PHILIPPE SATGÉ

Inégalités de miroir

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 18, nº 2 (1976-1977), exp. nº 18, p. 1-4
<http://www.numdam.org/item?id=SDPP_1976-1977__18_2_A2_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
18e année, 1976/77, n° 18, 4 p.

7 mars 1977

INÉGALITES DE MIROIR

par Philippe SATGÉ

Soit d un entier positif sans carré, $k = \underset{\sim}{Q}(\sqrt{d})$, $\bar{k} = \underset{\sim}{Q}(\sqrt{-3d})$, $\mathcal{H}$ et $\bar{\mathcal{H}}$ les groupes des classes de k et $\bar{k}$. Désignant respectivement par $\dim_3 \mathcal{H}$ et $\dim_3 \bar{\mathcal{H}}$ les dimensions des espaces vectoriels sur le corps à trois éléments des quotients de $\mathcal{H}$ et $\bar{\mathcal{H}}$ par leurs cubes, SCHOLTZ [2] établit l'inégalité

$$0 \leqslant \dim_3 \mathcal{H} - \dim_3 \mathcal{H} \leqslant 1 .$$

LEOPOLDT [1] a généralisé ce résultat en considérant un nombre premier impair ℓ , deux corps k et $\bar{k}$ galoisiens sur $\underset{\sim}{Q}$ et de degrés non divisibles par ℓ , et en établissant des inégalités entre les dimensions sur le corps à ℓ éléments de certaines parties des quotients des groupes des classes de k et $\bar{k}$ par leurs puissances ℓ-ièmes. Nous allons établir, dans certains cas, des inégalités analogues en supprimant l'hypothèse de non-divisibilité par ℓ des degrés de k et $\bar{k}$. Les démonstrations de ces inégalités étant relativement longues, nous ne les donnerons pas ici. Ce texte se divisera donc en deux parties : la première contenant les hypothèses et les notations, la seconde les résultats.

1. Notations.

Dans tout ce papier, ℓ est un nombre premier impair, et n un entier positif. On s'intéresse aux extensions cycliques $k/\underset{\sim}{Q}$ du corps $\underset{\sim}{Q}$ des rationnels dont le degré divise $(\ell - 1)\ell^{n-1}$ et qui vérifient les deux conditions suivantes :

(a) le corps k ne contient pas de racines ℓ-ièmes de l'unité non triviale ;

(b) si ℓ est sauvagement ramifié dans $k/\underset{\sim}{Q}$, alors le complété $\hat{k}$ de k au-dessus de ℓ (i. e. en une place de k divisant ℓ) ne contient pas de racines ℓ-ièmes de l'unité non triviales (un moyen simple de réaliser cette condition est de supposer que $\ell - 1$ ne divise pas le degré de $k/\underset{\sim}{Q}$ lorsque ℓ est sauvagement ramifié).

On désigne par ζ une racine primitive ℓ^n-ième de l'unité, par k' le corps $k(\zeta)$, par G et G' les groupes de Galois de $k/\underset{\sim}{Q}$ et de $k'/\underset{\sim}{Q}$, par E et $\mathcal{H}$ le groupe des unités et le groupe des classes de k , et par $(\underset{\sim}{Z}/\ell^n \underset{\sim}{Z})^*$ le groupe multiplicatif de l'anneau des entiers modulo ℓ^n. Si Ψ est un homomorphisme de G dans $(\underset{\sim}{Z}/\ell^n \underset{\sim}{Z})^*$, on note $\mathcal{H}_\Psi$ le sous-groupe de $\mathcal{H}$ formé des classes h , telles que $h^{\ell^n} = 1$ et $\sigma(h) = h^{\Psi(\sigma)}$ pour tout $\sigma \in G$, et $E(\Psi)$ le sous-groupe de E formé des $e \in E$ vérifiant $\sigma(e)e^{-\Psi(\sigma)} \in E^{\ell^n}$ (E^{ℓ^n} = puissances ℓ^n-ièmes de E) pour tout $\sigma \in G$.

