BULLETIN DE LA S. M. F.

GEORGES GRAS

Critère de parité du nombre de classes des extensions abéliennes réelles de Q de degré impair

Bulletin de la S. M. F., tome 103 (1975), p. 177-190

<http://www.numdam.org/item?id=BSMF_1975__103__177_0>

Bull. Soc. math. France,
103, 1975, p. 177-190.

CRITÈRE DE PARITÉ DU NOMBRE DE CLASSES DES EXTENSIONS ABÉLIENNES RÉELLES DE Q DE DEGRÉ IMPAIR

PAR

GEORGES GRAS

[Besançon]

RÉSUMÉ. — Ce travail établit un critère de parité du nombre de classes au sens ordinaire des extensions abéliennes réelles $K/\mathbf{Q}$ de degré impair. Ce critère est tout à fait effectif, et son utilisation pratique ne nécessite que la connaissance numérique :

(i) du conducteur f de K,

(ii) du sous-groupe de $(\mathbf{Z}/f\mathbf{Z})^*$ qui correspond canoniquement à K.

Sa démonstration utilise à la fois, et de façon essentielle, la théorie du corps de classes et la formule analytique du nombre de classes, cette dernière conduisant à l'étude des unités cyclotomiques (au sens de LEOPOLDT) du corps K. L'utilisation d'une propriété de ces unités cyclotomiques permet de caractériser la parité du nombre de classes au moyen de leurs seules signatures. La définition même des unités cyclotomiques de Leopoldt montre clairement que le critère obtenu ne dépend que des caractéristiques arithmétiques élémentaires du corps K, précisées au début de ce résumé.

Introduction

Dans un travail en commun avec Marie-Nicole GRAS [1], nous avons démontré une propriété remarquable du « quotient de Fermat » des unités cyclotomiques des corps cyclotomiques $\mathbf{Q}^{(m)}$, m impair, et déduit un critère simple de parité du nombre de classes (au sens ordinaire) des extensions cycliques de degré premier impair de $\mathbf{Q}$, ne faisant intervenir que la signature des unités cyclotomiques. Nous avions limité notre étude au cas cyclique de degré premier car l'interprétation arithmétique du nombre de classes utilisée était celle donnée primitivement par HASSE; or elle n'est pas générale. Celle de LEOPOLDT [2] valable pour une

extension abélienne quelconque permet de généraliser au cas abélien de degré impair le critère en question ([1], th. III. 2).

Je tiens à remercier ici B. ORIAT qui, en exposant les résultats de [2] au *Séminaire de Théorie des Nombres* de Besançon, m'en a considérablement facilité la compréhension.

I. Énoncé des principaux résultats

Soit $K/\mathbf{Q}$ une extension abélienne réelle de degré impair g à groupe de Galois G, et soit h_K le nombre de classes au sens ordinaire de K. Soient F (resp. F_+ et F_0) les groupes des unités cyclotomiques de K (resp. totalement positives et ayant un « quotient de Fermat » nul modulo 2) (*cf.* § II.2, et § III.4).

On établit facilement que h_K est pair si, et seulement si, $F_+ \cap F_0 \neq F^2$ (*cf.* th. III.1). Le résultat essentiel est alors le suivant (*cf.* th. III.2) :

Si $\bar{e}$ *est un idempotent de* $\mathscr{A} = \mathbf{F}_2[G]/\sum_{\sigma\in G}\sigma$, *on a* $(F/F^2)^{\bar{e}} \subset F_+/F^2$ *si, et seulement si,* $(F/F^2)^{\pi(\bar{e})} \subset F_0/F^2$, *où* π *est l'automorphisme de* $\mathscr{A}$ *induit par l'application* $\sigma \to \sigma^{-1}$ *sur* G.

Un corollaire à ce résultat est que la parité de h_K ne dépend que de F_+ : de façon précise, h_K est pair si, et seulement si, il existe un idempotent $\bar{e}$ de $\mathscr{A}$ tel que les deux sous-modules (non triviaux) $(F/F^2)^{\bar{e}}$ et $(F/F^2)^{\pi(\bar{e})}$ soient contenus dans F_+/F^2.

L'intérêt de ce critère est de ramener l'étude de la parité de h_K au calcul (élémentaire) des signatures des unités cyclotomiques.

II. Résultats de Leopoldt sur le nombre de classes des corps abéliens

Soit $K/\mathbf{Q}$ une extension abélienne réelle de degré g impair et de groupe de Galois G. Le degré de $K/\mathbf{Q}$ étant impair, il résulte de la théorie des groupes de ramification ([6], p. 75) que le conducteur f de K est impair.

1. Caractères et idempotents

(*a*) *Caractères de G.* — Soit $\mathfrak{X}$ l'ensemble des caractères de G irréductibles sur $\mathbf{Q}$; nous noterons ses éléments par χ, ψ, ... Soit $\mathfrak{X}'$ le groupe des caractères complexes de G de degré 1 dont les éléments

seront désignés par χ', ψ', ... Les éléments de $\mathfrak{X}$ sont obtenus de la manière suivante ([5], § 12) :

Disons que deux éléments χ' et ψ' de $\mathfrak{X}'$ sont conjugués s'ils engendrent le même sous-groupe de $\mathfrak{X}'$ (il revient au même de dire qu'ils ont le même noyau); notons $\tilde{\chi}$ la classe de χ' pour cette relation d'équivalence. Alors $\chi = \sum_{\chi' \in \tilde{\chi}} \chi'$ est un élément de $\mathfrak{X}$, et tout élément de $\mathfrak{X}$ est obtenu de cette façon. Le caractère unité est le même dans $\mathfrak{X}$ et $\mathfrak{X}'$, il sera noté 1.

Soit U_χ le noyau commun des $\chi' \in \tilde{\chi}$, et soit g_χ l'ordre commun des $\chi' \in \tilde{\chi}$ (on a $g_\chi = |\chi'(G)|$). Le sous-corps K_χ de K qui correspond à U_χ est une extension cyclique de $\mathbf{Q}$ de degré g_χ : on désigne par $G_\chi \simeq G/U_\chi$ le groupe de Galois de $K_\chi/\mathbf{Q}$ et par f_χ le conducteur de K_χ (f_χ est impair comme diviseur de f); f_χ est aussi appelé le conducteur de χ; f_χ est alors le plus petit entier tel que l'on ait $K_\chi \subset \mathbf{Q}^{(f_\chi)}$. Désignons enfin par σ_χ un élément de G tel que $\chi'(\sigma_\chi)$ engendre $\chi'(G)$ (l'image $\bar{\sigma}_\chi$ de σ_χ dans G_χ est donc un générateur de G_χ).

