ désigne le caractère unité de H et $\overline{\chi}_{0,H}$ le prolongement à G obtenu en posant $\overline{\chi}_{0,H}(x) = 0$ si $x \in G-H$. On voit facilement que si α n'est pas conjugué d'un élément de H, $\chi_H(\alpha) = 0$ si α est conjugué d'un élément de H, $\chi_H(\alpha) = \dfrac{\text{Card } \mathfrak{N}(\langle\alpha\rangle)}{\text{Card } H}$.

Il en résulte

$$\psi(\alpha) = \sum_{H \text{ cyclique}} \sum_{\substack{H' \supset H \\ H' \text{ cyclique}}} \frac{\text{Card } H}{\text{Card } G} \mu([H':H]) \frac{\text{Card } \mathfrak{N}(\langle\alpha\rangle)}{\text{Card } H} \Phi(z')$$

$$= \frac{\text{Card } \mathfrak{N}(\langle\alpha\rangle)}{\text{Card } G} \sum_{H}{}' \sum_{H'} \mu([H':H]) \Phi(z')$$

où Σ' signifie qu'on ne prend que les H cycliques contenant un conjugué de α . Remarquons qu'un H ne peut contenir qu'un sous-groupe conjugué de $\langle\alpha\rangle$ et que G contient $[G:\mathfrak{N}(\langle\alpha\rangle)]$ sous-groupes conjugués de $\langle\alpha\rangle$ d'où

$$\psi(\alpha) = \frac{\operatorname{Card} \mathfrak{N}(\langle\alpha\rangle)}{\operatorname{Card} G} \cdot [G:\mathfrak{N}(\langle\alpha\rangle)] \sum_{H}'' \sum_{H'} \mu([H':H]) \times \Phi(z')$$

où Σ'' signifie que l'on somme sur les H cycliques contenant $\langle\alpha\rangle$, on obtient après simplification.

$$\psi(\alpha) = \sum_{\substack{H' \text{ cyclique} \\ H' \supset \langle\alpha\rangle}} \Phi(z') \sum_{\substack{H \text{ cyclique} \\ H' \supset H \supset \langle\alpha\rangle}} \mu([H':H])$$

posons $\operatorname{Card} \langle\alpha\rangle = d$, $\operatorname{Card} H' = m'$ alors d divise m' et les H cycliques dans la somme intérieure correspondent bijectivement aux diviseurs de $\frac{m'}{d}$ d'où

$$\psi(\alpha) = \sum_{\substack{H' \text{ cyclique} \\ H' \supset \langle\alpha\rangle}} \Phi(z') \sum_{d' \mid \frac{m'}{d}} \mu(d')$$

on sait que la fonction de Möbius vérifie pour tout entier naturel n supérieur à 1 , $\sum_{d' \mid n} \mu(d') = 0$, il en résulte que le seul H' pour lequel $\sum_{d' \mid \frac{m'}{d}} \mu(d')$ sera distinct de 0 est $H' = \langle\alpha\rangle$, d'après ce qui a été dit au début de la démonstration $\Phi(z') = \Phi(\alpha)$, comme $\mu(1) = 1$ on a $\psi(\alpha) = \Phi(\alpha)$.

Si on remarque que le caractère trivial d'un sous-groupe G' quelconque de G est à valeurs rationnelles, on peut énoncer

COROLLAIRE. <u>Soit</u> G' <u>un sous-groupe de</u> G , <u>alors</u>

$$\chi_{G'} = \sum_{\substack{H \text{ cyclique} \\ H \subset G'}} C_H \chi_H \quad \underline{\text{avec}} \quad C_H = \frac{1}{[G:H]} \sum_{H'} \mu([H':H]) .$$

Application aux fonctions zeta.

On reprend les notations figurant dans les rappels du début et on pose $G' = \mathrm{Gal}\, K/L$, alors

$$\zeta(s,L) = L(s,1,K/\Omega_1) = L(s,\chi_G,K/k)$$

d'après les rappels a) et c) soit encore d'après le théorème de Brauer

$$\zeta(s,L) = L(s,\sum_H C_H \chi_H,K/k)$$

en appliquant la linéarité des fonctions L

$$\zeta(s,L) = \prod_H L(s,\chi_H,K/k)^{C_H} = \prod_H \zeta(s,K^H)^{C_H}$$

qui donne lieu à l'énoncé suivant :

THEOREME 2 (Brauer). *Soit* L *une extension intermédiaire de l'extension galoisienne de corps de nombres* K/k , *alors*

$$\zeta(s,L) = \prod_\Omega \zeta(s,\Omega)^{C_\Omega}$$

où Ω' *parcourt les extensions intermédiaires de* K/L *telles que* K/Ω *cyclique et où* $C_\Omega = \frac{1}{[\Omega:L]} \sum_{\Omega'} \mu([\Omega:\Omega'])$ *où* Ω' *les extensions intermédiaires de* Ω/L *telles que* K/Ω' *soit cyclique*.

