SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

MARIE-NICOLE GRAS

Calcul du nombre de classes et des unités des extensions abéliennes réelles de Q

Séminaire de théorie des nombres de Grenoble, tome 4 (1974-1975), exp. n° 9, p. 1-12

<http://www.numdam.org/item?id=STNG_1974-1975__4__A9_0>

Séminaire de Théorie des Nombres
20 février 1975
Grenoble

CALCUL DU NOMBRE DE CLASSES ET DES UNITES DES EXTENSIONS ABELIENNES REELLES DE $\mathbb{Q}$

par Marie Nicole GRAS

Cet exposé donne les principaux résultats d'un travail [1] fait en commun avec Georges GRAS.

Soit K une extension abélienne réelle de $\mathbb{Q}$. Leopoldt a donné une interprétation arithmétique de la formule analytique du nombre de classes de ces corps. A partir de cette interprétation et de la seule connaissance des unités cyclotomiques de K, nous établissons un algorithme permettant de déterminer le nombre de classes et les unités de K. L'algorithme est effectif grâce à un critère numérique de divisibilité du nombre de classes par un entier quelconque et grâce à une majoration du nombre de classes ne dépendant que de $[K:\mathbb{Q}]$, $Gal(K/\mathbb{Q})$, du conducteur de K et des unités cyclotomiques.

I - PRELIMINAIRES

Dans cette partie, on rappelle les principaux résultats de H.W. LEOPOLDT ([3] et [4]).

1. CARACTERES DES EXTENSIONS ABELIENNES DE $\mathbb{Q}$.

Soit K une extension abélienne réelle de $\mathbb{Q}$, de degré g , de groupe de Galois G et de conducteur f . Soit $\mathfrak{X}'$ le groupe des caractères complexes de K , i.e. le groupe des homomorphismes de $(\mathbb{Z}/f\mathbb{Z})^*$ dans $\mathbb{C}$ triviaux sur le sous-groupe correspondant à K . On définit sur $\mathfrak{X}'$ la relation d'équivalence suivante : soient χ' et $\psi' \in \mathfrak{X}'$; on dit que χ' et ψ' sont $\Gamma_{\mathbb{Q}}$-conjugués [5] si χ' et ψ' engendrent le même sous-groupe de $\mathfrak{X}'$; on vérifie que cette propriété est équivalente à $\ker \chi' = \ker \psi'$. Pour tout $\chi' \in \mathfrak{X}'$, soit $\tilde{\chi}$ la $\Gamma_{\mathbb{Q}}$ classe de conjugaison de χ' . On définit les applications χ par $\chi(\sigma) = \sum_{\chi' \in \tilde{\chi}} \chi'(\sigma)$; ces applications, à valeurs dans $\mathbb{Z}$, sont appelées les caractères rationnels irréductibles de K (ou plus brièvement les caractères de K). On notera par $\mathfrak{X}$ l'ensemble des caractères de K .

Pour tout $\chi' \in \mathfrak{X}'$, on considère le sous-corps $K_{\chi'}$ de K fixe par $U_{\chi'} = \ker \chi'$; ce corps est une extension cyclique de $\mathbb{Q}$, de degré $g_{\chi'}$ égal à l'ordre de χ' ; comme $U_{\chi'}$, $K_{\chi'}$ et $g_{\chi'}$ ne dépendent pas du choix de $\chi' \in \tilde{\chi}$, on peut les noter respectivement U_χ , K_χ et g_χ ; de même, le conducteur de K_χ sera noté f_χ .

On vérifie que lorsque χ parcourt $\mathfrak{X}$, alors les corps K_χ parcourent l'ensemble de tous les sous-corps de K cycliques sur $\mathbb{Q}$.

