Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Geneviève Cazes

Sur le nombre de classes d'idéaux de certains corps de nombres

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 10, nº 1 (1968-1969), exp. nº 4, p. 1-6
<http://www.numdam.org/item?id=SDPP_1968-1969__10_1_A3_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
10e année, 1968/69, n° 4, 6 p.

16 décembre 1968

SUR LE NOMBRE DE CLASSES D'IDÉAUX DE CERTAINS CORPS DE NOMBRES

par Geneviève CAZES

Soient K un corps de nombre (i. e. une extension finie de $\mathbb{Q}$), et A_K la fermeture de $\mathbb{Z}$ dans K. A_K est un anneau de Dedekind ; les idéaux fractionnaires de A_K sont dits, par définition, idéaux de K. Le groupe de classes d'idéaux C_K de K (i. e. les idéaux de K modulo les idéaux principaux $\neq 0$ de K) est fini. La détermination de son ordre h_K est un problème non résolu : en particulier, elle peut servir à résoudre le premier cas du théorème de Fermat.

Le premier cas du théorème de Fermat dit qu'il n'y a pas de solutions à l'équation $x^n + y^n = z^n$ parmi les entiers non divisibles par n. Si $h_{\mathbb{Q}(\zeta_n)}$ désigne le nombre de classes du corps cyclotomique $\mathbb{Q}(\zeta_n)$, où ζ_n est une racine primitive n-ième de l'unité, KUMMER a démontré que, si $n \nmid h_{\mathbb{Q}(\zeta_n)}$, alors le premier cas du théorème de Fermat est vrai pour n.

Or on a pu écrire $h_{\mathbb{Q}(\zeta_n)}$ sous la forme $h_1 h_2$, où h_2 est le nombre de classes du corps $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, plus grand sous-corps réel de $\mathbb{Q}(\zeta_n)$. KUMMER montre alors que si $n \nmid h_1$, alors $n \nmid h_{\mathbb{Q}(\zeta_n)}$, donc que le premier cas du théorème de Fermat est vrai. Nous allons donner ici un résultat différent, noté (A), contenu dans l'article de YOKOYAMA ([3]) : Si n est de la forme p^m, où p est un nombre premier, alors p divise $h_{\mathbb{Q}(\zeta_n)}$ si, et seulement si, p divise h_1.

Les résultats connus jusqu'ici donnent, soit des <u>formules</u> pour h_K en fonction des grandeurs liées au corps K (h_K est connu pour K extension quadratique ou cyclotomique de $\mathbb{Q}$, en utilisant la fonction ζ de Dedekind du corps K ; voir [1]), soit des <u>ordres de grandeur</u> de h_K [$(\log h_K R_K)/(\log \sqrt{|D_K|}) \to 1$ quand $|D_K| \to \infty$, où R_K (resp. D_K) est le régulateur (resp. le discriminant) du corps K ; voir [1] pour les définitions], soit encore des <u>relations</u>, le plus souvent de divisibilité, entre h_K et h_L si L est une extension de K. La recherche des corps euclidiens de faible degré (ce qui entraînerait $h_K = 1$ pour ces corps, donc des propriétés arithmétiques intéressantes pour ces corps) est aussi ouverte. De même, s'il existe une infinité de corps de faible degré (par exemple, quadratiques réels) dont le h correspondant soit divisible par un nombre donné, aussi grand que l'on veut.

Avant d'établir (A), prouvons quelques préliminaires :

THÉORÈME 1. - *Soient* k *un corps de nombres, et* E *une extension finie de* k, *telle qu'il n'y ait pas d'extension abélienne non ramifiée non triviale entre* k *et* E, *alors* h_k *divise* h_E.

Preuve. - Nous utiliserons ici un résultat très utile pour la recherche de h_k : h_k est le degré de l'extension $\bar{k}/k$, où $\bar{k}$ est l'extension abélienne maximale non ramifiée de k (voir [2], ou un exposé sur la théorie des corps de classes dans le groupe d'études de théorie des nombres, de cette année).

Considérons la situation

$$\begin{array}{ccc} \bar{k} & \text{———} & E\bar{k} \\ | & & | \\ k & \text{———} & E \end{array} ,$$

où E est une extension finie de k telle que $E \cap \bar{k} = k$, alors l'extension $E\bar{k}/E$ est aussi abélienne et non ramifiée, de même degré que $\bar{k}/k$ comme il est facile de le voir : $E\bar{k}$ est donc un sous-corps de $\bar{E}$, donc le degré de $E\bar{k}$ sur E, égal à h_k, divise celui de $\bar{E}$ sur E, égal à h_E. Or les conditions de l'énoncé entraînent bien $E \cap \bar{k} = k$, puisque $\bar{k} \cap E$ est la plus grande sous-extension de E contenant k abélienne et non ramifiée.