Remarque II.1. — Nous utiliserons souvent le fait suivant :

Soit $\chi \in \mathfrak{X}$, et soit H un sous-groupe de G non contenu dans U_χ. Alors si σ est un élément quelconque de G, on a

$$\sum_{\tau \in H} \chi(\tau\sigma) = 0.$$

(*b*) *L'algèbre* $\mathbf{Q}[G]$. — La décomposition de $\mathbf{Q}[G]$ en produit direct de sous-modules simples est obtenue au moyen des idempotents e_χ, $\chi \in \mathfrak{X}$,

$$e_\chi = \frac{1}{g} \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma;$$

les idéaux $\mathbf{Q}[G]e_\chi$ sont isomorphes aux corps cyclotomiques $\mathbf{Q}^{(g_\chi)}$, l'isomorphisme étant réalisé de la façon suivante : on vérifie que l'homomorphisme de $\mathbf{Q}[X]$ sur $\mathbf{Q}[G]e_\chi$, défini par $X \to \sigma_\chi e_\chi$, est surjectif, et a pour noyau le g_χ-ième polynôme cyclotomique; on a donc

$$\mathbf{Q}[G]e_\chi = \mathbf{Q}e_\chi[\sigma_\chi e_\chi] \simeq \mathbf{Q}^{(g_\chi)}.$$

Soit $\mathcal{O} = \mathbf{Z}[G][\ldots, e_\chi, \ldots]$ l'ordre de $\mathbf{Q}[G]$ obtenu par adjonction des idempotents à $\mathbf{Z}[G]$; $\mathcal{O}$ est l'ordre maximal de $\mathbf{Q}[G]$. Dans l'isomorphisme précédent $\mathcal{O}e_\chi$ a pour image l'anneau des entiers $\mathbf{Z}^{(g_\chi)}$ de $\mathbf{Q}^{(g_\chi)}$.

Donnons quelques propriétés des e_χ ([2], § 1 n° 2, et § 8 n° 4).

PROPOSITION II.1 :

(i) $e_\chi = \frac{1}{g}\sum_{\tau\in U_\chi}\tau\sum_{k=1}^{g_\chi}\chi(\sigma_\chi^{-k})\,\sigma_\chi^k$.

(ii) *Soit* $\delta_\chi = \sum_{\tau\in U_\chi}\tau\prod_{l\mid g_\chi,\ l\text{ premier}}(\sigma_\chi^{g_\chi/l}-1)\in\mathbf{Z}[G]$, *alors* $\delta_\chi e_\chi = \delta_\chi$.

(iii) *Soit* π *l'automorphisme de* $\mathbf{Q}[G]$ *induit par l'application* $\sigma\to\sigma^{-1}$ *dans* G; *alors* $\pi(e_\chi) = e_\chi$.

(*c*) *L'algèbre* $\mathbf{F}_2[G]$. — On sait que $\mathcal{O}$ est isomorphe à $\prod_{\chi\in\mathfrak{X}}\mathbf{Z}^{(g_\chi)}$, chaque facteur simple $\mathcal{O}e_\chi$ étant isomorphe à $\mathbf{Z}^{(g_\chi)}$. Par réduction modulo 2, et du fait que g est impair, on a $\mathbf{F}_2[G]\simeq\mathcal{O}/2\mathcal{O}$. Si $\bar{e}_\chi$ est l'image de e_χ dans $\mathbf{F}_2[G]$, alors

$$\mathbf{F}_2[G]\bar{e}_\chi\simeq\mathcal{O}e_\chi/2\mathcal{O}e_\chi\simeq\mathbf{Z}^{(g_\chi)}/2\mathbf{Z}^{(g_\chi)};$$

les idempotents $\bar{e}_\chi$ se décomposent sur $\mathbf{F}_2$: si n_χ est le nombre d'idéaux premiers $\mathfrak{p}_{\chi,i}$ au-dessus de (2) dans $\mathbf{Q}^{(g_\chi)}$, alors (2 n'étant pas ramifié dans $\mathbf{Q}^{(g_\chi)}$) on a

$$\mathbf{Z}^{(g_\chi)}/(2)\simeq\prod_{i=1}^{n_\chi}\mathbf{Z}^{(g_\chi)}/\mathfrak{p}_{\chi,i}.$$

Les facteurs simples de $\mathbf{F}_2[G]\bar{e}_\chi$ sont donc obtenus à partir de n_χ idempotents irréductibles $\bar{e}_{\chi,i}$ tels que $\bar{e}_\chi = \sum_{i=1}^{n_\chi}\bar{e}_{\chi,i}$, et en convenant que $\mathbf{F}_2[G]\bar{e}_{\chi,i}\simeq\mathbf{Z}^{(g_\chi)}/\mathfrak{p}_{\chi,i}$.

Remarque II.2. — Si M est un $\mathbf{Z}[G]$-module, nous noterons multiplicativement à gauche (resp. exponentiellement) la loi de module si la loi de groupe de M est additive (resp. multiplicative).

2. **Unités cyclotomiques** (d'après [2])

