MÉMOIRES DE LA S. M. F.

MARIE-NICOLE GRAS

Nombre de classes, unités et bases d'entiers des extensions cubiques cycliques de Q

Mémoires de la S. M. F., tome 37 (1974), p. 101-106

<http://www.numdam.org/item?id=MSMF_1974__37__101_0>

Journées arithmétiques
Bull. Soc. math. France,
Mémoire 37, 1974, p. 101-106

NOMBRE DE CLASSES, UNITES ET BASES D'ENTIERS DES EXTENSIONS CUBIQUES CYCLIQUES DE $\mathbb{Q}$

par

Marie Nicole GRAS

-:-:-:-

Soit K un corps cubique cyclique. Nous établissons un algorithme permettant de déterminer le nombre de classes h de K et un générateur ε du groupe E des unités de norme 1 de K, à partir de la seule connaissance d'un générateur du groupe des unités cyclotomiques de K. La connaissance du groupe des unités permet aussi une étude de l'existence des bases d'entiers de la forme $\{1, \vartheta, \vartheta^2\}$. L'utilisation d'un ordinateur nous a permis de dresser des tables, dont une donnant le nombre de classes et les unités pour les corps de conducteur inférieur à 4000. Ces méthodes faisant l'objet de publications ([2] et [3]), nous ne donnerons ici que les principaux résultats.

I. NOTATIONS ET RAPPELS.

Soit K une extension cubique cyclique de $\mathbb{Q}$ de conducteur m ; son discriminant est égal à m^2. Soit A l'anneau des entiers de K et soit σ un générateur de $G = \mathrm{Gal}(K/\mathbb{Q})$. Soit n le nombre de diviseurs premiers du discriminant de $K/\mathbb{Q}$; on posera $m = p_1 \ldots p_n$, en convenant que $p_n = 9$ si 3 est ramifié dans $K/\mathbb{Q}$. Avec ces notations, m se met dans tous les cas sous la forme $m = \frac{a^2+27b^2}{4}$; en choisissant $b > 0$, $a \equiv 1 \ (3)$ si $m \equiv 1 \ (3)$, $a = 3a'$, $a' \equiv 1 \ (3)$ sinon, le couple (a,b) est associé à un corps K unique et réciproquement.

Soit E le groupe des unités de norme 1 de K ; soit $j = \frac{-1+\sqrt{-3}}{2}$; E est un $\mathbb{Z}[j]$-module libre de dimension 1, l'opération étant définie par $\psi^j = \psi^\sigma$, $\psi \in E$. Soit ε un générateur de E. Soit E' le groupe des unités cyclotomiques de norme 1 de K ; c'est un sous-$\mathbb{Z}[j]$-module dont on notera $\eta = \varepsilon^{\lambda+\mu\sigma}$; $\lambda, \mu \in \mathbb{Z}$ un générateur. On sait que K se plonge dans $\mathbb{Q}^{(m)}$ et que η s'obtient comme norme relative de l'unité cyclotomique de $\mathbb{Q}^{(m)}$ ([4]).

Pour toute unité $\psi \in E$, on notera $R(\psi)$ le régulateur de ψ. On sait que le nombre de classes h de K est égal à l'indice de E' dans E, c'est-à-dire que $h = \frac{R(\eta)}{R(\varepsilon)} = \lambda^2 - \lambda\mu + \mu^2$.

II. NOMBRE DE CLASSES ET UNITES.

a) Détermination de E'.