C. Q. F. D.

Remarque. - Les conditions du théorème sont vérifiées, en particulier si E est une extension (non abélienne, ou ramifiée de k), de degré premier.

THÉORÈME 2. - *Soient* E *et* F *des extensions finies de* k, *telles que* $E \cap F = k$. *Soit* p *un nombre premier au degré de* F/k. *S'il n'y a pas d'extension abélienne non ramifiée non triviale entre* F *et* EF, *alors*

$$\frac{h_{F,p}}{h_{k,p}} \leqslant \frac{h_{EF,p}}{h_{E,p}} .$$

Nota. - $h_{K,p}$ désigne la plus haute puissance de p contenue dans la décomposition de h_K en facteurs premiers. Elle est presque partout égale à 1 lorsque p varie.

Preuve. - Elle repose sur le fait suivant : Si K est une extension finie de k, nous disposons, pour comparer h_k et h_K, de l'application canonique i de A_k dans A_K qui, à l'idéal I de k, fait correspondre l'idéal IA_K de K, et de l'application norme N de A_K dans A_k. i et N sont des applications respectivement de C_k dans C_K, et de C_K dans C_k ; elles ne sont ni injectives ni surjectives. En réduisant leur domaine de définition dans k et dans K, on va rendre l'une injective, l'autre surjective.

Supposons $[K:k] = n$; soit p premier à n ; soit $\mathfrak{C}_k$ (resp. $\mathfrak{C}_K$) le p-sous-groupe de Sylow de C_k (resp. C_K), appelé le " p-groupe de classe de k " (resp. "de K "). Alors i est une application injective de $\mathfrak{C}_k$ dans $\mathfrak{C}_K$ (en effet, si $\overline{\mathfrak{A}} \in \mathfrak{C}_k$, $i(\overline{\mathfrak{A}}) \in \mathfrak{C}_K$, et si $i(\overline{\mathfrak{A}}) = 1$ dans $\mathfrak{C}_K$, alors $N[i(\mathfrak{A})] = \mathfrak{A}^n = 1$ d'une part, et $\mathfrak{A}^{p^{n'}} = 1$ d'autre part, puisque $\overline{\mathfrak{A}}$ appartient à p-sous-groupe de Sylow de C_k. Comme $(p, n) = 1$, on a $\mathfrak{A} = 1$).

De même, N est une application surjective de $\mathfrak{C}_K$ dans $\mathfrak{C}_k$ [en fait, $N[i(\mathfrak{C}_k)]$ suffit à recouvrir $\mathfrak{C}_k$, car, quand $\overline{\mathfrak{A}}$ parcourt $\mathfrak{C}_k$, alors $\overline{N[i(\mathfrak{A})]} = \overline{\mathfrak{A}}^n$ parcourt aussi $\mathfrak{C}_k$, puisque $\mathfrak{C}_k$ est un p-groupe et que $(n, p) = 1$]. On montre facilement qu'en fait $\mathfrak{C}_K = i(\mathfrak{C}_k) \times \mathfrak{R}_{K/k}$ (produit direct, où $\mathfrak{R}_{K/k}$ désigne le noyau de N : en effet, $i(\mathfrak{C}_k) \cap \mathfrak{R}_{K/k} = \{1\}$, car si $\overline{\mathfrak{A}} \in i(\mathfrak{C}_k) \cap \mathfrak{R}_{K/k}$, $N(\mathfrak{A}) = \mathfrak{A}^n = 1$, d'où $\mathfrak{A} = 1$ et $\dfrac{\mathfrak{C}_K}{\mathfrak{R}_{K/k}} \simeq \mathfrak{C}_k$, puisque N est surjective ; donc $\mathfrak{C}_K$ est le produit de $i(\mathfrak{C}_k)$ et de $\mathfrak{R}_{K/k}$. Tous les groupes considérés ici sont <u>finis</u>).

