Astérisque

GEORGES GRAS

Parité du nombre de classes et unités cyclotomiques

Astérisque, tome 24-25 (1975), p. 37-45

<http://www.numdam.org/item?id=AST_1975__24-25__37_0>

Société Mathématique de France
Astérisque 24-25 (1975)

PARITÉ DU NOMBRE DE CLASSES ET UNITÉS CYCLOTOMIQUES

par

Georges GRAS

(D'après un travail en commun avec Marie-Nicole GRAS)

-:-:-:-

I. - INTRODUCTION. - Le nombre de classes h au sens ordinaire des extensions réelles est inaccessible, dès qu'on sort du cadre des extensions de "petit" degré ; on a souvent cherché à répondre au problème plus restreint suivant :

est-ce que $h \equiv 0 \mod p$, p premier ?

Dans le cas d'une extension abélienne réelle K , la formule analytique p-adique du nombre de classes a permis à Leopoldt et Fresnel ([7], [2]) d'écrire la congruence :

$$\frac{2^{n-1} h}{\sqrt{d}} \left(\frac{R_p}{p^{n-1}}\right) \equiv B \mod p \text{ , pour } p \text{ ne divisant pas } 2d \text{ ,}$$

où B est calculable à partir des nombres de Bernoulli généralisés, où $n = [K:\mathbb{Q}]$, d est le discriminant de K , R_p le régulateur p-adique ($\frac{R_p}{p^{n-1}}$ est p-entier).

Cependant, cette congruence ne donne pas un critère de divisibilité de h par p car $\frac{R_p}{p^{n-1}}$ peut être nul modulo p et on ne sait rien sur R_p.

Pour $p = 2$, nous avons établi un critère de parité du nombre de classes au sens ordinaire des extensions abéliennes $K/\mathbb{Q}$ de degré impair utilisant la signature des unités cyclotomiques de K (unités qui sont parfaitement connues et dont la signature est immédiate) ([3] et [4]).

Dans tout l'exposé nous supposons que $K/\mathbb{Q}$ est une extension abélienne de degré n impair et à groupe de Galois G. L'hypothèse n impair entraîne que le conducteur f est impair. Soit E le groupe des unités de norme 1 de K et soit $F \subset E$ le sous-groupe des unités cyclotomiques de K (au sens de Leopoldt [6]) ; on rappelle que F est déterminé à partir d'unités de $\mathbb{Q}_o^{(f)}$ de la forme suivante :

$$\varepsilon_a = \frac{\zeta^a - \zeta^{-a}}{\zeta - \zeta^{-1}},$$

où ζ est une racine $f^{\text{ème}}$ de l'unité (pas nécessairement primitive) et a un entier premier à f (cf. [6] et [4] pour la définition précise de F).

On montre alors facilement que l'interprétation arithmétique de h par Leopoldt conduit ici à la congruence (notée $(*)$) :

$$(*) \qquad h \equiv (E : F) \text{ modulo } (2).$$

Soient $E_+ = \{\varepsilon \in E,\ \varepsilon \gg 0\}$, $F_+ = F \cap E_+$, $\overline{F} = F/F^2$ et $\overline{F}_+ = F_+/F^2$ ($\varepsilon \gg 0$ signifie que ε et ses conjugués sont positifs).

II. - RÉSULTATS DÉJA CONNUS.

Résultat 1. - Désignons par h_{res} le nombre de classes au sens restreint de K. Alors h_{res} est pair si et seulement si $\overline{F}_+ \neq (1)$.

En effet, soient $\mathcal{H}_{res}$ et $\mathcal{H}$ les 2-groupes des classes au sens restreint et ordinaire et soit S l'homomorphisme signature :

$$S : K^* \longrightarrow \mathbb{F}_2^n$$

$$\alpha \qquad S(\alpha) = (s(\alpha^\sigma))_{\sigma \in G}$$

où $s(\alpha^\sigma) = 0$ (resp. 1) si $\alpha^\sigma > 0$ (resp. $\alpha^\sigma < 0$). On a la suite exacte :

$$1 \to S(K^*)/S(\pm E) \to \mathcal{H}_{res} \longrightarrow \mathcal{H} \to 1$$

$$Cl_{res}(\mathfrak{A}) \to Cl(\mathfrak{A})$$

et on sait que $\pm E/E^2$ est de dimension n sur $\mathbb{F}_2$. Si $\overline{F}_+ \neq (1)$ et si on suppose $\mathcal{H}_{res} = (1)$ alors $S(\pm E) = S(K^*)$ et $\mathcal{H} = (1)$; or, d'après $(*)$, $(E : F)$ est impair d'où $E_+ = F_+ \neq E^2$ soit $\dim(S(\pm E)) < n$ ce qui contredit $S(\pm E) = S(K^*)$.