Soit E_K le groupe des unités de K de norme absolue 1 (E_K est donc un $\mathbf{Z}$-module libre et, d'après le théorème de Dirichlet, on sait que $\mathbf{Q}\otimes E_K$ est isomorphe à $\oplus_{\chi\neq 1}\mathbf{Q}[G]e_\chi$ et que E_K/E_K^2 est isomorphe à $\oplus_{\chi\neq 1}\mathbf{F}_2[G]\bar{e}_\chi$). Par commodité, on se place dans $E = \mathcal{O}\otimes E_K$ (*cf.* § 1 (*b*)); on a toujours

$$\mathcal{O}\otimes E_K/2\mathcal{O}\otimes E_K\simeq E_K/E_K^2$$

puisque E est un $\mathbf{Z}$-module libre tel que $(E : E_K)$ soit impair. Posons $E_\chi = E^{e_\chi}$; on a

$$E = \oplus_{\chi\in\mathfrak{X}}E_\chi \qquad\text{et}\qquad E_1 = \{1\}.$$

(*a*) DÉFINITION DE Θ_χ. — Soit $\chi \in \mathfrak{X}$, $\chi \neq 1$, de conducteur f_χ, et soit $\zeta_\chi = \exp(i\pi/f_\chi + i\pi)$; c'est une racine primitive f_χ-ième de l'unité. Soit $\Theta_\chi = \prod_{t \in \mathfrak{A}_\chi} (\zeta_\chi^t - \zeta_\chi^{-t})$, où $\mathfrak{A}_\chi$ est un système exact de représentants dans $\mathbf{Z}$ de $\mathrm{Gal}(\mathbf{Q}_0^{(f_\chi)}/K_\chi)$ (après avoir identifié $\mathrm{Gal}(\mathbf{Q}^{(f_\chi)}/K_\chi)$ à un sous-groupe de $(\mathbf{Z}/f_\chi\,\mathbf{Z})^*$).

[Le nombre $\Theta_\chi \in \mathbf{Q}^{(f_\chi)}$ ainsi défini est, au signe près, celui de LEOPOLDT ([2], p. 37, (2)).] On rappelle que le quotient de Θ_χ par un de ses conjugués est une unité de K_χ ([2], p. 39).

(*b*) DÉFINITION DE F. — Soit $\chi \neq 1$. Soit a premier à f_χ tel que le $\mathbf{Q}$-automorphisme σ_a de $\mathbf{Q}^{(f_\chi)}$, défini par $\zeta_\chi^{\sigma_a} = \zeta_\chi^a$, n'appartienne pas à $\mathrm{Gal}(\mathbf{Q}^{(f_\chi)}/K_\chi)$ (a dépend donc de χ); soient

$$\varepsilon_{\chi,a} = \frac{\zeta_\chi^a - \zeta_\chi^{-a}}{\zeta_\chi - \zeta_\chi^{-1}} \qquad \text{et} \qquad \eta_{\chi,a} = \Theta_\chi^{(\sigma_a - 1)\,\delta_\chi}.$$

On remarque que

$$\eta_{\chi,a} = \prod_{t \in \mathfrak{A}_\chi} \left(\frac{\zeta_\chi^{at} - \zeta_\chi^{-at}}{\zeta_\chi^t - \zeta_\chi^{-t}} \right)^{\delta_\chi} = (N_{\mathbf{Q}_0^{(f_\chi)}/K_\chi}\, \varepsilon_{\chi,a})^{\delta_\chi};$$

$\eta_{\chi,a}$ est un élément de E_K contenu dans K_χ. D'après la proposition II.1 (ii), on a dans E la relation $\eta_{\chi,a}^{e_\chi} = \eta_{\chi,a}$, ce qui montre que $\eta_{\chi,a} \in E_\chi$.

Soit $F_{\chi,a}$ le sous-module de E engendré par $\eta_{\chi,a}$, et soit F le sous-module de E engendré par les $F_{\chi,a}$ pour $\chi \in \mathfrak{X}$, $\chi \neq 1$. On a $F = \oplus_{\chi \neq 1} F_{\chi,a}$; F est un sous-$\mathbf{Z}$-module libre de E de même rang ([2], p. 39-40). Donc $\bar{\eta} = \prod_{\chi \neq 1} \bar{\eta}_{\chi,a}$ est une base de $\bar{F}$ sur $\mathbf{F}_2[G]/(\bar{e}_1)$.

Remarque II.3. — Comme les nombres a sont fixés une fois pour toutes pour chaque caractère $\chi \neq 1$, nous simplifions les notations en posant $\varepsilon_\chi = \varepsilon_{\chi,a}$, $\eta_\chi = \eta_{\chi,a}$ et $F_\chi = F_{\chi,a}$ (on peut d'ailleurs dans la pratique prendre les nombres a de telle façon que l'image de σ_a dans G soit égale à σ_χ).

PROPOSITION II.2. — *Soit h_K le nombre de classes au sens ordinaire de K. On a la congruence $h_K \equiv \prod_{\chi \neq 1} (E_\chi : F_\chi)$ modulo (2).*

Démonstration (les références citées sont relatives à [2]). — Elle résulte de l'interprétation arithmétique de h_K de Leopoldt. Avec les notations de [2], on a

$$h_K = \frac{2^{q^K}\, Q_K}{Q_G} \prod_{\chi \neq 1} h_\chi.$$

(th. 21, p. 41); on vérifie facilement que Q_G est impair (p. 11, (11)), que Q_K est impair (th. 6, p. 24) et que $q^K = 0$ (en effet q^K est défini (p. 23, (4)) par $q^K = \sum_{\chi \neq 1} q_\chi^K$, $0 \leqslant q_\chi^K \leqslant q_\chi$, et q_χ est nul d'après le théorème 7, p. 28).

Montrons maintenant que $(E_\chi : F_\chi) \equiv h_\chi$ modulo (2).

On a $h_\chi = (\mathbf{E}_\chi^+ : \mathbf{H}_\chi)$ (p. 41, (2)), où $\mathbf{E}_\chi^+$ désigne le groupe des unités χ-relatives propres modulo la torsion (p. 19), et $\mathbf{H}_\chi$ le sous-module engendré par l'unité $H_\chi = \Theta_\chi^{D_\chi}$ (p. 39, (5)); on remarque que $\delta_\chi = |U_\chi| D_\chi$ et que $\eta_\chi = H_\chi^{(\sigma_a - 1)|U_\chi|}$, et on vérifie facilement que $(\mathbf{H}_\chi : F_\chi)$ est impair.

Le groupe $\mathbf{E}_\chi^+$ coïncide ici avec $\mathbf{E}_\chi$ (th. 7, p. 28) groupe des unités χ-relatives; on a donc $\mathbf{E}_\chi \subset E_\chi$ (th. 1, p. 21). Soit $\mathbf{E}^K = \oplus_{\chi \neq 1} \mathbf{E}_\chi$; alors $(E_K : \mathbf{E}^K) = Q_K$ est impair (p. 24, (8) et (11)), donc $(E : \mathbf{E}^K)$ est impair; or

$$(E : \mathbf{E}^K) = (\oplus_{\chi \neq 1} E_\chi : \oplus_{\chi \neq 1} \mathbf{E}_\chi) = \prod_{\chi \neq 1} (E_\chi : \mathbf{E}_\chi);$$

donc, les $(E_\chi : \mathbf{E}_\chi)$ sont impairs, d'où le résultat.