Plaçons-nous alors dans la situation de l'énoncé :

$$\begin{array}{ccc} F & \text{———} & EF \\ | & & | \\ k & \text{———} & E \end{array} .$$

Nous avons :

$$\left.\begin{array}{l} h_{F,p} = \text{ordre de } \mathfrak{C}_F \\ \\ h_{k,p} = \text{ordre de } \mathfrak{C}_k \end{array}\right\}, \qquad \text{donc } \frac{h_{F,p}}{h_{k,p}} = \text{ordre de } \mathfrak{R}_{F/k} ,$$

d'après ce qui précède. De même,

$$\frac{h_{EF,p}}{h_{E,p}} = \text{ordre de } \mathfrak{R}_{EF/E} ,$$

si p est premier au degré de $\frac{F}{k}$ (ce qui entraîne, p premier au degré de $\frac{EF}{E}$, car puisque $E \cap F = k$, on a degré $\frac{EF}{E}$ = degré $\frac{F}{k}$). Or il est facile de voir (avec des notations évidentes) que

$$N_{EF/F}(i(\mathfrak{C}_E)) = i'(\mathfrak{C}_h)$$

et

$$N_{EF/F}(\mathfrak{K}_{K/E}) \subset \mathfrak{K}_{F/k} \quad .$$

Pour montrer que l'ordre de $\mathfrak{K}_{F/k}$ est inférieur ou égal à celui de $\mathfrak{K}_{EF/E}$, il suffit de montrer que $N_{EF/F}$ est surjective de $\mathfrak{K}_{EF/E}$ dans $\mathfrak{K}_{F/k}$. Elle le sera si elle est déjà surjective de C_{EF} dans C_F . Or l'ordre de $\dfrac{C_F}{N_{EF/F}\, C_K}$ est égal au degré de l'extension abélienne maximale non ramifiée de F contenue dans EF (résultat de la théorie des corps de classe ; voir [2], ou l'exposé au groupe d'études). Donc il vaut 1 .

C. Q. F. D.

Montrons encore un résultat qui nous servira pour démontrer (A) :

THÉORÈME 3. - Soit K une extension de Galois de degré p^a de k , telle qu'il existe un seul idéal premier de k qui soit ramifié pour K/k . Alors si $p \mid h_K$, $p \mid h_k$.

Nota. - On sait déjà que si cet idéal était pleinement ramifié, alors $h_k \mid h_K$. La condition donnée revient à dire que le discriminant de K sur k est une puissance d'un seul idéal premier.

Preuve. - Elle utilise essentiellement les propriétés des p-groupes et le fait que le degré de ramification d'un idéal premier p de k dans une extension de Galois K/k est égal à l'ordre d'un groupe d'inertie $T_{\mathfrak{P}}$, sous-groupe du groupe de Galois $G(K/k)$, où $\mathfrak{P}$ est un idéal premier de K au-dessus de p .

En effet, soit $\overline{K}_p$ le sous-corps de $\overline{K}$, corps de classe de Hilbert de $\overline{K}$, tel que $G\left(\frac{\overline{K}_p}{K}\right)$ soit le plus grand p-groupe contenu dans $G\left(\frac{\overline{K}}{K}\right)$. L'ordre de $G\left(\frac{\overline{K}_p}{K}\right)$ est égal à $h_{K/p}$. Dire que $p \mid h_K$ revient à dire que $\overline{K}_p - K$ est une extension de degré p^b avec $b > 0$. On a alors la situation suivante :

$$\begin{array}{ccc} & & \overline{K}_p \\ & & \Big| \, p^b \\ k_p & \xrightarrow[p^a]{\qquad} & K \end{array} \quad .$$

Soient p le premier de k ramifié pour K/k, et $\mathfrak{P}$ un idéal premier de $\overline{K}_p$ au-dessus de p. Comme l'extension $\overline{K}_p/K$ est non ramifiée, p est le seul premier de k ramifié dans $\overline{K}_p$, et le cardinal de $T_{\mathfrak{P}}$ est inférieur ou égal au degré de K/k, donc $T_{\mathfrak{P}}$ est un sous-groupe d'indice strictement supérieur à p dans $G\left(\frac{\overline{K}_p}{k}\right)$. Tous les autres groupes d'inertie de G sont, soit l'identité, soit un conjugué de $T_{\mathfrak{P}}$ pour les idéaux premiers p' au-dessus de p. Or $G\left(\frac{\overline{K}_p}{k}\right)$ est un p-groupe d'ordre p^{a+b}. Donc $T_{\mathfrak{P}}$ est contenu dans un sous-groupe $\mathfrak{h}$ normal maximal de G d'indice p, et tous les autres groupes d'inertie de G sont contenus dans $\mathfrak{h}$. Si on considère le corps F qui correspond au sous-groupe $\mathfrak{h}$ de G, tous les groupes d'inertie de F sont nuls (car égaux à $\frac{T_{\mathfrak{P}}\,\mathfrak{h}}{\mathfrak{h}} = 1$), donc F est une extension non ramifiée de k, abélienne et de degré p, car $\frac{G}{\mathfrak{h}}$ est de degré p, donc abélien. F est donc contenue dans $\overline{k}_p$ qui est donc une extension non triviale de k, donc $p \mid h_k$.