2. L'ALGEBRE $\mathbb{Q}[G]$.

Pour tout $\chi \in \mathfrak{X}$, soit $e_\chi = 1/g \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma$; on vérifie que les e_χ forment un système d'idempotents orthogonaux de $\mathbb{Q}[G]$ et que $\mathbb{Q}[G] = \oplus_{\chi \in \mathfrak{X}} \mathbb{Q}[G]e_\chi$. On montre que $\mathbb{Q}[G]e_\chi$ est isomorphe au corps cyclotomique $\mathbb{Q}^{(g_\chi)} = \mathbb{Q}_\chi$ et que dans cet isomorphisme, l'anneau des entiers $\mathbb{Z}^{(g_\chi)} = \mathbb{Z}_\chi$ de $\mathbb{Q}_\chi$ correspond à $\mathbb{Z}[G]e_\chi$ (soit $\sigma_\chi \in G$ tel que l'image de σ_χ dans G/U_χ soit génératrice ; alors l'isomorphisme

précédent est entièrement déterminé par $\sigma_\chi e_\chi \to \exp(2i\pi/g_\chi)$.

3. ETUDE DU GROUPE DES UNITES DE K .

Soit E_K le groupe des unités de K ; puisque K est réelle, les seules racines de l'unité contenues dans K sont -1 et $+1$; on identifie $E_K/\{\pm 1\}$ à $|E_K|$ et on pose $|\varepsilon|^\sigma = |\varepsilon^\sigma|$ pour tout $\sigma \in G$.

Soit χ un caractère de K . Soit K_χ le sous-corps cyclique de K correspondant à $U_\chi = \ker \chi$. On dit qu'une unité ε de K_χ est χ-relative si $N_{K_\chi/k}(\varepsilon) = \pm 1$ pour tout sous-corps strict k de K_χ . On note E_χ le sous-groupe des unités χ-relatives de K_χ . D'après Leopoldt, on a les propriétés suivantes :

(i) $|E_\chi|$ est un $\mathbb{Z}$-module libre de rang $\varphi(g_\chi)$;

(ii) Une condition nécessaire et suffisante pour qu'une unité ε de K soit χ-relative est que $|\varepsilon|^{e_\chi} = |\varepsilon|$, $e_\chi = 1/g \sum_{\sigma\in G} \chi(\sigma^{-1})\sigma$ étant l'idempotent de $\mathbb{Q}[G]$ défini ci-dessus (c'est cette propriété qui donne à E_χ une structure de $\mathbb{Z}_\chi$-module) ;

(iii) Soit E^K le sous-G-module engendré par les E_χ ; on a $|E^K| = \bigoplus_{\chi\neq 1} |E_\chi|$;

(iv) Le groupe $|E_\chi|$ est un $\mathbb{Z}_\chi$-module sans torsion ; donc $|E_\chi|$ est isomorphe à un idéal de $\mathbb{Z}_\chi$. Mais $|E_\chi|$ n'est pas libre en général (en effet, $|E_\chi|$ est libre si et seulement si l'idéal est principal).

4. FORMULE ANALYTIQUE DU NOMBRE DE CLASSES.

Soit h_K le nombre de classes au sens ordinaire de K . Pour tout caractère χ de $\mathfrak{X}$, $\chi \neq 1$, on définit les unités cyclotomiques χ-relatives de K_χ de la manière suivante : K_χ de conducteur f_χ est

contenu dans $\mathbb{Q}^{(f_\chi)}$; soit H_χ le sous-groupe de $(\mathbb{Z}/f_\chi\mathbb{Z})^*$ correspondant à $\mathrm{Gal}(\mathbb{Q}^{(f_\chi)}/K_\chi)$ et soit G_χ un système exact de représentants de $H_\chi/\{-1,+1\}$; alors G_χ correspond à $\mathrm{Gal}(Q_o^{(f_\chi)}/K_\chi)$. Soit $\zeta'_\chi = \exp(i\pi/f_\chi)$ et soit $\Theta_\chi = \overline{\prod_{a\in G_\chi}} (\zeta'^{a}_\chi - \zeta'^{-a}_\chi)$; on pose

