Séminaire de théorie des nombres de Grenoble

Françoise Bertrandias

Sur le nombre de classes relatif d'une extension cyclique de degré ℓ^ν (ℓ premier impair) de corps de nombres

Séminaire de théorie des nombres de Grenoble, tome 1 (1971-1972), p. 104-107
<http://www.numdam.org/item?id=STNG_1971-1972__1__104_0>

SUR LE NOMBRE DE CLASSES RELATIF D'UNE EXTENSION CYCLIQUE DE DEGRE ℓ^ν (ℓ premier impair) DE CORPS DE NOMBRES

par Françoise BERTRANDIAS le 3.5.72

1. On note $K|k$ une extension cyclique de degré ℓ^ν de corps de nombres (ℓ premier $\neq 2$, et $\nu \geq 1$). Par définition, le nombre de classes relatif de cette extension, qu'on notera $h^*(K|k)$, est le nombre des classes d'idéaux de K dont la norme sur k est la classe principale.

Le but de cet exposé est de donner une démonstration du résultat suivant (démonstration obtenue en collaboration avec J.J. Payan) :

Théorème.

Le nombre de classes relatif $h^*(K|k)$ d'une extension cyclique de degré ℓ^ν (ℓ premier $\neq 2$) de corps de nombres est norme d'un idéal entier du corps $\mathbb{Q}^{(\ell)}$ des racines ℓ-èmes de l'unité.

(On trouve des énoncés voisins dans [1], [2], [4]).

Comme l'entier ℓ est norme d'un entier de $\mathbb{Q}^{(\ell)}$, il suffit, pour obtenir le résultat annoncé, de montrer que, quel que soit le nombre premier $p \neq \ell$, la participation de p à $h^*(K|k)$, qu'on notera $h_p^*(K|k)$, est une norme d'un idéal entier de $\mathbb{Q}^{(\ell)}$. On déduira donc le théorème du résultat suivant :

Proposition 1.

Pour tout nombre premier $p \neq \ell$, on a :

$$h_p^*(K|k) \equiv 1 \pmod{\ell} \quad .$$

La démonstration de la proposition 1 fournira également l'énoncé suivant :

Proposition 2.

On note : h_K (resp h_k) le nombre de classes de K (resp k)

$h_{K,p}$ (resp $h_{k,p}$) la participation du nombre premier p à h_K (resp h_k) .

Pour tout nombre premier $p \neq \ell$, on a :

$$h_p^*(K|k) = \frac{h_{K,p}}{h_{k,p}} \quad .$$

2. La démonstration des propositions 1 et 2 repose sur le lemme suivant :

Lemme.

Soit G un groupe cyclique d'ordre g opérant sur un groupe abélien H d'ordre h premier à g . On note σ un générateur de G et $N = 1+\sigma+..+\sigma^{g-1}$ l'endomorphisme norme de H .

On a : $H = \mathrm{Im}\ N \underset{\text{direct}}{\times} \ker N$.

De plus : $\mathrm{Im}\ N = H^G$ et $\ker N = H^{\sigma-1}$,

(où H^G est le sous-groupe des éléments de H invariants par G , et $H^{\sigma-1}$ le sous-groupe des éléments de H de la forme $x^{\sigma-1}$) .

Démonstration du lemme :

a) Montrons : $H = \mathrm{Im}\ N \times \ker N$.

Soient u et v deux entiers vérifiant $ug + vh = 1$; si appartient à H , on a : $x = x^{ug} = (Nx)^u \left(\frac{x^g}{Nx}\right)^u$. Or $\frac{x^g}{Nx}$ appartient à $\ker N$. D'où le résultat annoncé.

b) Montrons que $\mathrm{Im}\ N \cap \ker N = \{1\}$.

Soit x un élément de $\mathrm{Im}\ N \cap \ker N$; on a : $x = Ny$ et $Nx = 1$. Comme $Nx = (Ny)^g = 1$, $x^g = 1$, d'où $x = x^{ug} = 1$.

c) Montrons les égalités : $\mathrm{Im}\ N = H^G$ et $\ker N = H^{\sigma-1}$. Les groupes de cohomologie du G-module H sont donnés par :

$$\hat{H}^0(G,H) = \hat{H}^{2k}(G,H) = H^G/\mathrm{Im}N$$

$$\hat{H}^1(G,H) = \hat{H}^{2k+1}(G,H) = \ker N/H^{\sigma-1} \quad .$$

Ce sont des groupes dont l'ordre divise h ; or ces groupes sont annulés par g ([3] ch. VIII, §2, corollaire 1 prop.4). Par suite ces groupes sont réduits à $\{1\}$.

