MÉMOIRES DE LA S. M. F.

MARIE-NICOLE GRAS

Calcul de nombres de classes par dévissage des unités cyclotomiques

Mémoires de la S. M. F., tome 49-50 (1977), p. 109-112

<http://www.numdam.org/item?id=MSMF_1977__49-50__109_0>

Calculateurs en Math. (1975 - LIMOGES)
Bull. Soc. math France
Mémoire 49-50, 1977, p. 109-112

CALCUL DE NOMBRES DE CLASSES PAR DEVISSAGE DES UNITES CYCLOTOMIQUES

par Marie-Nicole GRAS

INTRODUCTION -

Cet exposé est la partie pratique d'un travail en commun avec Georges GRAS [2]

Le calcul du nombre de classes par dévissage des unités cyclotomiques se fait dans le cas abélien réel en partant de la formule du nombre de classes de Leopoldt [4]. Les calculs se simplifient dans le cas cyclique de degré premier et nous n'exposeront les résultats que dans ce cas là. On trouvera dans [2] le détail des démonstrations des résultats établis dans le cas général.

Notations et rappels -

Soit K une extension cyclique de $\mathbb{Q}$ de degré permier impair ℓ. Soit $G = Gal(K/\mathbb{Q})$ et soit σ un générateur de G. Soit f le conducteur de K; alors $K \subset \mathbb{Q}^{(f)}$. Soit ζ une racine primitive $f^{ième}$ de 1.

a) Base d'entiers de K.

Soit $\theta = Tr_{\mathbb{Q}^{(f)}/K}(\zeta)$; alors les éléments $1, \theta, \ldots, \theta^{\sigma^{\ell-2}}$ forment une base d'entiers de K. D'un point de vue pratique, soit H un système de représentants de $Gal(\mathbb{Q}^{(f)}/K)$ dans $(\mathbb{Z}/f\mathbb{Z})^*$. On suppose que σ est défini par la restriction $\zeta \to \zeta^a$ à K; alors $\theta = \sum_{x \in H} \cos \frac{2\pi x}{f}$, $\theta^\sigma = \sum_{x \in H} \cos \frac{2\pi x a}{f}$, ...

b) Unités cyclotomiques -

Soit $H' \subset H$ un système exact de représentants des classes de $Gal(\mathbb{Q}^{(f)}/K) / \{1, \tau_o\}$, τ_o désignant la conjugaison complexe; alors

$$\eta = \prod_{x \in H'} \frac{\zeta_{2f}^{ax} - \zeta_{2f}^{-ax}}{\zeta_{2f}^{x} - \zeta_{2f}^{-x}} = \prod_{x \in H'} \frac{\sin \pi \frac{a x}{f}}{\sin \pi \frac{x}{f}}$$

engendre le groupe des unités cyclotomiques de K.

D'un point de vue pratique, on calcule une valeur approchée de θ et η (et de leurs conjugués). Les fonctions symétriques de θ et de ses conjugués (et de η et ses conjugués) sont des entiers rationnels.

c) Formule du nombre de classes -

Soit E le groupe des unités de K, $|E|$ le groupe des valeurs absolues des unités de K, F le groupe des unités cyclotomiques de K (engendré par η et ses conjugués); alors la formule du nombre de classes de Leopoldt [4] se réduit ici à :

$$h = (|E| : |F|)$$

Principe du dévissage -

Le groupe E des unités de K est un $\mathbf{Z}[G]$-module annulé par la norme $1 + \sigma + \ldots + \sigma^{\ell-1}$; c'est donc un $\mathbf{Z}^{(\ell)}$-module. Nous supposerons dans la suite que $\mathbf{Z}^{(\ell)}$ est principal (dans le cas contraire, l'algorithme de dévissage existe mais est plus compliqué).

On vérifie facilement que les propriétés suivantes sont équivalentes :

(i) p divise h

(ii) p^{n_p} divise h, n_p désignant le degré résiduel de p dans $\mathbf{Z}^{(\ell)}$

(iii) il existe un élément ω de $\mathbf{Z}^{(\ell)}$ de norme p^{n_p} et une unité ε de E tels que $\eta = \varepsilon^{\omega}$.

Soit p un nombre premier. Si p est égal à 2, des conditions nécessaires et suffisantes portant sur la signature de η permettent de dire si h est pair ou non et dans l'affirmative le dévissage est légèrement différent de celui obtenu en supposant p impair, mais le principe est le même.