Nous pouvons maintenant montrer le théorème (A).

THÉORÈME (A). - Soit le corps cyclotomique $\mathbb{Q}(\zeta_n)$, où ζ_n est une racine primitive n-ième de l'unité, avec $n = p^m$, où p est un nombre premier. Soit $h_{\mathbb{Q}(\zeta_n)}$ le nombre de classes d'idéaux du corps $\mathbb{Q}(\zeta_n)$, qui est égal à $h_1\, h_2$, où h_2 est le nombre de classes du corps $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = K$. Alors p divise $h_{\mathbb{Q}(\zeta_n)}$ si, et seulement si, p divise h_1.

Preuve. - Il est facile de voir que $\mathbb{Q}(\zeta_n)$ est une extension quadratique de K, donc $h_1 = h_{\mathbb{Q}(\zeta_n)}/h_K$ est un nombre entier (remarque du théorème 1). Si p divise h_1, alors p divise $h_{\mathbb{Q}(\zeta_n)}$ évidemment. Réciproquement, supposons que p divise $h_{\mathbb{Q}(\zeta_n)}$. Soit le corps cyclotomique $\mathbb{Q}(\zeta_p)$, où ζ_p est une racine primitive p-ième de l'unité. On sait que $\mathbb{Q}(\zeta_n)$ est une extension de degré p^{m-1} de $\mathbb{Q}(\zeta_p)$, et qu'il y a un seul idéal de $\mathbb{Q}(\zeta_p)$, ramifié dans $\mathbb{Q}(\zeta_n)$ (à savoir celui qui est au-dessus de l'idéal (p) de $\mathbb{Q}$). D'après le théorème 3, p divise $h_{\mathbb{Q}(\zeta_p)}$. Un théorème de Kummer affirme alors que p divise $h_{\mathbb{Q}(\zeta_p)}/h_{K_p}$, où K_p désigne le plus grand sous-corps réel de $\mathbb{Q}(\zeta_p)$. Si nous considérons la situation suivante :

$$\begin{tikzcd}[arrows=dash]
\mathbb{Q}(\zeta_p) \arrow[r, "p^{m-1}"] \arrow[d, "2"'] & \mathbb{Q}(\zeta_{p^m}) \arrow[d, "2"] \\
K_p \arrow[r] & K
\end{tikzcd} \quad ,$$

il est facile de vérifier qu'elle vérifie toutes les hypothèses du théorème 1, avec $p \neq 2$, pour que p soit premier au degré de $\underset{\sim}{Q}(\zeta_p)$ sur K_p (on prend $k = K_p$, $E = K$, et $F = \underset{\sim}{Q}(\zeta_p)$). Donc p divise $h_{\underset{\sim}{Q}(\zeta_{p^m})}/h_K$.

C. Q. F. D.

Le cas $p = 2$ s'examine à part ; on trouve que 2 ne divise pas $h_{\underset{\sim}{Q}(\zeta_n)}$, donc l'énoncé du théorème reste vrai pour $p = 2$.

Remarque. - Le théorème peut se généraliser à une extension de Galois L de degré $p^m(p-1)$ sur $\underset{\sim}{Q}$, qui contient $\underset{\sim}{Q}(\zeta_p)$, et telle qu'un seul premier de $\underset{\sim}{Q}(\zeta_p)$ soit ramifié dans L, et même totalement ramifié. Alors p divise h_L si, et seulement si, p divise $\frac{h_L}{h_K}$, où K est le plus grand sous-corps réel de L.

BIBLIOGRAPHIE

[1] BOREVIČ (Z. I.) et SAFAREVIČ (I. R.). - Théorie des nombres. - Paris, Gauthier-Villars, 1967 (Monographies internationales de Mathématiques modernes, 8).

[2] Algebraic number theory. Edited by CASSELS (J. W. S.) and FRÖHLICH (A.). - London, Academic Press ; Washington, Thompson Book Company, 1967.

[3] YOKOYAMA (Akio). - On the relative class number of finite algebraic number fields, J. of Math. Soc. of Japan, t. 19, 1967, p. 179-184.

(Texte remis le 23 juillet 1969)

Mlle Geneviève CAZES
Ass. Fac. Sc. Paris
12 rue du Commandeur
75 - PARIS 14