3. Démonstration des propositions 1 et 2.

Notations.

$\mathcal{H}_K$ (resp $\mathcal{H}_k$) désigne le groupe des classes d'idéaux de K (resp k) .

$j : \mathcal{H}_k \to \mathcal{H}_K$ désigne l'homomorphisme induit par l'injection canonique du groupe des idéaux de k dans le groupe des idéaux de K .

$N_{K|k} : \mathcal{H}_K \to \mathcal{H}_k$ désigne l'homomorphisme induit par l'homomorphisme norme du groupe des idéaux de K dans le groupe des idéaux de k .

$\mathcal{H}_{K,p}$ (resp $\mathcal{H}_{k,p}$) désigne le p-sous-groupe de Sylow de $\mathcal{H}_K$ (resp $\mathcal{H}_k$) .

$j_p : \mathcal{H}_{k,p} \to \mathcal{H}_{K,p}$ la restriction de j à $\mathcal{H}_{k,p}$.

$N_{K|k,p} : \mathcal{H}_{K,p} \to \mathcal{H}_{k,p}$ la restriction de $N_{K|k}$ à $\mathcal{H}_{K,p}$.

$G = \text{Gal}\,(K|k)$.

$\mathcal{H}^*(K|k)$ désigne le groupe des classes relatives de $K|k$, c'est-à-dire le sous-groupe de $\mathcal{H}(K|k)$ formé des classes dont la norme sur k est la classe principale ; $\mathcal{H}^*_p(K|k)$ désigne le p sous-groupe de Sylow de $\mathcal{H}^*(K|k)$.

On sait que G opère sur $H : \mathcal{H}_{K,p}$; on voit que les endomorphismes $N : H \to H$ et $\varphi : H \to H$ défini par $\varphi(x) = x^{\ell^\nu}$ sont liés aux homomorphismes j_p et $N_{K|k,p}$ par les relations :

$$j_p \circ N_{K|k,p} = N$$

$$N_{K|k,p} \circ j_p = \varphi \ .$$

On suppose $p \neq \ell$; l'homomorphisme φ est alors bijectif et cela entraîne : j_p injectif. Par suite le noyau de N coïncide avec le noyau de $N_{K|k,p}$, c'est-à-dire avec le p-groupe $\mathcal{H}^*_p(K|k)$ des classes relatives.

Le lemme du §2 entraîne donc :

$$H = \mathcal{H}_{K,p} = \mathcal{H}^G_{K,p} \underset{\text{direct}}{\times} \mathcal{H}^*_p(K|k)$$

($\mathcal{H}_{K,p}^{G}$ est le p-groupe des classes ambiges).

Par suite le groupe G opère sur $\mathcal{H}_p^*(K|k)$ en laissant invariante la seule classe principale ; les trajectoires des classes non principales de $\mathcal{H}_p^*(K|k)$ comportent donc $\ell^{\nu'}$ éléments , avec $1 \leq \nu' \leq \nu$. Il en résulte :

$$h_p^* \ (K/k) \equiv 1 \pmod{\ell}$$

c'est-à-dire le résultat de la proposition 1.

La proposition 2 se déduit de la décomposition en produit direct ci-dessus de $\mathcal{H}_{K,p}$ et du fait que :

$$\mathcal{H}_{K,p}^{G} = j_p(\mathcal{H}_{k,p})$$

qui se démontre comme suit : si c est une p-classe ambige, on a l'égalité $c^{\ell^\nu} = Nc = j_p \circ N_{K|k,p}(c)$ qui entraîne : c^{ℓ^ν} , et donc c , appartient à $j_p(\mathcal{H}_{k,p})$.

[1] - A. BRUMER - "On the group of units of an absolutely cyclic number field of prime degree". J. Math. Soc. Japan vol. 21, N°3, 1969, pp. 357-358.

[2] - S.N. KURODA - "Uber die Klassenzahl eines relativzyklischen Zahlkörpers vom Primzahlgrade". Proc. Japan Acad. Vol. 40, 1964, pp. 623-620.

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

[4] - H. YOKOÏ - "On the divisibility of the class number in an algebraic number field". J. Math. Soc. Japan Vol. 20, N°1.2, 1968, pp. 411-418.