III. Démonstrations des résultats sur la parité de h_K

1. Bases normales

Dans ce paragraphe, on fixe une fois pour toutes un caractère $\chi \in \mathfrak{X}$, $\chi \neq 1$.

Soit $\mathbf{Z}_{(2)}$ le localisé de $\mathbf{Z}$ en (2), et soit A (resp. B) la clôture intégrale de $\mathbf{Z}_{(2)}$ dans K_χ (resp. $Q^{(f_\chi)}$). D'après [4] (chap. II, § 6, p. 21), on a $A \simeq \mathbf{Z}_{(2)}[G_\chi]$ et, d'après [4] (th. II.1, p. 15), on a $\mathrm{Tr}_{Q^{(f_\chi)}/K_\chi}(B) = A$, car 2 est non ramifié dans $Q^{(f_\chi)}/K_\chi$. Posons $\theta_{\chi,d} = \mathrm{Tr}_{Q^{(f_\chi)}/K_\chi}(\zeta_\chi^d)$ pour tout d diviseur de f_χ; pour $d = 1$, on pose $\theta_{\chi,1} = \theta_\chi$.

(*a*) *Idempotents de* $\mathbf{Z}_{(2)}[G_\chi]$. — Si ψ'_0 est un caractère de degré 1 de G_χ dans C, soit ψ' le composé de ψ'_0 et de la projection canonique $G \to G_\chi$; alors $\psi' \in \mathfrak{X}'$, et on a $U_\chi \subset U_\psi$; dans cette correspondance, les éléments de $\tilde{\psi}_0$ correspondent bijectivement à ceux de $\tilde{\psi}$; par conséquent les caractères de G_χ irréductibles sur $\mathbf{Q}$ peuvent être regardés comme étant les éléments $\psi \in \mathfrak{X}$ tels que $U_\chi \subset U_\psi$, et les idempotents de $\mathbf{Z}_{(2)}[G_\chi]$ sont

$$e'_\psi = \frac{1}{g_\chi} \sum_{k=1}^{g_\chi} \psi(\sigma_\chi^{-k}) \bar{\sigma}_\chi^k.$$

pour ψ tel que $U_\chi \subset U_\psi$ ($\bar{\sigma}_\chi$ désignant l'image de σ_χ dans G_χ). Comme le remarque LEOPOLDT ([2], § 5), on peut encore noter e_ψ les idempotents de $\mathbf{Z}_{(2)}[G_\chi]$ en raison du fait suivant :

Décomposons G modulo U_χ; on a

$$e_\psi = \frac{1}{g}\sum_{\tau \in U_\chi} \tau \sum_{k=1}^{g_\chi} \psi(\sigma_\chi^{-k})\,\sigma_\chi^k ;$$

alors si M est un G-module sur lequel U_χ opère trivialement (donc un G_χ-module), on a pour tout $\alpha \in M$,

$$e_\psi \alpha = \frac{1}{g}\sum_{\tau \in U_\chi} \tau \sum_{k=1}^{g_\chi} \psi(\sigma_\chi^{-k})\,\sigma_\chi^k(\alpha) = \frac{1}{g_\chi}\sum_{k=1}^{g_\chi} \psi(\sigma_\chi^{-k})\,\sigma_\chi^k(\alpha) = e'_\psi \alpha.$$

On remarque enfin que l'on a

$$\mathbf{Z}_{(2)}[G_\chi]\, e'_\psi \simeq \mathbf{Z}_{(2)}[G]\, e_\psi \simeq \mathbf{Z}_{(2)}^{(g_\psi)}.$$

(*b*) *Étude de* $A\,e_\chi$. — Comme A est un G-module sur lequel U_χ opère trivialement et qui, en tant que G_χ-module, est isomorphe à $\mathbf{Z}_{(2)}[G_\chi]$, on aura $A = \bigoplus_\psi A\,e_\psi$, la somme étant étendue aux éléments $\psi \in \mathfrak{X}$ tels que $U_\chi \subset U_\psi$; chaque terme $A\,e_\psi$ est isomorphe à $\mathbf{Z}_{(2)}[G]\,e_\psi$, donc à $\mathbf{Z}_{(2)}^{(g_\psi)}$, et en particulier $A\,e_\chi \simeq \mathbf{Z}_{(2)}^{(g_\chi)}$.

PROPOSITION III.1. — *Le sous-module* $A\,e_\chi$, *considéré comme* $\mathbf{Z}_{(2)}[G]\,e_\chi$*-module* (*libre de dimension* 1), *admet* $e_\chi\,\theta_\chi$ *pour base.*

Démonstration. — Donnons une démonstration directe de ce résultat qui peut se déduire de [3] : Il suffit de montrer que $e_\chi\,\theta_\chi$ engendre $A\,e_\chi$; en effet, $\mathbf{Z}_{(2)}[G]\,e_\chi$ étant un anneau de Dedekind, ceci sera suffisant.

D'après la relation $\mathrm{Tr}_{\mathbf{Q}^{(f_\chi)}/K_\chi}(B) = A$, il en résulte que A est engendré sur $\mathbf{Z}_{(2)}$ par les $\theta_{\chi,d}$ pour d divisant f_χ (les ζ_χ^y, $y = 1, 2, \ldots, f_\chi$, engendrent B sur $\mathbf{Z}_{(2)}$). Si on montre que, pour tout $d \neq 1$, d divisant f_χ, $e_\chi\,\theta_{\chi,d} = 0$, il en résulte bien la proposition. Soit $d \neq 1$; on a $\theta_{\chi,d} = \mathrm{Tr}_{\mathbf{Q}^{(f_\chi)}/K_\chi}\zeta_\chi^d$ qui est un élément de $L = \mathbf{Q}^{(f_\chi/d)} \cap K_\chi$; soit $H = \mathrm{Gal}(K/L)$, on a $H \neq U_\chi$ sinon K_χ serait contenu dans $\mathbf{Q}^{(f_\chi/d)}$ et ne serait pas de conducteur f_χ, ce qui est absurde.

