MÉMOIRES DE LA S. M. F.

GEORGES GRAS

Approche numérique de la structure du groupe des classes des extensions abéliennes de $\mathbb{Q}$

Mémoires de la S. M. F., tome 49-50 (1977), p. 101-107

<http://www.numdam.org/item?id=MSMF_1977__49-50__101_0>

Calculateurs en Math. (1975 - LIMOGES)
Bull. Soc. math. France
Mémoire 49-50, 1977, p. 101-107

APPROCHE NUMERIQUE DE LA STRUCTURE DU GROUPE DES CLASSES DES EXTENSIONS ABELIENNES DE $\mathbb{Q}$

par Georges GRAS

INTRODUCTION -

On considère une extension abélienne $K/\mathbb{Q}$. Le problème de la détermination numérique de $\mathcal{H}_K$ (le ℓ-groupe des classes de K, pour ℓ premier fixé) est un problème difficile. Considérons comme possible le calcul de $|\mathcal{H}_K|$; les seules méthodes possibles pour la détermination de la structure de $\mathcal{H}_K$ comme $Gal(K/\mathbb{Q})$-module sont d'ordre géométrique (cf. algorithmes et programmes de SMADJA [9]). Elles nécessitent de connaître $|\mathcal{H}_K|$, sont assez longues à programmer et permettent difficilement de démontrer des théorèmes concernant cette structure (elles sont non arithmétiques).

Nous nous proposons de montrer que certaines informations arithmétiques (et numériquement accessibles) permettent d'approcher la structure de $\mathcal{H}_K$ et de la déterminer dans certaines circonstances simples.

Nous montrons enfin comment un certain nombre de conjectures peuvent être étudiées sur le plan numérique.

Dans toute la suite, les extensions $K/\mathbb{Q}$ considérées sont de degré premier à ℓ et on suppose $\ell \neq 2$.

I - RAPPEL DES PROPRIETES INHERENTES AU CAS " SEMI-SIMPLE " ([2])

1) Caractères -

Soit $\mathbb{Q}^a$ la réunion de toutes les extensions abéliennes de $\mathbb{Q}$ de degré premier à ℓ (ℓ premier impair). On réalise un plongement $\mathbb{Q}^a \to \Omega_\ell$ (où Ω_ℓ est une clôture algébrique de $\mathbb{Q}_\ell$). On pose $\mathcal{G} = Gal(\mathbb{Q}^a/\mathbb{Q})$.

a) Caractères de degré 1 -

Ce sont les homomorphismes $\chi' : \mathcal{G} \to \Omega_\ell$ tels que $\mathrm{Ker}\,\chi'$ soit fermé et d'indice fini dans $\mathcal{G}$; χ' est à valeurs dans le groupe des racines g^e de l'unité si g est l'ordre de χ'. On appelle $\mathcal{X}'$ leur ensemble. A partir de $\mathcal{X}'$ on définit deux ensembles de caractères : les caractères rationnels et les caractères ℓ-adiques.

b) Caractères rationnels -

Soit $\chi' \in \mathcal{X}'$, d'ordre g; on pose : $\chi = \sum_{a \in (\mathbb{Z}/g\mathbb{Z})^*} \chi'^a$. On note $\mathcal{X}$ l'ensemble de ces fonctions appelées caractères rationnels (irréductibles) de $\mathcal{G}$.

c) Caractères ℓ-adiques -

Dans $(\mathbb{Z}/g\mathbb{Z})^*$ on appelle H le sous-groupe engendré par l'image de ℓ, $\overline{\ell}$ ($\overline{\ell} \in (\mathbb{Z}/g\mathbb{Z})^*$ car ℓ ne divise pas g) et on pose : $\phi = \sum_{a \in H} \chi'^a$. On note Φ

l'ensemble de ces fonctions appelées caractères ℓ-adiques irréductibles de $\mathcal{G}$.

Exemple -

Si χ' est d'ordre 5 et $\ell = 19$, on peut former $\chi = \chi' + \chi'^2 + \chi'^3 + \chi'^4 \in \mathcal{X}$, $\phi = \chi'^4 + \chi' \in \Phi$ et $\phi' = \chi'^3 + \chi'^2 \in \Phi$; on a $\phi + \phi' = \chi$.