$$\Lambda_\chi = \frac{1}{\|U_\chi\|} \Big(\sum_{\tau\in U_\chi} \tau \Big) \overline{\prod_{\substack{\ell/g_\chi \\ \ell \text{ premier}}}} (1 - \sigma_\chi^{g_\chi/\ell})$$

et on considère $\eta_\chi = \Theta_\chi^{\Lambda_\chi}$. On vérifie que η_χ est une unité χ-relative de K_χ et qu'elle engendre un sous-module F_χ d'indice fini dans E_χ ; on appelle η_χ l'unité cyclotomique χ-relative génératrice. Le groupe $|F_\chi|$ est un sous-$\mathbb{Z}_\chi$-module libre de $|E_\chi|$, de dimension 1 .

Soit $h_\chi = (|E_\chi|:|F_\chi|)$; alors le nombre de classes h_K est donné par la formule $h_K = \frac{Q_K}{Q_G} \prod_{\chi\neq 1} h_\chi$, où $Q_K = (|E_K|:|E^K|)$ et $Q_G = (g^{g-2}/\prod_\chi d_\chi)^{1/2}$ où d_χ désigne le discriminant du corps $\mathbb{Q}_\chi$.

II - MAJORATION DES INDICES $h_\chi = (|E_\chi|:|F_\chi|)$.

Soit $\chi \neq 1$ un élément fixé de $\mathfrak{X}$. Soit K_χ le sous-corps de K fixe par U_χ et soit $G_\chi = \mathrm{Gal}(K_\chi/\mathbb{Q})$. Soit F un sous-G_χ-module de E_χ de même rang ; soit $r(F)$ l'indice $(|E_\chi|:|F|)$. On établit dans ce chapitre une majoration générale de $r(F)$ indépendante de E_χ qui sera évidemment appliquée au cas particulier $F = F_\chi$.

1. PLONGEMENT LOGARITHMIQUE DE E_χ .

On considère dans $\mathbf{R}^{g_\chi}$ le plongement logarithmique de $|E_\chi|$: si $|\varepsilon| \in |E_\chi|$, on pose $L_\chi(\varepsilon) = (\ldots, \log|\varepsilon^\sigma|, \ldots)_{\sigma\in G_\chi}$. L'image de $|E_\chi|$ par L_χ est un réseau relatif de dimension $\varphi(g_\chi)$ contenu dans l'hyperplan $\pi_\chi = \{x = (x_\sigma)_{\sigma\in G_\chi} , \sum_{\sigma\in G_\chi} x_\sigma = 0\}$. Désignons par V_χ le sous-espace de $\mathbf{R}^{g_\chi}$ engendré sur $\mathbf{R}$ par $L_\chi(E_\chi)$. Soient

$$\mathcal{B}_\chi = \{x = (x_\sigma)_{\sigma\in G_\chi} \ , \ |x_\sigma| \leq 1 \text{ pour tout } \sigma \neq 1\}$$

et

$$D_\chi = \mathcal{B}_\chi \cap V_\chi \ ;$$

on vérifie que D_χ est un compact convexe symétrique par rapport à 0, de mesure finie non nulle (i.e. une jauge). On note m_χ la mesure de D_χ.

2. RESULTAT FONDAMENTAL : MAJORATION DE $r(F)$.

Soit donc F un sous-G_χ-module de E_χ. Le sous-groupe $L_\chi(F)$ de $L_\chi(E_\chi)$ est un réseau qui engendre aussi V_χ. Nous noterons $m_\chi(F)$ la mesure du domaine fondamental du réseau $L_\chi(F)$; on a alors

$$(|E_\chi| : |F|) = \frac{m_\chi(F)}{m_\chi(E_\chi)} \ .$$

Soit Φ une fonction polynôme homogène à coefficients réels de degré $d_\Phi \geq 1$ des variables réelles x_σ, $\sigma \in G_\chi$. Alors