Si $\overline{F}_+ = (1)$, c'est que $S(\pm E) = S(K^*)$, que $(E : F)$ est impair et aussi que $h_{res} = h$, d'où h_{res} impair.

Résultat 2 ([5]). - Si h est pair alors $\overline{F}_+ \neq (1)$.
(C'est le premier résultat indiqué par Hasse qui est trivial à partir de $(*)$).

La réciproque est fausse en général ; cependant on a le cas particulier suivant :

Résultat 3 ([1]). - Si G est un ℓ-groupe (ℓ premier, $\ell \neq 2$) tel que l'ordre de 2 modulo ℓ soit pair alors h est pair si et seulement si $\overline{F}_+ \neq (1)$.

On a ici un critère de parité mais G est très particulier.

Ce résultat provient du fait que sous ces hypothèses on a égalité des rangs (ρ_{res} et ρ) de $\mathcal{K}_{res}$ et $\mathcal{K}$ ([1]) et l'égalité $\rho_{res} = \rho$ provient d'une obstruction purement galoisienne (dans $\mathbb{F}_2[G]$) qui n'est pas générale.

Supposons alors $\overline{F}_+ \neq (1)$ et h impair ; on aura d'après (*) : $E_+/E^2 \neq (1)$ soit $S(K^*)/S(\pm E) \neq (1)$, d'où $\mathcal{K}_{res} \neq (1)$; l'égalité $\rho_{res} = \rho$ entraînant alors $\mathcal{K} \neq (1)$.

On se rend compte que $\rho_{res} = \rho$ est faux en général : par exemple si K est le sous-corps de degré 7 de $\mathbb{Q}^{(29)}$ alors on a $\rho_{res} = 3$, $\dim \overline{F}_+ = 3$ mais $\rho = 0$. On remarque ainsi que la parité de h n'est pas caractérisée par la non trivialité de $\overline{F}_+$.

L'objet du paragraphe suivant est de montrer en quoi la théorie de Kummer comparée à la théorie du corps de classes peut conduire au résultat que nous avons en vue.

III. - CRITÈRE GÉNÉRAL DE PARITÉ DE h. - Soit $\varepsilon \in E$; on dira que ε est 2-primaire si l'extension $K(\sqrt{\varepsilon})$ est non ramifiée pour les idéaux premiers. Vues les hypothèses faites sur n on sait qu'il est équivalent de dire que pour tout idéal premier $\mathfrak{P}$ de K au-dessus de 2 il existe $\xi_{\mathfrak{P}} \in K$ tel que $\varepsilon \equiv \xi_{\mathfrak{P}}^2 \bmod \mathfrak{P}^2$.

Soit alors $F_o = \{\eta \in F$, η est 2-primaire$\}$ et soit $\overline{F}_o = F_o / F^2$.

Résultat 4. - On a h pair si et seulement si $\overline{F}_+ \cap \overline{F}_o \neq (1)$.

D'après $(*)$, h pair entraîne $\overline{F}_+ \cap \overline{F}_o \neq (1)$. Soit alors $\eta \in (F_+ \cap F_o) \setminus F^2$; distinguons deux cas :

a) Si $\eta \in K^{*2}$ alors $\eta \in E^2 \setminus F^2$ et $(E : F)$ est pair.

b) Si $\eta \notin K^{*2}$ alors l'extension $K(\sqrt{\eta}) / K$ est une extension quadratique non ramifiée en toute place de K (finie ou infinie) ; la théorie du corps de classes prouve que h est encore pair.