Supposons donc p impair; il existe un entier ω de $\mathbf{Z}^{(\ell)}$ de norme p^{n_p} (une infinité dès que $\ell > 3$). Mais il y a seulement $(\ell-1)/n_p$ entiers ω de $\mathbf{Z}^{(\ell)}$ non équivalents modulo les unités de $\mathbf{Z}^{(\ell)}$ (pour $p = \ell$, il n'y en a qu'un : $1 - \zeta$). Pour chaque ω ainsi déterminé, on cherche s'il existe $\varepsilon \in E$ tel que $\eta = \varepsilon^{\omega}$. Cette relation s'inverse, en considérant ε comme un entier algébrique, pas nécessairement dans K à priori; on obtient

$$\varepsilon = \eta^{\frac{\Omega}{n_p}} \quad \text{où} \quad \Omega = \prod_{\substack{S \in Gal(Q^{(\ell)}/Q) \\ S \neq 1}} \omega^{S}$$

($\eta^{\frac{\Omega}{n_p}}$ désigne $\sqrt[p^{n_p}]{\eta^{\Omega}}$, quantité réelle); on définit de même ε_σ par $\varepsilon_\sigma = (\eta^{\sigma})^{\frac{\Omega}{n_p}}$, pour tout $\sigma \in G$.

Or on a le résultat suivant :

Une condition nécessaire et suffisante pour que les nombres ε_σ, $\sigma \in G$ appartiennent à K est que le polynôme $P = \prod_{\sigma \in G}(X - \varepsilon_\sigma)$ soit à coefficients entiers rationnels. Lorsque cette condition est réalisée, on a alors $\varepsilon_\sigma = \varepsilon^{\sigma}$ pour tout $\sigma \in G$.

Nous disposons donc d'une méthode numérique qui permet de savoir si n'importe quel nombre premier divise ou non h. Cet algorithme ne donne que des diviseurs du nombre de classes. Mais nous avons montré [2] que le nombre de classes de K est majoré dans le cas général par une quantité effectivement calculable. Dans le cas où K est cyclique de degré premier ℓ, on obtient

$$h \leq \frac{\mathcal{R}(\eta)}{(\mathrm{Log}\sqrt{\frac{f}{\ell+1}})^{\ell-1}}$$

où $\mathcal{R}(\eta)$ désigne le régulateur de l'unité η et ses conjugués.

Nous disposons donc d'une méthode qui permet en théorie (par dévissages successifs) de calculer le nombre de classes de n'importe quel corps cyclique de degré premier (et abélien dans le cas général). Les contraintes qui restent ne peuvent plus qu'être d'ordre numérique.

PROBLEMES NUMERIQUES POSES PAR LA METHODE -

1) Ordre de grandeur de la majoration du nombre de classes

Lorsque ℓ est égal à 3, des tables [3] ont déjà été obtenues et la majoration est très bonne. D'après les premiers exemples, la majoration est bonne pour $\ell = 5, 7$ mais mauvaise pour $\ell = 11, 13$. Par exemple

$\ell = 5$	f	h ≤	$\ell = 7$	f	h ≤	$\ell = 11$	f	h ≤
	11	276		29	2964		23	10^9
	25	84		43	6819		67	2.10^7
	31	144		49	1493		89	3.10^7
	41	232		71	6340			
	61	122		113	1962			

Remarque -

La majoration augmente avec le degré ℓ, mais le nombre d'essais à faire diminue relativement (il y a surtout à essayer les nombres premiers p, $p \equiv 1(\ell)$, les autres, intervenant à une certaine puissance, dépassent rapidement la borne).

2) Problèmes posés par la précision

En double précision, on obtient sur ordinateur 15 à 16 chiffres.

Soit p un nombre premier; pour savoir si p^{n_p} divise ou non h, il faut déterminer si le polynôme $\prod(X - \varepsilon_\sigma)$ défini précédemment est à coefficients entiers ou non. Dans certains cas, les coefficients de ce polynôme sont trop grands pour que l'on sache déterminer si ce sont des entiers on non.

On peut d'abord remarquer que ε_σ est un entier de K si et seulement s'il s'écrit comme combinaison linéaire à coefficients entiers de $1, \theta, \ldots, \theta^{\sigma^{\ell-2}}$. Les coefficients se calculent facilement (en tant que nombres réels) et sont d'un ordre de grandeur plus petit que les coefficients du polynôme irréductible.

Des conditions nécessaires arithmétiques se déduisant de [1], prop. I.5 sont toujours programmées. Elles permettent souvent de conclure et évitent un très grand nombre de dévissages.

L'idéal serait d'avoir un programme permettant de calculer en réel avec un nombre arbitrairement grand de décimales.

BIBLIOGRAPHIE

[1] GRAS G.- Approche numérique de la structure du groupe des classes des extensions abéliennes de $\mathbb{Q}$.- Journées de Limoges sur l'utilisation des calculateurs en Mathématiques pures.- Septembre 1975.

[2] GRAS G. et M.N. GRAS.- Calcul du nombre de classes et des unités des extensions abéliennes réelles de $\mathbb{Q}$.- Publ. Math. Univ. de Besançon.- (1974-75).

[3] GRAS M.N.- Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$.- Journal de Crelle.- (1975).- vol. 277.- p. 89-116.

[4] LEOPOLDT H.W.- Über Einheitengruppe und Klassenzahl reller abelscher Zahlkörper.- Abh. Deutsche Akad. Wiss.- Berlin.- Math. 2.- (1954.

Marie-Nicole GRAS
Département de Mathématiques
U.E.R. des SCIENCES
La Bouloie
Route de Gray
25030 BESANCON Cédex