$$\sup_{\substack{x\in \mathbf{R}^{g_\chi} \\ x\neq 0}} \left(|\Phi(x)| / \max_{\sigma\in G_\chi} (|x_\sigma|^{d_\Phi})\right)$$

existe et est un nombre réel strictement positif noté μ_Φ. On suppose qu'il existe une constante M_Φ, ne dépendant que de Φ, vérifiant $M_\Phi > \mu_\Phi$ et telle que, pour tout $\varepsilon \in E_\chi$, $|\varepsilon| \neq 1$, on ait $|\Phi(\ldots,\varepsilon^\sigma,\ldots)| \geq M_\Phi$ (de telles fonctions Φ existent, par exemple le discriminant ou des produits de résolvantes de Lagrange). Avec les notations ci-dessus, on a :

THEOREME. $$r(F) \leq \frac{m_\chi(F)}{m_\chi} \left(\frac{1}{2d_\Phi} \log \frac{M_\Phi}{\mu_\Phi}\right)^{-\varphi(g_\chi)} \ ;$$

en particulier

$$h_\chi \leq \frac{m_\chi(F_\chi)}{m_\chi} \left(\frac{1}{2d_\Phi} \log \frac{M_\Phi}{\mu_\Phi}\right)^{-\varphi(g_\chi)} \ .$$

LEMME. *Il existe dans* E_χ *une unité* ε_o, $|\varepsilon_o| \neq 1$, *telle que*

$$\max_{\sigma\in G_\chi} (\log|\varepsilon_o|^\sigma) \leq 2(m_\chi(F)/m_\chi r(F))^{1/\varphi(g_\chi)} \ .$$

Démonstration : On considère le réseau relatif

$$L'_\chi = \frac{1}{2}(\mathcal{M}_\chi(F)/m_\chi r(F))^{-1/\varphi(g_\chi)} L_\chi(E_\chi) \ ;$$

son $\mathbb{Z}$-rang est égal à $\varphi(g_\chi)$ et la mesure de sa maille vaut

$$\mathcal{M}_\chi(L'_\chi) = [\frac{1}{2}(\mathcal{M}_\chi(F)/m_\chi r(F))^{-1/\varphi(g_\chi)}]^{\varphi(g_\chi)} \mathcal{M}_\chi(E_\chi) = \frac{1}{2^{\varphi(g_\chi)}} \frac{r(F)m_\chi}{\mathcal{M}_\chi(F)} \mathcal{M}_\chi(E_\chi)$$

$$= \frac{m_\chi}{2^{\varphi(g_\chi)}}$$

puisque $r(F) = \mathcal{M}_\chi(F)/m_\chi(E_\chi)$; donc $m_\chi = 2^{\varphi(g_\chi)} \mathcal{M}_\chi(L'_\chi)$; d'après le théorème de Minkowski, la jauge compacte D_χ de mesure m_χ contient un point de L'_χ autre que l'origine, que nous noterons

$$\frac{1}{2}(\mathcal{M}_\chi(F)/m_\chi r(F))^{-1/\varphi(g_\chi)} L_\chi(\varepsilon'_o) \ ;$$

l'unité ε'_o vérifie donc, pour tout $\sigma \neq 1$,

$$|\log |\varepsilon_o'^{\sigma}|| \leq 2(\mathcal{M}_\chi(F)/m_\chi r(F))^{1/\varphi(g_\chi)} \ ;$$

mais si une jauge contient l'image d'une unité, elle contient celle de son inverse. L'unité ε_o égale à ε'_o à $\varepsilon_o'^{-1}$ et telle que $\log |\varepsilon_o| < 0$ répond donc au problème.