Ce critère conduit à un procédé de calcul qui est le suivant :

Considérons l'algèbre semi-simple $\mathcal{A} = \mathbb{F}_2[G] / (\sum_{\sigma \in G} \sigma)$; on sait que $\overline{F}$ est isomorphe à $\mathcal{A}$ et que par conséquent $\overline{F}_+$ et $\overline{F}_o$ seront des sommes directes de sous-modules simples distincts de la forme $\overline{F}^e$ (e idempotents de $\mathcal{A}$). On détermine alors une unité $\eta \in F$ dont l'image dans $\overline{F}$ engendre $\overline{F}$ sur $\mathbb{F}_2[G]$ (l'unité η est explicitement connue [6]) ; la détermination de $\overline{F}_+$ et $\overline{F}_o$ se conduit de la façon suivante :

a) Détermination de $\overline{F}_+$. L'image de S est un G-module si l'on pose, pour $\alpha \in K^*$: $\tau(S(\alpha)) = S(\alpha^\tau)$ pour tout $\tau \in G$. Si on se limite aux éléments de K^* de norme 1 , on vérifie que l'image de S est un G-module isomorphe à $\mathcal{A}$ et que $\overline{F}_+ = \bigoplus_{e\, S(\eta)=0} \overline{F}^e$.

b) Détermination de $\overline{F}_o$. On utilise le quotient de Fermat $\varphi(\alpha) = \frac{\alpha^{2^\gamma - 1} - 1}{2}$ considéré modulo (2) et pour α premier à 2 , où γ est le degré résiduel de 2

dans K ($\varphi(\alpha)$ est donc un élément de $A/(2)$ où A est le localisé en (2) de l'anneau des entiers de K). Si on se limite aux nombres de norme 1 les propriétés "logarithmiques" de φ ([7]) font que l'image de φ est encore un G-module isomorphe à $\mathfrak{A}$. Il suffit alors de constater que le noyau de φ coïncide avec l'ensemble des nombres 2-primaires pour pouvoir écrire :

$$\overline{F}_o = \bigoplus_{e\,\varphi(\eta)=0} \overline{F}^e \quad .$$

Nous avons entrepris une étude numérique dans le cas le plus simple où le résultat 3 n'est pas valable, à savoir le cas où G est cyclique d'ordre 7. L'algèbre $\mathfrak{A}$ possède deux idempotents e et e' et tous les exemples numériques obtenus étaient l'un des quatre suivants, pour le couple $(\overline{F}_+ , \overline{F}_o)$:

$$((1), (1)) \; ; \; (\overline{F}^e, \overline{F}^{e'}) \; ; \; (\overline{F}^{e'}, \overline{F}^e) \; ; \; (\overline{F} , \overline{F}) \quad .$$

Cela nous a suggeré que $\overline{F}_+$ et $\overline{F}_o$ n'étaient pas indépendants, d'autant plus que pour G cyclique d'ordre 3 on sait qu'il y a égalité $\overline{F}_o = \overline{F}_+$ ([1]).

L'objet du paragraphe suivant est de décrire sommairement ce lien, lequel provient d'une étude plus complète du quotient de Fermat des unités cyclotomiques (voir [3] et [4] pour les démonstrations).

IV. - RÉSULTAT FONDAMENTAL. - Compte tenu de la définition de F , il est clair qu'il suffit d'étudier le quotient de Fermat des unités de la forme ε_a

Nous avons obtenu ([3]) pour $\varphi(\varepsilon_a)$ l'expression suivante :

$$\varphi(\varepsilon_a) = \sum_{x \in X} \zeta^x \quad , \quad X = \{x,\ 0 < x \prec f \ ,\ R(x) + R(\tfrac{x}{l}) \text{ impair}\}$$

où R désigne la fonction résidu positif modulo f. Le lien de $\varphi(\varepsilon_a)$ avec la signature de ε_a peut alors être mis en évidence par la remarque suivante : Prenons comme racine primitive $f^{\text{ème}}$ de l'unité $\zeta = \exp(i\frac{\pi}{f} + i\pi)$; soit x premier à f et soit σ_x le $\mathbb{Q}$-automorphisme défini par $\zeta^{\sigma_x} = \zeta^x$, alors

$$\varepsilon_a^{\sigma_x \sigma_a^{-1}} = \frac{\zeta^{R(x)} - \zeta^{-R(x)}}{\zeta^{R(\frac{x}{a})} - \zeta^{-R(\frac{x}{a})}} = \frac{\sin\left((\frac{\pi}{f}+\pi)\,R(x)\right)}{\sin\left((\frac{\pi}{f}+\pi)\,R(\frac{x}{a})\right)}$$

qui est du signe de $(-1)^{R(x)+R(\frac{x}{a})}$ (donc -1 si et seulement si $x \in X$).