Soit $m = p_1 \ldots p_n$; il y a 2^{n-1} corps cubiques K de conducteur m et on peut représenter les 2^{n-1} groupes de Galois des extensions $\mathbb{Q}^{(m)}/K$ par les 2^{n-1} groupes d'entiers modulo m suivants :

$$H = \mathcal{G}^3 \times \langle g_1 g_2^{r_1}, g_2 g_3^{r_2}, \ldots, g_{n-1} g_n^{r_{n-1}} \rangle \quad , \quad \text{où}$$

g_i est d'ordre $\varphi(p_i)$ modulo m (φ : fonction d'Euler),

$g_i \equiv 1$ modulo $\prod_{j \neq i} p_j$,

$r_i = 1$ ou 2,

et où $\mathcal{G} = \{\prod_{i=1}^{n} g_i^{x_i}$, $1 \leq x_i \leq \varphi(p_i)\}$ représente $\mathrm{Gal}(\mathbb{Q}^{(m)}/\mathbb{Q})$.

On en déduit numériquement :

(i) les valeurs de a et b associées à chaque corps K ;

(ii) un générateur η du groupe des unités cyclotomiques de norme 1 de chaque corps K (d'après H. HASSE ([4])) : $\eta = \prod_{x \in H'} \frac{\sin \pi \frac{g_1 x}{m}}{\sin \pi \frac{x}{m}}$, où $H' \subset H$ correspond à $\mathrm{Gal}(\mathbb{Q}_o^{(m)}/K)$.

b) Majoration du nombre de classes h de K.

Théorème 1. *Soit $\psi \in E$ et soit r l'indice dans E du sous $\mathbb{Z}[j]$-module engendré par ψ ; alors*

$$r \leq \frac{16}{3} \frac{R(\psi)}{\mathrm{Log}^2 \frac{m-3}{3}} .$$

Corollaire. *Le nombre de classes h de K vérifie l'inégalité :*

$$h \leq \frac{16}{3} \frac{R(\eta)}{\mathrm{Log}^2 \frac{m-3}{3}} .$$

c) "Dévissage" de η .

Soit p un nombre premier, soit f son degré résiduel dans $\mathbb{Q}(j)/\mathbb{Q}$ et soit $q = p^f$; nous rappelons que $p|h$ si et seulement si $q|h$. Si $q > \frac{16}{3}R(\eta)/\log^2 \frac{m-3}{3}$, alors p ne divise pas h ; sinon, soient ω et ω' deux entiers de $\mathbb{Q}(j)$, complexes conjugués, de norme q (si $f = 2$, $\omega = \omega' = p$) ; une méthode nous permet de tester numériquement s'il existe une unité $\varphi \in E$ telle que $\eta = \varphi^{\omega''}$ ($\omega'' = \omega$ ou ω') : dans ce cas q divise h ; sinon q ne divise pas h . Lorsque q divise h , la recherche des diviseurs de h/q se fait au moyen du même critère, à partir de l'unité φ et du majorant $\frac{16}{3} R(\varphi)/\log^2 \frac{m-3}{3}$. Cette méthode permet de déterminer tous les diviseurs premiers de h avec leur ordre de multiplicité. Un générateur ε de E est la dernière unité φ obtenue.

d) Relation entre les "classes ambiges" de K .

La connaissance d'un générateur ε de E permet de déterminer la relation entre les "classes ambiges" de K (cf. [1]). En effet, d'après le théorème 90 de Hilbert, $\varepsilon = \rho^{1-\sigma}$, $\rho = 1+\varepsilon+\varepsilon\varepsilon^{\sigma}$; (ρ) est un idéal ambige qui peut donc s'écrire $(\rho) = q \prod \mathfrak{p}_i^{x_i}$, $q \in \mathbb{Q}$, $\mathfrak{p}_i$ idéal 1er au-dessus de p_i ; les x_i ne sont pas tous congrus à zéro modulo 3, sinon ε ne serait pas un générateur de E ; ceci donne la relation cherchée.

e) Résultats numériques.