Démonstration du théorème : D'après le lemme, il existe une unité ε_o de E_χ , $|\varepsilon_o| \neq 1$, telle que $\underset{\sigma \in G_\chi}{\text{Max}} (\log |\varepsilon_o^\sigma|) \leq 2(\mathcal{M}_\chi(F)/m_\chi r(F))^{1/\varphi(g_\chi)}$; considérons $\Phi(\ldots, \varepsilon_o^\sigma, \ldots)$; il existe une constante μ_Φ telle que

$$|\Phi(\ldots, \varepsilon_o^\sigma, \ldots)| \leq \mu_\Phi \underset{\sigma \in G_\chi}{\text{Max}} (|\varepsilon_o^\sigma|^{d_\Phi})$$

et on suppose qu'il existe une constante M_Φ telle que $M_\Phi > \mu_\Phi$ et telle que $|\Phi(\ldots, \varepsilon_o^\sigma, \ldots)| \geq M_\Phi$; (en pratique, cette condition doit être vérifiée pour toute unité ε) ; donc

$$\underset{\sigma \in G_\chi}{\text{Max}} (|\varepsilon_o^\sigma|^{d_\Phi}) \geq \frac{M_\Phi}{\mu_\Phi} > 1$$

et comme log est une fonction croissante,

$$\underset{\sigma \in G_\chi}{\text{Max}} (\log |\varepsilon_o^\sigma|) \geq \frac{1}{d_\Phi} \log \frac{M_\Phi}{\mu_\Phi} > 0 \ ;$$

en comparant avec la 1ère inégalité, on obtient

$$(\frac{1}{d_\Phi} \log \frac{M_\Phi}{\mu_\Phi})^{\varphi(g_\chi)} \leq 2^{\varphi(g_\chi)} \frac{\mathcal{M}_\chi(F)}{m_\chi r(F)} ,$$

soit

$$r(F) \leq \frac{\mathcal{M}_\chi(F)}{m_\chi} (\frac{1}{2d_\Phi} \log \frac{M_\Phi}{\mu_\Phi})^{-\varphi(g_\chi)} .$$

Cas particulier : Si $K/\mathbb{Q}$ est cubique, cyclique, prenons

$$\Phi(x_1, x_\sigma, x_{\sigma^2}) = (x_1 + jx_\sigma + j^2 x_{\sigma^2})(x_1 + j^2 x_\sigma + j\, x_{\sigma^2}) ,$$
$$j^3 = 1 ;$$

on vérifie que $M_\Phi = f$, $\mu_\Phi = 4$, $m_\chi = 4\sqrt{3}$ et $\mathcal{M}_\chi(F_\chi) = \sqrt{3}\,\mathcal{R}(\eta)$, $\mathcal{R}$ désignant le régulateur ; il en résulte que $h \leq 4\,\mathcal{R}(\eta)/(\log f/4)^2$.

Remarque : Cette majoration améliore légèrement celle trouvée dans [2], par une autre méthode. En fait, la méthode utilisée dans [2] conduit aussi à la même majoration à condition d'utiliser les meilleures constantes possibles.

III - CALCULS EXPLICITES DES CONSTANTES

La majoration obtenue dans le II ne présente d'intérêt que si l'on sait calculer de manière effective les constantes $\mathcal{M}_\chi(F)$, m_χ , M_Φ et μ_Φ .

1. CALCUL DE $\mathcal{M}_\chi(F)$ et m_χ .

Soit $\gamma_\chi = (g_\chi \varphi(g_\chi)/d_\chi)^{1/2}$, où d_χ désigne le discriminant de $\mathbb{Q}^{(g_\chi)}$; on montre que :

(i) $\mathcal{M}_\chi(F) = R_\chi(F)/\gamma_\chi$, $R_\chi(F)$ désignant le χ-régulateur de F [3] (différent du régulateur ; par exemple si $g_\chi = \ell$, nombre premier, $R_\chi(F) = \ell \mathcal{R}_\chi(F)$, $\mathcal{R}_\chi(F)$ désignant le régulateur de F) .

(ii) $m_\chi = \gamma_\chi \nu_\chi$, ν_χ désignant le volume du domaine de $\mathbf{R}^{g_\chi}$ conte-

nu dans le cube $|x_\sigma| \leq 1$, $\sigma \neq 1$. Ce volume ne se calcule simplement que si $g_\chi = \ell$ et alors $\gamma_\chi = 2^{\ell-1}$.