On emploie la notation $\chi' | \phi$, $\phi | \chi$ pour dire que χ' est un terme de ϕ et ϕ un terme de χ. Si ϕ et ϕ' sont deux caractères ℓ-adiques divisant un même caractère χ, on dira que ϕ et ϕ' sont conjugués.

Remarque -

On dit que χ est un caractère rationnel car ses valeurs sont dans $\mathbb{Z}$, et que ϕ est un caractère ℓ-adique car ses valeurs sont dans $\mathbb{Z}_\ell$.

d) Caractère θ -

Soit $\sigma \in \mathcal{G}$, soit ζ_ℓ une racine d'ordre ℓ de l'unité et soit $a \in \mathbb{Z}$ tel que $\zeta_\ell^\sigma = \zeta_\ell^a$; on définit $\theta(\sigma)$ comme étant la racine $\ell-1^e$ de l'unité congrue à a module ℓ; comme $\mathbb{Q}_\ell$ contient les racines $\ell-1^e$ de l'unité, on a $\theta \in \Phi$.

e) Caractères pairs et impairs -

Soit $-1 \in \mathcal{G}$ la conjugaison complexe. Si $\chi'(-1) = 1$ (resp. -1) on dit que χ' est pair (resp. impair); cette propriété subsistant pour tout conjugué de χ', on peut dire qu'un caractère rationnel ou ℓ-adique est pair ou impair.

On démontre la propriété suivante :

PROPOSITION I.1 -

L'ensemble $\mathcal{X}$ est en bijection avec l'ensemble des extensions cycliques de $\mathbb{Q}$ contenues dans $\mathbb{Q}^a$. Dans cette bijection les caractères pairs correspondent aux extensions réelles et les caractères impairs aux extensions imaginaires.

On peut donc noter toute extension cyclique K_χ, $\chi \in \mathcal{X}$. La correspondance $\mathcal{X} \leftrightarrow \{K_\chi\}$ est la suivante : si $\chi' | \chi$, K_χ est le corps fixe par $\operatorname{Ker} \chi'$.

Nous poserons $G_\chi = \operatorname{Gal}(K_\chi/\mathbb{Q})$ et nous désignerons par g_χ l'ordre commun des $\chi' | \chi$.

2) ℓ-groupe des classes des sous-corps de $\mathbb{Q}^a$ -

On désigne par $\mathcal{H}_{K_\chi}$ le ℓ-groupe des classes de K_χ. C'est un G_χ-module, donc un $\mathbb{Z}_\ell[G_\chi]$-module. On pose $\mathcal{H}_\chi = (\mathcal{H}_{K_\chi})^{e_\chi}$ où e_χ est l'idempotent $\frac{1}{g_\chi} \sum_{\sigma \in G_\chi} \chi(\sigma^{-1})\, \sigma \in \mathbb{Z}_\ell[G_\chi]$; $\mathcal{H}_\chi$ est un sous-module de $\mathcal{H}_{K_\chi}$.

On pose $\mathcal{H}_\phi = \mathcal{H}_\chi^{e_\phi}$, où e_ϕ est l'idempotent irréductible sur $\mathbb{Z}_\ell$: $\frac{1}{g_\chi} \sum_{\sigma \in G_\chi} \phi(\sigma^{-1})\, \sigma \in \mathbb{Z}_\ell[G_\chi]$, pour $\phi \in \Phi$. On a alors la relation :

$$\mathcal{H}_\chi = \bigoplus_{\phi | \chi} \mathcal{H}_\phi$$

On démontre que les $\mathcal{H}_\chi$ (donc les $\mathcal{H}_\phi$) permettent de reconstituer tous les groupes de classes dans le cas semi-simple :

PROPOSITION I.2 -

Soit $L \subset \mathbb{Q}^a$. Alors $\mathcal{H}_L \simeq \bigoplus_{K_\chi \subset L} \mathcal{H}_\chi$

On remarque alors que la famille $\{\mathcal{H}_\phi\}_{\phi \in \Phi}$ donne la décomposition la plus fine possible des ℓ-groupes de classes : c'est une famille universelle de modules dont on aimerait bien connaître tous les éléments.