On a

$$e_\chi\,\theta_{\chi,d} = \frac{1}{g}\sum_{\tau \in H}\sum_{\sigma'} \chi(\tau^{-1}\sigma'^{-1})\,\sigma'(\theta_{\chi,d})$$

où $\sigma' \in G$ parcourt un système de représentants de G modulo H;

$$e_\chi \theta_{\chi,d} = \frac{1}{g} \sum_{\sigma'} \sigma'(\theta_{\chi,d}) \sum_{\tau \in H} \chi(\tau^{-1}\sigma'^{-1}) = 0$$

d'après la remarque II.1.

Remarque III.1. — Le G-module $A\, e_\chi / 2\, A\, e_\chi$ est isomorphe à $\mathbf{Z}^{(g_\chi)}/(2)$, et l'image de $e_\chi\, \theta_\chi$ dans $A\, e_\chi / 2\, A\, e_\chi$ est encore une $\mathbf{Z}^{(g_\chi)}/(2)$-base (autrement dit, si $\omega \in \mathbf{Z}_{(2)}[G]$ est tel que $\omega\, e_\chi\, \theta_\chi \equiv 0 \bmod 2\, A$, alors $\omega\, e_\chi\, \theta_\chi \equiv 0 \bmod 2\, A\, e_\chi$, et $\omega\, e_\chi \equiv 0 \bmod (2)$).

2. Signatures

On rappelle la définition de l'homomorphisme signature (surjectif), $S : K^* \to \mathbf{F}_2^g$, défini par $S(\alpha) = (s(\alpha^\sigma))_{\sigma \in G}$, où $s(\alpha^\sigma) = 0$ (resp. 1) si $\alpha^\sigma > 0$ (resp. < 0) (notation additive). On munit $S(K^*)$ d'une structure de $\mathbf{F}_2[G]$-module en posant $\tau(S(\alpha)) = S(\alpha^\tau)$. Soit alors $c = (c_\tau)_{\tau \in G}$ la signature définie par $c_1 = 1$ et $c_\tau = 0$ pour tout $\tau \neq 1$. On a alors la relation

$$S(\alpha) = \sum_{\sigma \in G} s(\alpha^{\sigma^{-1}})\, \sigma\, c = \left(\sum_{\sigma \in G} s(\alpha^{\sigma^{-1}})\, \sigma\right) c;$$

c est une base du $\mathbf{F}_2[G]$-module $S(K^*)$ qui est isomorphe à $\mathbf{F}_2[G]$.

3. Congruences de Kummer

Comme (2) est non ramifié dans $\mathbf{Q}^{(f)}$, pour tout $\alpha \in \mathbf{Q}^{(f)}$ premier à (2), on peut considérer son « quotient de Fermat »

$$\varphi(\alpha) = \frac{\alpha^{2^n - 1} - 1}{2},$$

où n est le degré résiduel de 2 dans $\mathbf{Q}^{(f)}/\mathbf{Q}$. Le quotient de Fermat de α est un élément de $\mathbf{Z}_2^{(f)}$, et on rappelle ([1], § 6, *c*)) le résultat suivant.

PROPOSITION III.2. — *L'extension* $\mathbf{Q}^{(f)}(\sqrt{\alpha})$ *est non ramifiée en* (2) *si, et seulement si, le quotient de Fermat de* α *est congru à* 0 *modulo* (2) *dans* $\mathbf{Z}_{(2)}^{(f)}$.

Nous noterons donc $\bar{\varphi}(\alpha)$ l'image dans $\mathbf{Z}_{(2)}^{(f)}/(2)$ du quotient de Fermat de α. On rappelle que $\bar{\varphi}$ est un homomorphisme de $\mathrm{Gal}(\mathbf{Q}^{(f)}/\mathbf{Q})$-modules du groupe formé des α premiers à (2) dans $\mathbf{Z}_{(2)}^{(f)}/(2)$.

4. Critère de parité de h_K

(*a*) DÉFINITION. — Soit $\bar{F} = F/F^2$; si $\eta \in F$, son image dans $\bar{F}$ sera notée $\bar{\eta}$. On définit les sous-G-modules suivants :

$$F_+ = \{\eta \in F;\ S(\eta) = (0)\}, \qquad F_0 = \{\eta \in F;\ \bar{\varphi}(\eta) = 0\};$$

on note $\bar{F}_+$, $\bar{F}_0$ leurs images dans $\bar{F}$ (on remarque que

$$\bar{F}_+ \cap \bar{F}_0 = (F_+ \cap F_0)/F^2).$$

On sait que $\bar{F} \simeq \oplus_{\chi \neq 1} \oplus_{i=1}^{n_\chi} \mathbf{F}_2[G]\,\bar{e}_{\chi,i}$; il en résulte que les $\bar{F}^{\bar{e}_{\chi,i}}$ sont des sous-modules simples distincts et que tout sous-module de $\bar{F}$ est égal à une somme directe de tels modules simples distincts.

On peut donc poser :

$$\bar{F}_+ = \oplus_{\chi \neq 1} \oplus_{i \in I_\chi} \bar{F}^{\bar{e}_{\chi,i}} \qquad \text{et} \qquad \bar{F}_0 = \oplus_{\chi \neq 1} \oplus_{j \in J_\chi} \bar{F}^{\bar{e}_{\chi,j}},$$

où I_χ et J_χ sont des sous-ensembles de $\{1, 2, \ldots, n_\chi\}$.

On a

$$\bar{F}^{\bar{e}_{\chi,i}} = \bar{F}^{\bar{e}_\chi \bar{e}_{\chi,i}} = \bar{F}_\chi^{\bar{e}_{\chi,i}},$$

par conséquent $\bar{F}_\chi$ est engendré par $\bar{\eta}_\chi$, et $\bar{F}^{\bar{e}_{\chi,i}} = \bar{\eta}_\chi^{\mathbf{F}_2[G]\bar{e}_{\chi,i}}$.

PROPOSITION III.3. — *On a*

$$I_\chi = \{i \in \{1, 2, \ldots, n_\chi\};\ \bar{e}_{\chi,i} S(\eta_\chi) = (0)\}$$

et

$$I_\chi = \{j \in \{1, 2, \ldots, n_\chi\},\ \bar{e}_{\chi,i} \bar{\varphi}(\eta_\chi) = 0\},$$

pour $\chi \neq 1$.