Pour tout $\sigma \in G'$, on définit $\theta(\sigma) \in (\underset{\sim}{Z}/\ell^n \underset{\sim}{Z})^*$ par l'égalité $\sigma(\zeta) = \zeta^{\theta(\sigma)}$. Si

Ψ est un homomorphisme de G dans $(\underset{\sim}{Z}/\ell^n \underset{\sim}{Z})^*$ et si $\sigma \in G'$, on pose

$$\overline{\Psi}(\sigma) = \Psi(\sigma^{-1}|_k)\ \theta(\sigma),$$

où $\sigma^{-1}|_k$ est la restriction de l'inverse de σ à k. L'application $\overline{\Psi}$ est un homomorphisme de G' dans $(\underset{\sim}{Z}/\ell^n \underset{\sim}{Z})^*$

On désigne par $\overline{k}$ le corps des invariants du noyau de $\overline{\Psi}$, par $\overline{G}$ le groupe de Galois de $\overline{k}/\underset{\sim}{Q}$, par $\overline{\mathcal{H}}$ le groupe des classes de $\overline{k}$, et par $\overline{\mathcal{H}}^{\overline{\Psi}}$ le quotient de $\overline{\mathcal{H}}$ par son sous-groupe engendré par les h^{ℓ^n} et les $\sigma(h)h^{-\overline{\Psi}(\sigma)}$, où h décrit $\overline{\mathcal{H}}$ et σ décrit $\overline{G}$. On voit que $\overline{k}/\underset{\sim}{Q}$ est une extension cyclique dont le degré divise $(\ell - 1)\ell^{n-1}$, et que $\overline{\mathcal{H}}^{\overline{\Psi}}$ est le plus grand quotient de $\overline{\mathcal{H}}$ annulé par ℓ^n sur lequel les éléments de $\sigma \in \overline{G}$ agissent comme l'élévation à la puissance $\overline{\Psi}(\sigma)$.

Enfin, nous aurons besoin de préciser quelques notations concernant les ℓ-groupes abéliens finis. Soit A un tel groupe, il est isomorphe à un produit $\prod_{i=1}^{t} (\underset{\sim}{Z}/\ell^{n_i} \underset{\sim}{Z})$; l'ensemble des n_i, pour $i = 1, \ldots, t$, est un invariant de A. Pour tout entier k, on appelle ℓ^k-rang de A et on note $r_k(A)$ le nombre des i tels que $n_i \geqslant k$.

2. Enoncé des résultats.

Les hypothèses et les notations sont celles introduites au § 1. On suppose de plus que l'homomorphisme Ψ est injectif. Pour énoncer les résultats nous devrons distinguer un cas spécial : nous dirons que l'on est dans le cas spécial si $\ell - 1$ divise le degré de $\overline{k}/\underset{\sim}{Q}$ et si ℓ est totalement décomposé dans le sous-corps de degré $\ell - 1$ de $\overline{k}$. On voit facilement que cela est équivalent au fait que le complété $\hat{k}$ de k au-dessus de ℓ contient un $\mu \neq 1$ tel que $\mu^\ell = 1$ et que, pour tout σ dans le groupe de décomposition de ℓ dans k, on ait $\sigma(\mu) = \mu^{\Psi(\sigma)}$ (En identifiant le groupe de décomposition de ℓ dans k avec le groupe de $\hat{k}/\underset{\sim}{Q}_\ell$).

On pose

$$e_j(\Psi) = r_j(E(\Psi)/E^{\ell^n}), \qquad r_j(\Psi) = r_j(\mathcal{H}_\Psi) \text{ et } R_j(\overline{\Psi}) = r_j(\overline{\mathcal{H}}^{\overline{\Psi}}) ;$$

on a alors le théorème suivant.

THÉORÈME 1. - Soit j un entier, $j \in \{1, \ldots, n\}$.

Si l'on n'est pas dans le cas spécial, alors

$$r_j(\Psi) + e_j(\Psi) \geqslant R_j(\overline{\Psi}) \geqslant r_j(\Psi) - 1$$

si ℓ n'est pas sauvagement ramifié dans k, et

$$r_j(\Psi) + e_j(\Psi) \geqslant R_j(\overline{\Psi}) \geqslant r_j(\Psi) - 2$$

sinon.