Si $g_\chi = \ell$, on a donc $m_\chi(F)/m_\chi = R_\chi(F)/2^{\ell-1}$.

2. CALCUL DE M_Φ .

a) Φ = discriminant Δ_χ ; $\Delta_\chi(\ldots,x_\sigma,\ldots) = \left| \prod_{\substack{\sigma,\tau\in G_\chi \\ \sigma\neq\tau}} (x_\sigma - x_\tau) \right|$.

On a le résultat suivant : si ε est une unité χ-relative autre que ± 1, alors ε est primitive et $\Delta_\chi(\ldots,\varepsilon^\sigma,\ldots) \geq \Delta(K_\chi)$.

b) Φ = résolvante de Lagrange ; soit ψ' un caractère complexe de G_χ ; on pose $\langle x,\psi'\rangle = \sum_{\sigma\in G_\chi} \psi'(\sigma^{-1})x_\sigma$, $\psi'(\sigma^{-1})$ racine g_ψ ième de 1 et on pose $N_\psi^\chi(x) = \prod_{\psi'\in\tilde{\psi}} \langle x,\psi'\rangle$. C'est une fonction polynomiale homogène de degré $\varphi(g_\psi)$; on démontre les résultats suivants :

(i) Si θ est un élément primitif et entier de K_χ et si $\langle\theta,\psi'\rangle \neq 0$, alors $|N_\psi^\chi(\ldots,\theta^\sigma,\ldots)| \geq f_\psi^{\varphi(g_\psi)/2}$.

(ii) Soit θ un élément primitif de K_χ ; pour tout sous-corps strict k de K_χ , il existe un caractère ψ' de G_χ non trivial sur $\mathrm{Gal}(K_\chi/k)$ tel que $\langle\theta,\psi'\rangle \neq 0$ pour tout $\psi' \in \tilde{\psi}$.

Cas particulier : Si $g_\chi = \ell^n$, alors pour tout élément primitif θ de K_χ , on a $\langle\theta,\chi\rangle \neq 0$; alors $|N_\chi^\chi(\ldots,\theta^\sigma,\ldots)| \geq f_\chi^{\varphi(g_\chi)/2}$.

3. CALCUL DE μ_Φ .

a) Discriminant : On pose $\mu_{\Delta_\chi} = \delta_n$, avec $n = g_\chi$; on montre que $\delta_2 = 4$ et pour tout $n \geq 2$, $\delta_{n+1} = \dfrac{(n+1)^{(n+1)}(n-1)^{(n-1)}}{(2n-1)^{(2n-1)}}\,\delta_n$.

Les premières valeurs de δ_n sont : $\delta_2 = 4$, $\delta_3 = 4$, $\delta_4 = 2^{12}/5^5$,

$\delta_5 = 2^{12}3^3/7^7$; on vérifie que $\delta_{n+1}/\delta_n \sim 2ne/4^n$ et que la condition $M_\Phi/\mu_\Phi > 1$ est toujours vérifiée, quel que soit l'extension K considérée.

b) Résolvante de Lagrange N_χ^χ : On montre que pour $\Phi = N_\chi^\chi$,

$$\mu_\Phi \leq \left(\frac{g_\chi^2}{\varphi(g_\chi)}\left(1-\frac{1}{\ell^2}\right)\right)^{\frac{\varphi(g_\chi)}{2}} ,$$

où ℓ est le plus petit diviseur premier impair de g_χ (si g_χ est une puissance de 2 , on a seulement

$$\mu_\Phi \leq \left(\frac{g_\chi^2}{\varphi(g_\chi)}\right)^{\frac{\varphi(g_\chi)}{2}}) .$$

Cas particulier : Si $K/\mathbb{Q}$ est cyclique de degré premier impair ℓ , alors $\mu_\Phi \leq (\ell+1)^{\frac{\ell-1}{2}}$, $M_\Phi = f^{\frac{\ell-1}{2}}$, $m_\chi(F_\chi)/m_\chi = R(\eta)/2^{\ell-1}$, $h_K = h_\chi$ où χ est l'unique caractère rationnel irréductible non trivial de K , d'où

$$\boxed{h_K \leq \frac{R(\eta)}{(\log\sqrt{\frac{f}{\ell+1}})^{\ell-1}}} .$$

IV - CALCUL DU NOMBRE DE CLASSES DE K .