Démonstration. — On aura $i \in I_\chi$ si et seulement si $\bar{\eta}_\chi^{\bar{e}_{\chi,i}} \in \bar{F}_+$ (car les $\bar{\eta}_\chi^{\mathbf{F}_2[G]\bar{e}_{\chi,i}}$ sont des sous-modules simples), donc si et seulement si, $\eta_\chi^{e_{\chi,i}} \in F_+$ (où $e_{\chi,i}$ est un représentant quelconque de $\bar{e}_{\chi,i}$ dans $\mathbf{Z}[G]$), donc si, et seulement si, $\bar{e}_{\chi,i} S(\eta_\chi) = (0)$. Même démonstration pour J_χ.

(*b*) CRITÈRE GÉNÉRAL DE PARITÉ

THÉORÈME III.1. — *Une condition nécessaire et suffisante pour que* h_K *soit pair est qu'il existe* $\eta \in F$ *telle que* $\eta \in (F_+ \cap F_0) \setminus F^2$.

Démonstration. — Si h_K est pair, alors d'après la proposition II.2, il existe $\chi \neq 1$ tel que $(E_\chi : F_\chi)$ soit pair, et il existe $\varepsilon \in E_\chi$ telle que $\eta = \varepsilon^2 \in F_\chi \setminus F_\chi^2$; on a bien

$$\eta \in (F_+ \cap F_0) \setminus F^2 \quad (F = \oplus_{\chi \neq 1} F_\chi).$$

Inversement, si une telle unité η existe, alors il y a deux cas :

Si η est un carré dans K, c'est le carré d'une unité ε; on aura $\eta = \varepsilon^2$, $\varepsilon \in E/F$, et $(E : F) = \prod_{\chi \neq 1} (E_\chi : F_\chi)$ est pair.

Si η n'est pas un carré dans K, alors l'extension $K(\sqrt{\eta})/K$ est quadratique et non ramifiée en toute place finie ou non (*cf.* prop. III.2); par conséquent, le nombre de classes au sens ordinaire de K est pair. La détermination de $F_+ \cap F_0 \setminus F^2$ est équivalente à celle de

$$\overline{F}_+ \cap \overline{F}_0 = \overline{F_+ \cap F_0}.$$

(*c*) Quotient de Fermat de η_χ. — On rappelle que dans [1] nous avons établi une formule donnant le quotient de Fermat d'une unité de la forme

$$\varepsilon_a = \frac{\zeta^a - \zeta^{-a}}{\zeta - \zeta^{-1}}, \qquad \text{où} \quad \zeta = \exp(i\pi/m + i\pi) \quad \text{pour } m \text{ impair:}$$

$$\varphi(\varepsilon_a) \equiv \sum_{d \mid m,\, d \neq m} \sum_{\sigma \in \Gamma_{0,d}} s(\varepsilon_{a,d}^{\sigma})\, \sigma(\zeta^{ad} + \zeta^{-ad}) \bmod (2),$$

avec

$$\varepsilon_{a,d} = \frac{\zeta^{ad} - \zeta^{-ad}}{\zeta^d - \zeta^{-d}} \qquad \text{et} \qquad \Gamma_{0,d} = \mathrm{Gal}(\mathbf{Q}_0^{(m/d)}/\mathbf{Q}).$$

Appliquée à $m = f_\chi$, cette formule devient (*cf.* remarque II.3 pour les conventions de notation) :

$$\varphi(\varepsilon_\chi) \equiv \sum_{d \mid f_\chi\, d \neq f_\chi} \sum_{\sigma \in \Gamma_{0,\chi,d}} s(\varepsilon_{\chi,d}^{\sigma})\, \sigma(\zeta_\chi^{ad} + \zeta_\chi^{-ad}) \text{ modulo } (2),$$

où

$$\Gamma_{0,\chi,d} = \mathrm{Gal}(\mathbf{Q}_0^{(f_\chi/d)}/\mathbf{Q}) \qquad \text{et} \qquad \varepsilon_{\chi,d} = \frac{\zeta_\chi^{ad} - \zeta_\chi^{-ad}}{\zeta_\chi^d - \zeta_\chi^{-d}}$$

(on rappelle que a dépend de χ).

D'après les propriétés de φ, on peut écrire :

$$\begin{aligned}
\varphi(\eta_\chi) &\equiv \delta_\chi \mathrm{Tr}_{\mathbf{Q}_0^{(f_\chi)}/K_\chi}(\varphi(\varepsilon_\chi)) \\
&\equiv \sum_{d \mid f_\chi\, d \neq f_\chi} \sum_{\sigma \in \Gamma_{0,\chi,d}} s(\varepsilon_{\chi,d}^{\sigma})\, \delta_\chi \mathrm{Tr}_{\mathbf{Q}_0^{(f_\chi)}/K_\chi}\, \sigma(\zeta_\chi^{ad} + \zeta_\chi^{-ad}) \\
&\equiv \sum_{d \mid f_\chi,\, d \neq f_\chi} \sum_{\sigma \in \Gamma_{0,\chi,d}} s(\varepsilon_{\chi,d}^{\sigma})\, \delta_\chi \sigma \sigma_a(\theta_{\chi,d}) \bmod (2);
\end{aligned}$$

comme $\eta_\chi^{e_\chi} = \eta_\chi$, il en résulte que $e_\chi \varphi(\eta_\chi) \equiv \varphi(\eta_\chi) \bmod (2)$; la nullité de $e_\chi \theta_{\chi,d}$ pour tout $d \neq 1$ (prop. III.1) entraîne alors :

$$\varphi(\eta_\chi) \equiv \sum_{\sigma \in \Gamma_{0,\chi}} s(\varepsilon_\chi^\sigma)\, \delta_\chi \sigma_a \sigma(\theta_\chi) \bmod (2),$$

où $\Gamma_{0,\chi} = \Gamma_{0,\chi,1} = \mathrm{Gal}(\mathbf{Q}_0^{(f_\chi)}/\mathbf{Q})$ et $\varepsilon_\chi = \varepsilon_{\chi,1}$.