Exemples :

1) Considérons le composé K de deux extensions cycliques de degré premier p sur $\mathbb{Q}$, il y a $p+1$ extensions intermédiaires de degré p sur $\mathbb{Q}$, soient : $L_1,\ldots,L_{p+1}$. On voit facilement que la seule extension intermédiaire donnant une relation non triviale est $\mathbb{Q}$, d'où on tire

$$\zeta(s,Q) = \zeta(s,K)^{C_K} \prod_{i=1}^{p+1} \zeta(s,L_i)^{C_{L_i}} .$$

Un calcul facile donne $C_K = -\frac{1}{p}$ et $C_{L_i} = \frac{1}{p}$ d'où

$$\zeta(s,K)\zeta(s,\mathbb{Q})^p = \prod_{i=1}^{p+1} \zeta(s,L_i) .$$

2) Considérons $K/\mathbb{Q}$ à groupe de Galois G défini par les générateurs σ, τ où $\sigma^p = 1$, $\tau\sigma\tau^{-1} = \sigma^r$, $\tau^m = 1$ où p est un nombre premier impair, m un diviseur de $p-1$ et r une racine primitive m-ième de l'unité modulo p . Il y a p extensions intermédiaires, de degré p sur $\mathbb{Q}$, soient $L_1, \ldots, L_p$ et une extension intermédiaire cyclique de degré m sur $\mathbb{Q}$ soit k . Les seules extensions intermédiaires donnant lieu à une relation non triviale sont les extensions contenues strictement dans k . Dans le cas où m est premier, il n'y en a qu'une, à savoir $\mathbb{Q}$.

$$\zeta(s,\mathbb{Q}) = \zeta(s,k)^{C_k} \zeta(s,K)^{C_K} \prod_{i=1}^{p} \prod_{\Omega} \zeta(s,\Omega)^{C_\Omega}$$

où Ω parcourt l'ensemble des extensions intermédiaires de K/L_i différentes de K . Si $L_i \neq \Omega \neq K$, alors $C_\Omega = \sum_{d \mid \frac{m}{[\Omega:L_i]}} \mu(d)$ avec $\frac{m}{[\Omega:L_i]} > 1$ d'où $C_\Omega = 0$, le $\prod_{i=1}^{p} \prod$ se réduit donc à $\prod_{i=1}^{p} \zeta(s,L_i)^{C_{L_i}}$ les L_i étant conjugués, les $\zeta(s,L_i)$ coïncident et un calcul facile montre que

$$\boxed{\zeta(s,K)\zeta(s,\mathbb{Q})^m = \zeta(s,k)\zeta(s,L)^m} \quad .$$

On sait que le nombre de classes h_K d'une extension finie K du corps des rationnels est lié au résidu en 1 de la fonction $\zeta(s,K)$, plus précisément

$$\lim_{s\to 1^+} (s-1)\zeta(s,K) = \frac{2^{s_K+t_K} \pi^{t_K} R_K h_K}{\omega_K \sqrt{|D_K|}}$$

où ω_K désigne le nombre de racines de l'unité dans K , D_K le discriminant et R_K le régulateur de K .

On obtient facilement des relations analogues à celles du théorème 2 pour les discriminants et les nombres de racines de l'unité contenues dans chaque extension. On peut alors en déduire une formule où ne figurent que des nombre de classes et des régulateurs. Dans certains cas particuliers, on peut simplifier la partie correspondant aux régulateurs et obtenir des formules liant les nombres de classes. Pour le groupe de Klein on trouvera une démonstration dans [3], pour le groupe diédral voir [4] .

BIBLIOGRAPHIE

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

[2] CASSELS et FRÖHLICH - Algebraic Number Theory. Chap.VIII. London-New-York Academic Press (1967).

[3] HASSE H. - Über die Klassenzahl abelscher Zahlkörper. Berlin. Akademic Verlag, 1952.

[4] MOSER N. - Unités et nombre de classes d'une extension galoisienne diédrale de $\mathbb{Q}$. Sém. Th. Nb. Grenoble, 1973-74.

[5] SERRE J.P. - Représentations linéaires des groupes finis. 2ème Ed. Hermann Paris 1971.

-o-o-