1. DEVISSAGE DES UNITES CYCLOTOMIQUES.

Soit $\chi \neq 1$ un caractère fixé de K . On reconnait si un nombre algébrique est puissance $q^{\text{ième}}$ dans K_χ grâce à la propriété suivante :

LEMME 1. Soit θ un entier primitif de K_χ et soit $q \in \mathbb{Z}$, $q > 1$. On suppose que lorsque q est pair, alors on a $\theta \gg 0$ (θ totalement positif). Pour tout $\sigma \in G_\chi$, on pose $t_\sigma = (\theta^\sigma)^{1/q}$ (pour q pair, $t_\sigma = \sqrt[q]{\theta^\sigma} > 0$; pour q impair t_σ est la racine $q^{\text{ième}}$ réelle de θ^σ) :

(i) Dans le cas q impair, une condition nécessaire et suffisante pour que les nombres t_σ appartiennent à K_χ est que le polynôme $P = \prod_{\sigma \in G_\chi} (X - t_\sigma)$ soit à coefficients entiers rationnels. Lorsque cette condition est réalisée, alors $t_\sigma = t_1^\sigma$, pour tout $\sigma \in G_\chi$.

(ii) Dans le cas q pair, une condition nécessaire et suffisante pour que les nombres t_σ appartiennent à K_χ est qu'il existe des nombres $\delta_\sigma \in \{-1, +1\}$ tels que le polynôme $P = \prod_{\sigma \in G_\chi} (X - \delta_\sigma t_\sigma)$ soit à coefficients entiers rationnels. Lorsque cette condition est réalisée, on a $t_\sigma = \delta_1 \delta_\sigma t_1^\sigma$.

Soit F un sous G_χ-module de E_χ, de même rang ; on a posé $r(F) = (|E_\chi| : |F|)$; soit $H(F)$ la constante qui majore $r(F)$ relativement à une fonction Φ. Supposons pour simplifier l'exposé que $\mathbb{Z}_\chi$ soit principal (lorsque $\mathbb{Z}_\chi$ n'est pas principal, l'algorithme existe, mais est plus compliqué à décrire). Dans ce cas, on peut trouver une $\mathbb{Z}_\chi$-base de F notée η. Soit p un nombre premier, soit n_p son degré résiduel dans $\mathbb{Z}_\chi$ et soit $H_\chi = \mathrm{Gal}(\mathbb{Q}_\chi/\mathbb{Q})$; comme $\mathbb{Z}_\chi$ est supposé principal, on peut trouver un entier $\omega \in \mathbb{Z}_\chi$ de norme $\pm p^{n_p}$; on a la proposition :

PROPOSITION 1. Les conditions suivantes sont équivalentes :

(i) p divise $r(F)$

(ii) p^{n_p} divise $r(F)$

(iii) il existe un élément $\omega \in \mathbb{Z}_\chi$ de norme $\pm p^{n_p}$ et une unité $\varepsilon \in E_\chi$ tels que $\eta^\Omega = \varepsilon^{n_p}$, où $\Omega = \prod_{\substack{s \in H_\chi \\ s \neq 1}} \omega^s$.

Elle résulte trivialement du fait qu'on a des modules libres de dimension 1 sur $\mathbb{Z}_\chi$.

On a enfin le lemme :

LEMME 2. Soit $\eta \in E_\chi$; on suppose que $\eta = \epsilon^q$, $q \in \mathbb{Z}$, $q > 1$, $\epsilon \in K_\chi^*$; alors ϵ est un élément de E_χ .