Soit $H = \mathrm{Gal}(\mathbf{Q}_0^{(f_\chi)}/K_\chi)$, alors :

$$\begin{aligned}\varphi(\eta_\chi) &\equiv \sum_{\tau \in H, \bar{\sigma} \in G_\chi} s(\varepsilon_\chi^{\tau\sigma})\, \delta_\chi \sigma_a \sigma(\theta_\chi)\\ &\equiv \sum_{\bar{\sigma} \in G_\chi} s(N_{\mathbf{Q}_0^{(f_\chi)}/K_\chi}\, \varepsilon_\chi^\sigma)\, \delta_\chi \sigma_a \sigma(\theta_\chi)\\ &\equiv \sum_{\bar{\sigma} \in G_\chi} s(\varepsilon_\chi'^\sigma)\, \delta_\chi \sigma_a \sigma(\theta_\chi) \bmod (2), \qquad \text{où} \quad \varepsilon_\chi' = N_{\mathbf{Q}_0^{(f_\chi)}/K_\chi}(\varepsilon_\chi).\end{aligned}$$

PROPOSITION III.4. — *On a les relations suivantes, pour tout* $\chi \neq 1$,

$$\varphi(\eta_\chi) \equiv \sum_{\sigma \in G_\chi} s(\eta_\chi)\, \sigma_0 \sigma(\theta_\chi) \bmod (2), \qquad \text{où} \quad \sigma_0 = \sigma_a \prod_{l \mid g_\chi\, l \text{ premier}} \sigma_\chi^{g_\chi/l}$$

Démonstration. — Posons $\delta_\chi = (\sigma' - 1)\, \delta_\chi'$, avec $\sigma' \in G_\chi$ de la forme $\bar{\sigma}_\chi^{g_\chi/l}$ (*cf.* prop. II.1, (ii));

$$\begin{aligned}\varphi(\eta_\chi) &\equiv \sum_{\sigma \in G_\chi} s(\varepsilon_\chi'^\sigma)\, \delta_\chi' (\sigma' - 1)\, \sigma_a \sigma(\theta_\chi)\\ &\equiv \sum_{\sigma \in G\chi} s(\varepsilon_\chi'^\sigma)\, \delta_\chi' \sigma_a \sigma\sigma'(\theta_\chi) - \sum_{\sigma \in G_\chi} s(\varepsilon_\chi'^\sigma)\, \delta_\chi' \sigma_a \sigma(\theta_\chi)\\ &\equiv \sum_{\tau \in G_\chi} s(\varepsilon_\chi'^{\tau\sigma'^{-1}})\, \delta_\chi' \sigma_a \tau(\theta_\chi) - \sum_{\sigma \in G_\chi} s(\varepsilon_\chi'^\sigma)\, \delta_\chi' \sigma_a \sigma(\theta_\chi)\\ &\equiv \sum_{\sigma \in G_\chi} (s(\varepsilon_\chi'^{\sigma\sigma'^{-1}}) - s(\varepsilon_\chi'^\sigma))\, \delta_\chi' \sigma_a \sigma(\theta_\chi)\\ &\equiv \sum_{\sigma \in G_\chi} s(\varepsilon_\chi'^{(\sigma'^{-1}-1)\sigma})\, \delta_\chi' \sigma_a \sigma(\theta_\chi) \bmod (2);\end{aligned}$$

or $\sigma'^{-1} - 1 = \sigma'^{-1}(1 - \sigma')$ et $s(\varepsilon_\chi^{1-\sigma'}) = s(\varepsilon_\chi^{\sigma'^{-1}})$, d'où

$$\varphi(\eta_\chi) \equiv \sum_{\sigma \in G_\chi} s(\varepsilon_\chi'^{(\sigma'^{-1})\sigma})\, \delta_\chi' \sigma_a \sigma\sigma'(\theta_\chi);$$

d'où finalement :

$$\varphi(\eta_\chi) \equiv \sum_{\sigma \in G_\chi} s(\varepsilon_\chi'^{\delta_\chi \sigma})\, \sigma_0 \sigma(\theta_\chi) \equiv \sum_{\sigma \in G_\chi} s(\eta_\chi^\sigma)\, \sigma_0 \sigma(\theta_\chi) \bmod (2).$$

THÉORÈME III.2. — *Les notations étant celles introduites dans le paragraphe* III, 4, *on a, entre* $\bar{F}^+$ *et* $\bar{F}_0$, *la relation suivante :*

Si $\bar{F}_+ = \bigoplus_{\chi \neq 1} \bigoplus_{i \in I_\chi} \bar{F}^{e_{\chi,i}}$, *alors* $\bar{F}_0 = \bigoplus_{\chi \neq 1} \bigoplus_{i \in I_\chi} \bar{F}^{\pi(e_{\chi,i})}$.

Démonstration. — Comme $\eta_\chi \in K_\chi$, $\theta_\chi \in K_\chi$ et $|U_\chi| \equiv 1 \bmod (2)$, on a

$$\sum_{\sigma \in G_\chi} s(\eta_\chi^\sigma)\, \sigma_0 \sigma(\theta_\chi) \equiv \sum_{\sigma \in G} s(\eta_\chi^\sigma)\, \sigma_0 \sigma(\theta_\chi) \bmod (2).$$

On a

$$\varphi(\eta_\chi) \equiv \sum_{\sigma \in G} s(\eta_\chi^\sigma)\, \sigma_0\, \sigma(\theta_\chi) = \left(\sum_{\sigma \in G} s(\eta_\chi^\sigma)\, \sigma\right) e_\chi\, \sigma_0(\theta_\chi)$$

puisque

$$e_\chi\, \varphi(\eta_\chi) \equiv \varphi(\eta_\chi) \bmod (2); \qquad \varphi(\eta_\chi) \equiv \omega\, e_\chi\, \sigma_0(\theta_\chi) \bmod (2),$$

où $\omega = \sum_{\sigma \in G} s(\eta_\chi^\sigma)\, \sigma$. On sait (*cf.* § III, 1) que

$$S(\eta_\chi) = \left(\sum_{\sigma \in G} s(\eta_\chi^{\sigma^{-1}})\, \sigma\right) c = \pi(\omega)\, c = \pi(\omega)\, e_\chi\, c,$$

puisque $e_\chi\, S(\eta_\chi) = S(\eta_\chi)$. On a donc

$$\varphi(\eta_\chi) \equiv \omega\, e_\chi\, \sigma_0(\theta_\chi) \bmod (2) \qquad \text{et} \qquad S(\eta_\chi) = \pi(\omega)\, e_\chi\, c.$$

Or $\overline{F}^{e_{\chi,i}} \subset \overline{F}_0$ est équivalent à $e_{\chi,i}\, \varphi(\eta_\chi) \equiv 0 \bmod (2)$ (prop. III.3), soit $e_{\chi,i}\, \omega\, e_\chi\, \sigma_0(\theta_\chi) \equiv 0 \bmod (2)$, donc à $e_{\chi,i}\, \omega \equiv 0 \bmod (2)$ (remarque III.1); or on a $e_{\chi,i}\, \omega \equiv 0 \bmod (2)$ si, et seulement si, $\pi(e_{\chi,i})\, \pi(\omega) \equiv 0 \bmod (2)$, soit $\pi(e_{\chi,i})\, S(\eta_\chi) = (0)$, par conséquent, si, et seulement si, $\overline{F}^{\pi(e_{\chi,i})} \subset \overline{F}^+$, d'où le théorème.