3) Structures de $\mathbb{Z}_\ell^{(g_\chi)}$-modules de $\mathcal{H}_\phi$ -

Soit $\phi \in \Phi$. Alors $\mathcal{H}_\phi = \mathcal{H}_\chi^{e_\phi}$ est un $\mathbb{Z}_\ell[G_\chi]e_\phi$-module et on vérifie facilement que : $\mathbb{Z}_\ell[G_\chi]e_\phi$ est isomorphe à $\mathbb{Z}_\ell^{(g_\chi)}$; c'est un anneau de Dedekind local d'idéal maximal (ℓ). On a donc la décomposition

$$\mathcal{H}_\phi \simeq \prod_{i \geq 1} \mathbb{Z}_\ell^{(g_\chi)}/(\ell)^{n_{i,\phi}(\mathcal{H})}$$

$n_{i,\phi}(\mathcal{H}) \geq 0$. Les $n_{i,\phi}(\mathcal{H})$ caractérisent la structure de $\mathcal{H}_\phi$, donc celle de tous les groupes de classes dans le cas semi-simple.

On définit d'abord des invariants moins fins :

$$m_\phi(\mathcal{H}) = \sum_{i \geq 1} n_{i,\phi}(\mathcal{H}) \qquad m_\chi(\mathcal{H}) = \sum_{\phi | \chi} m_\phi(\mathcal{H}).$$

On a par définition $|\mathcal{H}_\phi| = \ell^{\phi(1)m_\phi(\mathcal{H})}$ et $|\mathcal{H}_\chi| = \ell^{\phi(1)m_\chi(\mathcal{H})}$.

Remarque -

La notation "$\mathcal{H}$" rappelle que ces invariants sont relatifs à la structure des groupes de classes $\mathcal{H}$.

Le problème est donc de déterminer $m_\chi(\mathcal{H})$ puis $m_\phi(\mathcal{H})$ et enfin les $n_{i,\phi}(\mathcal{H})$ à partir d'informations arithmétiques numériquement calculables. Avant d'étudier très partiellement ce problème nous allons rassembler le maximum d'informations de nature arithmétique.

II - INFORMATIONS RELATIVES AUX INVARIANTS "$\mathcal{H}$" -

Nous allons rappeler celles qui sont connues et en donner une nouvelle.

1) Formules analytiques du nombre de classes -

a) Cas réel (χ pair) - On démontre ([4], voir aussi [8]) à partir des formules analytiques que $|\mathcal{H}_\chi| = (E_\chi : F_\chi)$ où E_χ est le groupe des χ-unités et F_χ le groupe des χ-unités cyclotomiques. On a $E_\chi = \{\varepsilon, \text{ unité de } K_\chi, |\varepsilon|^{e_\chi} = |\varepsilon|\}$; les groupes E_χ ne sont pas connus à priori tandis que les groupes F_χ sont parfaitement connus numériquement (pour la détermination de $|\mathcal{H}_\chi|$ et de $m_\chi(\mathcal{H})$, cf [3]). On a ainsi un moyen pour calculer l'invariant $m_\chi(\mathcal{H})$. Mais en plus, on dispose d'un G_χ-module E_χ/F_χ et on peut conjecturer que la structure de ce module donne des informations sur la structure de $\mathcal{H}_\chi$. C'est pour cette raison que nous allons définir les invariants résumant la structure de E_χ/F_χ :

On montre facilement que la composante en e_ϕ du ℓ-sous-groupe de Sylow de E_χ/F_χ est isomorphe à un $\mathbb{Z}_\ell^{(g_\chi)}$-module monogène de la forme $\mathbb{Z}_\ell^{(g_\chi)}/(\ell)^{m_\phi(h)}$. Ceci définit, pour ϕ pair, l'invariant analytique $m_\phi(h)$; on définit alors $m_\chi(h) = \sum_{\phi|\chi} m_\phi(h)$. On a donc par définition $m_\chi(\mathcal{H}) = m_\chi(h)$, mais rien ne prouve que $m_\phi(\mathcal{H}) = m_\phi(h)$.