Si l'on est dans le cas spécial, alors

$$r_j(\Psi) + e_j(\Psi) + 1 \geqslant R_j(\overline{\Psi}) \geqslant r_j(\Psi) - 2 .$$

Ce théorème s'améliore dans deux cas particuliers ; Tout d'abord lorsque ℓ ne divise pas le degré de $k/\underset{\sim}{Q}$ (k est alors une extension cyclique de $\underset{\sim}{Q}$ dont le degré divise $\ell - 1$), on a le théorème suivant.

THÉORÈME 2. - Si $k/\underset{\sim}{Q}$ est une extension cyclique dont le degré divise $\ell - 1$, alors si l'on n'est pas dans le cas spécial, on a

$$-1 \leqslant r_j(\Psi) - R_j(\overline{\Psi}) \leqslant 0 \quad \text{si } k \text{ est réel}$$

et

$$0 \leqslant r_j(\Psi) - R_j(\overline{\Psi}) \leqslant 1 \quad \text{si } k \text{ est complexe.}$$

Si l'on est dans le cas spécial, on a

$$-2 \leqslant r_j(\Psi) - R_j(\overline{\Psi}) \leqslant 1 \quad \text{si } k \text{ est réel}$$

et

$$-1 \leqslant r_j(\Psi) - R_j(\overline{\Psi}) \leqslant 2 \quad \text{si } k \text{ est complexe.}$$

Enfin, si le degré de $k/\underset{\sim}{Q}$ est égal à ℓ (on ne peut pas être alors dans le cas spécial, et $\hat{k}$ ne peut pas contenir de racines ℓ-ièmes non triviales de l'unité), on a le résultat ci-après.

THÉORÈME 3. - Si $k/\underset{\sim}{Q}$ est une extension cyclique de degré ℓ, alors

$$r_j(\Psi) + 1 \geqslant R_j(\overline{\Psi}) \geqslant r_j(\Psi) - 1$$

si ℓ n'est pas ramifié dans k, et

$$r_j(\Psi) + 1 \geqslant R_j(\overline{\Psi}) \geqslant r_j(\Psi) - 2$$

sinon.

Remarque 1. - Dans le cas du théorème 3, on peut voir que quel que soit n et quel que soit Ψ, le groupe $\mathcal{H}_\Psi$ est le groupe des classes ambiges de k. Les $r_j(\Psi)$ pour $j > 1$ sont donc nuls, et le $r_1(\Psi)$ est donné par la formule de Chevaley. Le théorème 3 donne alors de bonnes informations sur $R_j(\overline{\Psi})$.

Remarque 2. - L'hypothèse d'injectivité de Ψ est indispensable dans nos théorèmes lorsque ℓ divise le degré de $k/\underset{\sim}{Q}$. En effet, si l'on supprimait cette hypothèse, on pourrait appliquer ces théorèmes avec $n = 1$ et $\Psi = 1$ (i. e. $\Psi(\sigma) = 1 \in (\underset{\sim}{Z}/\ell)^*$ pour tout $\sigma \in G$). Le groupe $\mathcal{H}_\Psi$ serait alors le groupe des classes ambiges de k. Il en résulterait que l'on peut avoir $r_1(\Psi)$ arbitrairemant grand en choisissant bien k. D'autre part, le corps $\overline{k}$ serait alors le corps des racines ℓ-ièmes de l'unité et donc $R_1(\overline{\Psi})$ est une constante indépendante de k. On ne peut donc pas avoir d'inégalité du type $R_j(\overline{\Psi}) \geqslant r_j(\Psi) - c$, où c est une constante.

BIBLIOGRAPHIE

[1] LEOPOLDT (H.-W.). - Zur Struktur der ℓ-Klassengruppe galoisscher Zahlkörper, J. für reine und angew. Math., t. 199, 1958, p. 165-174.

[2] SCHOLTZ (A.). - Über die Beziehung der Klassenzahlen quadratischer Körper zueinander, J. für reine und angew. Math., t. 166, 1932, p. 201-203.

(Texte reçu le 14 mars 1977)

Philippe SATGÉ
UER de Sciences
Département de Mathématiques
Université de Caen
14032 CAEN CEDEX

NOTE ajoutée à la correction des épreuves [Juin 1977]. - Depuis la rédaction de ce travail, ces résultats ont été généralisés par Bernard ORIAT. Les nouveaux résultats seront publiés dans un article rédigé en commun par ORIAT et moi-même. Cet article contiendra les démonstrations de tout ce qui est annoncé ici.