Nous avons établi des tables donnant le nombre de classes de tous les corps cubiques cycliques de conducteur $m < 4000$, ainsi que des tables partielles, pour $4000 < m < 20000$. Donnons un aperçu des résultats obtenus :

(i) Il y a 630 corps cubiques cycliques de conducteur $m < 4000$; parmi eux, il y a :

272 corps de conducteur $m = p_1$ (alors $h \equiv 1(3)$) et $h = 1$ pour 230 d'entre eux,

310 corps de conducteur $m = p_1 p_2$ (alors $h \equiv 0(3)$) et $h = 3$ pour 249 d'entre eux,

48 corps de conducteur $m = p_1 p_2 p_3$ (alors $h \equiv 0(9)$) et $h = 9$ pour 43 d'entre eux.

(ii) Les corps dont un générateur ε de E est totalement positif sont assez rares. Il y en a cinq pour des conducteurs $m < 4000$: ce sont les corps définis par : $m = 19\cdot37$ $(a = 25\ ,\ b = 9)$, $m = 9\cdot79$ $(a = 12\ ,\ b = 10)$, $m = 1009$, $m = 1699$ et $m = 31\cdot103$ $(a = 55\ ,\ b = 19)$.

(iii) Exemples :

a) $m = 4867 = 31\cdot157$, $a = 136$, $b = 6$, $\frac{16}{3} R(\eta)/\log^2 \frac{m-3}{3}$ a pour partie entière 942 ; $h = 228 = 3\cdot4\cdot19$ et $\eta = \varepsilon^{-14+2\sigma}$.

b) $m = 7351$ $\quad h = 49$ $\quad \eta = \varepsilon^{(3+2\sigma)^2}$

$m = 8563$ $\quad h = 49$ $\quad \eta = \varepsilon^{(3+2\sigma)^2}$

$m = 10267$ $\quad h = 49$ $\quad \eta = \varepsilon^{7}$

$m = 18367$ $\quad h = 49$ $\quad \eta = \varepsilon^{(3+2\sigma)^2}$.

II. EXISTENCE DES $\mathbb{Z}$-BASES D'ENTIERS DE LA FORME $\{1,\vartheta,\vartheta^2\}$.

L'anneau des entiers A d'un corps cubique sera dit monogène s'il existe une $\mathbb{Z}$-base d'entiers de la forme $\{1,\vartheta,\vartheta^2\}$ ([5]) .

a) Principaux résultats. (Pour les démonstrations se reporter à [3]).

Théorème 2. Soit K un corps cubique cyclique de conducteur $m = \frac{a^2+27b^2}{4}$. L'anneau des entiers de K est monogène si et seulement si l'équation diophantienne en $u,v \in \mathbb{Z}$,

$$bu(u^2-9v^2) + av(u^2-v^2) = 1 \tag{1}$$

admet une solution.

Théorème 3. Soit K un corps cubique cyclique de conducteur m . L'anneau des entiers de K est monogène si et seulement si K possède une unité w de norme 1 vérifiant les conditions :

(i) $\mathrm{Tr}_{K/\mathbb{Q}}(w+w^{-1}) = 3$,

(ii) $\mathrm{Tr}_{K/\mathbb{Q}}(\frac{w^2-w^{-1}}{m})$ est le cube d'un entier rationnel γ .

Théorème 4. Soit m un conducteur ; il existe un corps K cubique cyclique de conducteur m dont l'anneau des entiers est monogène, si et seulement si m est de la forme $m = \frac{\alpha^2+27}{4\gamma^3}$, $\alpha,\gamma \in \mathbb{Z}$, $\alpha \not\equiv \pm 9 \ (27)$. Lorsque cette condition est réalisée, K est le corps de décomposition du polynôme $X^3 - \frac{\alpha-3}{2}X^2 - \frac{\alpha+3}{2}X - 1$.