Conjecture A^+ -

On a $m_\phi(\mathcal{H}) = m_\phi(h)$ pour tout ϕ pair.

b) Cas imaginaire (χ impair) -

Ce cas est un peu plus simple et plus complet. On démontre que $|\mathcal{H}_\chi|$ est égal à la ℓ-participation de $\prod_{\chi'|\chi} B_1(\chi'^{-1})$ (les $B_1(\chi'^{-1})$ étant les nombres de Bernoulli généralisés ([5])) (lorsque $\theta|\chi$, on doit faire une légère modification à cet énoncé (cf. [2])). Ces nombres sont ℓ-entiers dans $\mathbb{Q}^{(g_\chi)}$, conjugués pour $\chi'|\chi$ et facilement calculables. Par analogie, on définit les invariants $m_\phi(h)$ par $(B_1(\chi'^{-1}))\,\mathbb{Z}_\ell^{(g_\chi)} = (\ell)^{m_\phi(h)}$ pour $\chi'|\phi$ et pour chaque $\phi|\chi$. On pose encore $m_\chi(h) = \sum_{\phi|\chi} m_\phi(h)$. On a par définition $m_\chi(\mathcal{H}) = m_\chi(h)$.

Conjecture A^- -

On a $m_\phi(\mathcal{H}) = m_\phi(h)$ pour tout ϕ impair.

Contrairement au cas réel, on a une information supplémentaire en direction de cette conjecture : c'est le résultat de Stickelberger ([7]).

2) THEOREME DE STICKELBERGER -

On peut énoncer ce théorème sous la forme suivante :

PROPOSITION I.3 -

Muni de sa structure de $\mathbb{Z}_\ell^{(g_\chi)}$*-module,* $\mathcal{H}_\phi$ (*pour* ϕ *impair*) *est annulé par* $\ell^{m_\phi(h)}$. *De façon équivalente, on a* $n_{i,\phi}(\mathcal{H}) \leq m_\phi(h)$ *pour tout* i.

Ceci est un renseignement précieux et qui permet parfois de conclure.

Nous allons examiner deux autres informations reliant cette fois des $\mathcal{H}_\phi$ pour des caractères ϕ non conjugués.

3) " SPIEGELUNGSSATZ " (Leopoldt ([6])).

Soit $\phi \in \Phi$, $\phi = \sum_{\chi'|\phi} \chi'$; on pose $\overline{\phi} = \theta \sum_{\chi'|\phi} \chi'^{-1} \in \Phi$; on montre facilement que $\overline{\overline{\phi}} = \phi$ et que ϕ est pair si et seulement si $\overline{\phi}$ est impair et inversement. Ce caractère $\overline{\phi}$ est appelé le miroir de ϕ. Appelons $\dim_\phi$ le $\mathbb{Z}_\ell[G_\chi]e_\phi$-rang d'un $\mathbb{Z}_\ell[G_\chi]e_\phi$-module. On a le résultat suivant :

PROPOSITION I.4 -

Soit $\phi \in \Phi$, ϕ *pair. Alors :*

i) $0 \leq \dim_{\overline{\phi}} \mathcal{H}_{\overline{\phi}} - \dim_\phi \mathcal{H}_\phi \leq a_\phi$, où a_ϕ est défini par $a_\phi = 1$ (resp. 0)

si $(E_\chi/E_\chi^\ell)^{e_\phi}$ est engendré par l'image des unités ℓ-primaires de E_χ (resp. sinon).

ii) $a_\phi = 1$ entraîne $\mathcal{H}_{\underline{\phi}} \neq 1$

4) GENERALISATION DU CRITERE DE FRESNEL - ([1]).