IV. Conséquences du théorème précédent

COROLLAIRE IV.1. — *On a* $\dim_{\mathbf{F}_2} \overline{F}_0 = \dim_{\mathbf{F}_2} \overline{F}_+$.

COROLLAIRE IV.2. — *Une condition nécessaire et suffisante pour que* h_K *soit pair est qu'il existe un idempotent* $\bar{e}_{\chi,i}$, $\chi \neq 1$, $i \in \{1, 2, \ldots, n_\chi\}$ *tel que* $\bar{e}_{\chi,i}\, S(\eta_\chi) = \pi(\bar{e}_{\chi,i})\, S(\eta_\chi) = (0)$.

COROLLAIRE IV.3. — *Soit* $\overline{E}_K = E_K/E_K^2$, *et soit* $\overline{E}_{K+}$ *l'image dans* $\overline{E}_K$ *du sous-groupe des unités totalement positives. S'il existe* $\bar{e}_{\chi,i}$, $\chi \neq 1$, *tel que* $\overline{E}_K^{\bar{e}_{\chi,i}}$ *et* $\overline{E}_K^{\pi(e_{\chi,i})}$ *soient contenus dans* $\overline{E}_{K+}$ *alors* h_K *est pair.*

En effet, si h_K était impair, on aurait $(E : F)$ impair, soit $\overline{E} \simeq \overline{F}$ et $\overline{E}_+ \simeq \overline{F}_+$, et le corollaire IV.2 serait contradictoire.

Évidemment, dans le cas de $\overline{E}_K$, la condition n'est nullement nécessaire comme le montre l'exemple du corps cubique K de conducteur 163 ($\overline{E}_{K+} = \{1\}$ et h_K pair).

Remarque IV.1. — Les unités η_χ s'obtiennent comme des produits de sinus ou d'inverses de sinus de la forme $\sin((\pi/f_\chi + \pi)\, r)$, r premier à f_χ; le calcul de la signature de η_χ est alors immédiat (*cf.* [1], lemme II.6).

Remarque IV.2. — Le critère de parité peut se simplifier dans certains cas compte tenu du résultat suivant : si la conjugaison complexe appartient au groupe de décomposition de 2 dans $\mathbf{Q}^{(g_\chi)}/\mathbf{Q}$, on a $\pi(\bar{e}_{\chi,i}) = \bar{e}_{\chi,i}$ pour tout $i = 1, 2, \ldots, n_\chi$; sinon π opère en permutant deux par deux les éléments de $\{\bar{e}_{\chi,i}\}_{i=1,2,\ldots,n_\chi}$.

Remarque IV.3. — Étant donné un corps K, l'ensemble des sous-corps K_χ ($\chi \in \mathfrak{X}$) coïncide avec l'ensemble des sous-corps de K qui sont cycliques sur $\mathbf{Q}$; de plus, $[K : \mathbf{Q}]$ étant impair, si L est un sous-corps de K ayant un nombre de classes pair, alors h_K est pair : une condition nécessaire et suffisante pour que h_K soit pair est qu'il existe un sous-corps cyclique de K ayant un nombre de classes pair. Il suffit donc en pratique de traiter le cas des extensions cycliques de degré impair de $\mathbf{Q}$. Par exemple l'étude de la parité du nombre de classes des extensions d'exposant l (l premier impair) se ramène à celle des extensions cycliques de degré l.

Remarque IV.4. — En ce qui concerne le nombre de classes au sens restreint, on vérifie facilement qu'il est pair si, et seulement si, $\overline{F}_+ \neq \{1\}$.

Exemple numérique (obtenu en collaboration avec M.-N. GRAS). — Une étude numérique portant sur les extensions $K/\mathbf{Q}$, abéliennes de degré 15 et de conducteur premier, a donné l'exemple suivant : si on écarte le cas des extensions pour lesquelles la parité de h_K ne provient que de celle du nombre de classes de l'un des deux sous-corps de K, alors le premier exemple rencontré (pour les conducteurs f croissants) l'est pour $f = 18\,121$; le nombre de classes de K est pair (donc divisible par 8) tandis que les nombres de classes du sous-corps cubique et du sous-corps de degré 5 de K sont impairs.

BIBLIOGRAPHIE

[1] GRAS (Georges) et GRAS (Marie-Nicole). — Signature des unités cyclotomiques et parité du nombre de classes des extensions cycliques de $\mathbf{Q}$ de degré premier impair, *Ann. Inst. Fourier, Grenoble*, t. 25, 1975, fasc. 1.

[2] LEOPOLDT (H. W.). — Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper, *Abh. Deutsche Akad. Wiss. Berlin, Kl. Math.*, 1953, n° 2, 48 p.

[3] LEOPOLDT (H. W.). — Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, *J. reine angew. Math.*, t. 201, 1959, p. 119-149.

[4] MARTINET (J.). — Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre $2p$, *Ann. Inst. Fourier*, Grenoble, t. 19, 1969, fasc. 1, p. 1-80.

[5] SERRE (J.-P.). — *Représentations linéaires des groupes finis.* — Paris, Hermann, 1967 (*Collection Méthodes*).

[6] SERRE (J.-P.). — *Corps locaux.* — Paris, Hermann, 1962 (*Act. scient. et ind.*, 1296).

(Texte reçu le 3 février 1975.)

Georges GRAS,
Mathématiques,
Université de Besançon,
25030 Besançon Cedex.