Conditions nécessaires pour que A soit monogène. On définit le corps K par a et b $(m = \frac{a^2+27b^2}{4})$ et, si ε est un générateur de E , on pose $t = Tr_{K/\mathbb{Q}}(\varepsilon)$, $s = Tr_{K/\mathbb{Q}}(\varepsilon^{-1})$. Chacune des conditions suivantes est une condition nécessaire de monogénéité (cf. [5] pour 1,3,4) :

1) a et b sont impairs ;
2) si $a \equiv 0 \ (3)$, alors $b \equiv \pm 1 \ (9)$ $(b>0)$,
   si $b \equiv 0 \ (3)$, alors $a \equiv 1 \ (9)$ $(a \equiv 1 (3))$;
3) la relation entre les idéaux ambiges de K est $\mathfrak{p}_1 \ldots \mathfrak{p}_n \sim (1)$;
4) ε non totalement positif ;
5) $s+t$ est impair ;
6) $s+t+3 \equiv 0 \ (m)$.

b) Résultats numériques.

Les résultats numériques proviennent essentiellement de l'étude de l'équation diophantienne

$$bu(u^2-9v^2) + av(u^2-v^2) = 1 \ . \tag{1}$$

En recherchant des formes de a et b pour lesquels cette équation admet nécessairement une solution en (u,v) , on démontre le résultat suivant :

Proposition. Les corps cubiques cycliques dont le conducteur m est de la forme $\frac{(b^2-8)^2+27b^2}{4}$ ou $m = \frac{(1-8b^2)^2+27b^2}{4}$, b impair, admettent une $\mathbb{Z}$-base d'entiers $\{1,\vartheta,\vartheta^2\}$.

En se donnant u et v et en cherchant si l'équation (1) admet des solutions en a et b telles que $m = \frac{a^2+27b^2}{4}$ soit un conducteur, on obtient un procédé qui nous a permis de trouver 24 corps de conducteur $m < 10\,000$, admettant une base d'entiers de la forme $\{1,\vartheta,\vartheta^2\}$ et autres que les 101 corps dont le conducteur est de la forme $\frac{a^2+27}{4}$ ou $\frac{1+27b^2}{4}$, lesquels admettent trivialement une telle base. Donnons la liste de ces 24 corps qui ont été obtenus

en faisant parcourir à u et v les valeurs entières telles que u^2+3v^2 soit inférieur à 100000.

m	a	b	m	a	b	m	a	b
241	-17	5	1381	31	13	31.163	-77	23
373	13	7	7.229	43	13	9.613	111	9
379	-29	5	1879	73	9	13.457	-83	25
463	-23	7	2539	-83	11	7.883	-71	27
751	-41	7	9.307	57	17	7621	-161	13
19.61	37	11	2797	-89	11	7.31.37	97	29
1213	-17	13	19.211	-113	11	7.13.97	-125	27
1321	-71	3	37.109	43	23	13.19.37	103	31

Nous ne savons pas s'il existe d'autres corps de conducteur $m < 10000$ et admettant une $\mathbb{Z}$-base d'entiers de la forme $\{1,\vartheta,\vartheta^2\}$. Une telle étude ne peut se faire qu'en étudiant l'équation (1) au moyen des méthodes de Baker.

-:-:-:-

BIBLIOGRAPHIE

[1] - C. CHEVALLEY - La théorie du corps de classes dans les corps finis et les corps locaux (Thèse), Journal of the Faculty of Science, Tokyo (1933).

[2] - M.N. GRAS - Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$ (à paraître au Journal de Crelle).

[3] - M.N. GRAS - Extensions cubiques cycliques de $\mathbb{Q}$ dont l'anneau des entiers est monogène. Ann. Fac. Sc., Besançon, 1973.

[4] - H. HASSE - Über die Klassenzahl abelscher Zahlkörpern, Chapitre I et II, Berlin (1952).

[5] - J.J. PAYAN - Sur les classes ambiges et les ordres monogènes d'une extension cyclique de degré premier impair sur $\mathbb{Q}$ ou sur un corps quadratique imaginaire (à paraître à Arkiv för mathematik).

-:-:-:-

Marie-Nicole GRAS
Institut de Mathématiques Pures
Laboratoire associé au CNRS n°188
BP 116 38402 - ST MARTIN D'HERES