Dans les exemples numériques, où $\dim_\phi \mathcal{H}_\phi$ est souvent 0 ou 1, la connaissance de a_ϕ serait primordiale; or elle exige celle des unités, ce qui peut se faire numériquement pour chaque cas mais ne saurait conduire à un théorème. Les travaux de FRESNEL et LEOPOLDT sur les fonctions L_ℓ ℓ-adiques suggèrent que si a_ϕ n'est pas connu à priori, b_ϕ, le même nombre calculé avec les unités cyclotomiques est connu : on pose $b_\phi = 1$ (resp. 0) si $(F_\chi/F_\chi^\ell)^{e_\phi}$ est engendré par les images des unités ℓ-primaires de F_χ (resp. sinon). On a $a_\phi \leq b_\phi$.

Nous avons obtenu dans [2] le résultat suivant :

PROPOSITION I.5 -

On a $b_\phi = 1$ si et seulement si $m_{\underline{\phi}}(h) > 0$.

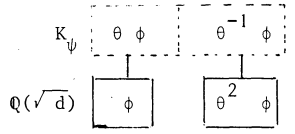
Cette proposition généralise les résultats de FRESNEL et d'autres auteurs dans le sens qu'il y avait toujours un cas qui échappait (ce résultat provient en fait d'une congruence généralisant des congruences classiques : par exemple, nous obtenons les congruences de ANKENY - ARTIN - CHOWLA sur les corps quadratiques (pour $\ell = 3$) dans tous les cas, même le cas " spécial " où les congruences de ces auteurs se réduisent à $0 \equiv 0 \mod 3$).

III - ETUDE NUMERIQUE DE LA CONJECTURE A SUR UN EXEMPLE -

Le point de vue est le suivant : on essaye de trouver des contre-exemples aux conjectures A^+ et A^-. Pour cela on doit se placer dans les plus mauvaises conditions, compte tenu de toutes les informations précédentes qui sont plutôt "favorables" à la conjecture.

On constate que toutes nos " informations " relient soit des groupes $\mathcal{H}_\phi$ pour des caractères ϕ conjugués, soit des groupes $\mathcal{H}_\phi$ et $\mathcal{H}_{\underline{\phi}}$. On est donc amené à considérer des ensembles $C \subset \Phi$ stables par les deux opérations conjugaison et passage au caractère miroir. On a ainsi des classes d'équivalence C dans lesquelles on peut raisonner.

Nous prenons l'exemple suivant (pour d'autres résultat se reporter à [2]) : Soit $\chi' = \phi = \chi$ un caractère quadratique pair ($g_\chi = 2$) associé à un corps quadratique réel $Q(\sqrt{d})$, $d \neq 5$. On obtient une classe C représentée par le schéma suivant (pour $\ell = 5$) :



$[K_\psi : \mathbb{Q}] = 4$, K_ψ imaginaire

La classe C est engendrée de la façon suivante : On a $\overline{\phi} = \theta\ \phi$ et $\theta\ \phi$ étant d'ordre 4 admet un unique autre conjugué $\theta^{-1}\ \phi$; on a alors $\theta^{-1}\ \phi = \theta^2\ \phi$, d'ordre 2 et qui correspond au corps quadratique réel $\mathbb{Q}(\sqrt{5\,d})$; le caractère rationnel $\psi = \theta\ \phi + \theta^{-1}\ \phi$ correspond à une extension cyclique imaginaire de degré 4.

Voici ce que l'on peut dire numériquement au sujet de cette classe.

Supposons par exemple $B_1(\theta\ \phi) \not\equiv 0 \bmod 5$; on a donc $m_{\theta\phi}(h) = 0$ et d'après le résultat de Stickelberger (prop. I.3), $\mathcal{H}_{\theta\phi} = (1)$; d'après l'égalité $m_\chi(h) = m_\chi(\mathcal{H})$, on en déduit que la conjecture A^- est vérifiée dans ce cas. Un contre-exemple nécessite donc d'avoir :

$B_1(\theta\ \phi) \equiv B_1(\theta^{-1}\ \phi) \equiv 0 \bmod 5$ (i. e. $m_{\theta\phi}(h) \geq 1$ et $m_{\theta^{-1}\phi}(h) \geq 1$).