Les résultats ci-dessus conduisent à l'algorithme suivant (lorsque $\mathbb{Z}_\chi$ est principal) :

ALGORITHME. Appelons $H(F)$ la constante définie par le théorème du §2 . On part de l'unité $\eta_1 = \eta_\chi$ qui engendre $F_1 = F_\chi$; pour les nombres premiers p_1 (considérés par ordre croissant) tels que $p_1^{np_1} \leq H(F_1)$, on teste la divisibilité de $r(F_1)$ par $p_1^{np_1}$ au moyen du lemme 1 et de la proposition 1 . Si le test est toujours négatif, alors $r(F_1) = h_\chi = 1$. Dans le cas contraire, on a trouvé p_1 minimum tel que $p_1^{np_1}$ divise $r(F_1)$. Soit η_2 l'unité (de E_χ nécessairement, en vertu du lemme 2) telle que $\eta_1^{\Omega_1} = \eta_2^{p_1^{np_1}}$ (notations de la proposition 1) et soit F_2 le G_χ-module engendré par η_2 (on a $(|F_2|:|F_1|) = p_1^{np_1}$ et $(|E_\chi|:|F_2|) = r(F_2)$ est égal à $h_\chi/p_1^{np_1}$) . On est alors ramené intégralement à un problème identique à partir de F_2 au lieu de F_1 ; $H(F_2)$ est égal à $H(F_1)/p_1^{np_1}$ et on effectue les tests de divisibilité relatifs aux nombres premiers $p_2 \geq p_1$ tels que $p_2^{np_2} \leq H(F_2)$. Lorsque $H(F_n)$ devient inférieur strictement à $p_n^{np_n}$ pour la dernière valeur p_n considérée, on est sûr que $r(F_n) = 1$, autrement dit que $F_n = E_\chi$. On a ainsi un générateur de E_χ (c'est η_n) et la valeur de h_χ ,

$$h_\chi = \prod_{j=1}^{n} p_j^{np_j} .$$

2. CALCUL DE h_K ET DETERMINATION DE E_K .

La formule donnant le nombre de classes de K est $h_K = \frac{Q_K}{Q_G} \prod_{\chi \neq 1} h_\chi$. Ayant déterminé le produit des h_χ , il reste à trouver h_K , donc à calculer Q_K/Q_G . D'après Leopoldt, $Q_G = (g^{g-2}/\prod_\chi d_\chi)^{1/2}$ et $Q_K = (|E_K|:|E^K|)$, où $|E^K| = \bigoplus_{\chi \neq 1} |E_\chi|$ vient d'être trouvé ; la détermination de $|E_K|$ est donc un problème de dévissage ; il est plus délicat, car on n'a plus les

structures de $\mathbb{Z}_\chi$-modules, mais on sait que les diviseurs premiers possibles de Q_K à considérer sont 2 et les diviseurs de $g = [K:\mathbb{Q}]$. Remarquons que dans le cas cyclique de degré premier, $Q_K/Q_G = 1$.

Cette méthode doit pouvoir, à priori, traiter les extensions abéliennes réelles de degré quelconque. Bien entendu, le temps de calcul sur ordinateur ainsi que les ordres de grandeur des nombres manipulés sont des fonctions rapidement croissantes du degré et du conducteur, et les limites sont dues à des problèmes de programmation.

-o-o-

BIBLIOGRAPHIE

[1] GRAS G. et GRAS M.N. - Calcul du nombre de classes et des unités des extensions abéliennes réelles de $\mathbb{Q}$, à paraître.

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

[3] LEOPOLDT H.W. - Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper, Abh. Deutsche Akad. Wiss, Berlin, Math. 2 (1954).

[4] ORIAT B. - Exposé sur "Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper" de Leopoldt, séminaire de Théorie des Nombres de Besançon (1974).

[5] SERRE J.P. - Représentations linéaires des groupes finis". Hermann, Paris (1967).

-o-o-