Supposons avoir $m_{\theta\phi}(h) = m_{\theta^{-1}\phi}(h) = 1$ (i. e. des nombres de Bernoulli divisibles par 5 mais non par 25). On a donc $\mathcal{H}_\psi$ d'ordre 25. A priori on a trois cas :

$\mathcal{H}_{\theta\phi} \simeq \mathbb{Z}/5\mathbb{Z}$ $\quad \mathcal{H}_{\theta^{-1}\phi} \simeq \mathbb{Z}/5\mathbb{Z}$ (cas 1)

$\mathcal{H}_{\theta\phi} \simeq \mathbb{Z}/25\mathbb{Z}$ $\quad \mathcal{H}_{\theta^{-1}\phi} = (1)$ (ou vice-versa)(cas 2)

$\mathcal{H}_{\theta\phi} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, $\mathcal{H}_{\theta^{-1}\phi} = (1)$ (ou vice-versa)(cas 3)

Le premier cas est le cas où A^- est vérifiée et le deuxième est impossible à cause du résultat de Stikelberger (Prop. I.3). On doit donc supposer que l'on est dans le cas 3, avec, par exemple, $\mathcal{H}_{\theta^{-1}\phi} = (1)$. Mais on a $m_{\theta^{-1}\phi}(h) = 1$ et, d'après la généralisation du critère de FRESNEL (Prop. I.5), on aura $b_{\theta^2\phi} = 1$, si $a_{\theta^2\phi} = 1$, d'après le Spiegelungssatz (Prop. I.4., (ii)), on aura $\mathcal{H}_{\theta^{-1}\phi} \neq 1$ ce qui est absurde, donc $a_{\theta^2\phi} = 0$; mais si $a_{\theta^2\phi} = 0$ c'est que l'unité cyclotomique de $\mathbb{Q}(\sqrt{5\,d})$ est puissance 5^e d'unité, d'où $m_{\theta^2\phi}(h) > 0$, soit $m_{\theta^2\phi}(\mathcal{H}) > 0$ (pour un corps quadratique la conjecture A^+ est évidemment vraie) et à nouveau d'après le Spiegelungssatz (Prop. I.4, (i)), $\mathcal{H}_{\theta^{-1}\phi} \neq (1)$, ce qui est absurde.

Conclusion -

Il est nécessaire que l'un des deux nombres de Bernoulli soit divisible par 25 et l'autre par 5. On voit que l'on obtient une condition numérique assez sévère.

Signalons qu'un programme pour le calcul de ces nombres de Bernoulli vient d'être élaboré pour rechercher un tel exemple.

BIBLIOGRAPHIE

[1] FRESNEL (J.).- Nombres de Bernoulli et fonctions L p-adiques.- Ann. Inst. Fourier.- Grenoble 17, 2 (1967).- 281-333.

[2] GRAS (G.).- Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés (à paraître).

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

[4] LEOPOLDT (H.-W).- Über Einheitengruppe und Klassen zahl reeller abelscher Zahlkörper.- Abh. Deutsche Akad. Wiss. Berlin.- Math. 2 (1954).

[5] LEOPOLDT (H.W.).- Eine Verallgemeinerung der Bernoullischen Zahlen.- Abh. Math. Sem. Univ. Hamburg.- 22 (1958).- 131-140.

[6] LEOPOLDT (H.-W.).- Zur Struktur der ℓ-Klassengruppe galoisscher Zahlkörper.- Jour. für die reine und ang.- Math. 199 (1958).- 165-174.

[7] LEOPOLDT (H.-W.).- Zur Arithmetik in abelschen Zahlkörper.- Jour. für die reine und ang. Math.- 209 (1962).- 54-71.

[8] ORIAT (B.).- Traduction française de " Über Einheitengruppe und Klassenzahl reeler abelscher Zahlkörper " de Leopoldt.- Publ. Math. Univ. Besançon (1974-75).

[9] SMADJA (R.).- Sur le groupe des classes des corps de nombres.- C.R.A.S.- A, 276.- (1973).- (1639-1641).

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