On obtient alors le résultat suivant en exploitant convenablement l'expression de $\varphi(\varepsilon_a)$:

THÉORÈME. - Soit ψ l'automorphisme de $\mathcal{A}$ induit par l'application $\sigma \to \sigma^{-1}$ sur G. Si on identifie $\overline{F}$ à $\mathcal{A}$ alors on a la relation :

$$\overline{F}_o = \psi(\overline{F}_+) \ .$$

V. - CONSÉQUENCES DU THÉORÈME PRÉCÉDENT

a) On a finalement un critère de parité ne faisant intervenir que $\overline{F}_+$: h pair équivaut à $\overline{F}_+ \cap \psi(\overline{F}_+) \neq (1)$. On retrouve aussi le résultat 3 cité au début car les hypothèses du théorème d'Armitage et Fröhlich sont faites précisément pour que ψ opère trivialement sur l'ensemble des sous-modules simples $\overline{F}^e$ de $\mathcal{A}$ (i.e. $\overline{F}_+ \cap \psi(\overline{F}_+) = \overline{F}_+$ dans ce cas).

b) La signature des unités fondamentales donne un renseignement partiel

sur la parité de h ; on obtient :

$$\overline{E}_+ \cap \psi(\overline{E}_+) \neq (1) \quad \text{entraîne h pair.}$$

c) De nombreux exemples numériques sont possibles car tous les calculs se ramènent à l'étude de l'expression $R(x) + R(\frac{x}{a})$. Notamment, le cas cyclique de degré 7 confirme les résultats numériques obtenus initialement : les idempotents e et e' vérifient $e' = \psi(e)$ et le seul cas où $F_+ \cap \psi(F_+)$ soit non trivial est le cas où $F_+ = F$ (ici on a h pair si et seulement si $\eta \gg 0$). Le plus petit exemple où la condition " h pair si et seulement si $\eta \gg 0$ " est fausse est relatif aux extensions cycliques de degré 17 (cf. [3] pour un exemple numérique).

VI. - CONCLUSION. - Le théorème obtenu est de nature analytique mais la façon très naturelle qu'il a de généraliser le critère de parité particulier relatif au résultat d'Armitage et Fröhlich suggère qu'il existe un lien général entre classes au sens large et classes au sens restreint plus subtil que " $\rho = \rho_{res}$ " et qui conduirait au critère de parité énoncé.

-:-:-:-

BIBLIOGRAPHIE

[1] ARMITAGE J.V. and FRÖHLICH A. - Class numbers and unit signatures. Mathematika, 14 (1967), 94-98.

[2] FRESNEL J. - Applications arithmétiques de la formule p-adique des résidus. Sém. Delange-Pisot-Poitou, 8e année, 1966-1967, n° 18.

[3] GRAS G. et GRAS M. -N. - Signature des unités cyclotomiques et parité du nombre de classes des extensions cycliques de $\mathbb{Q}$ de degré premier impair. A paraître aux Annales de l'Institut Fourier.

[4] GRAS G. - Signature des unités cyclotomiques et parité du nombre de classes des extensions abéliennes de $\mathbb{Q}$ de degré impair. A paraître au Bulletin de la S. M. F.

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

[6] LEOPOLDT H. W. - Über einheitengruppe und klassenzahl reeller abelscher Zahlkörper. Abh. Deutsche Akad. Wiss. Berlin Math., 2 (1954).

[7] LEOPOLDT H. W. - Über Fermatquotienten von Kreiseinheiten und Klassenzahlformeln modulo p. Rend. Cir. Mat. Palermo, Serie 2, t. 9 (1960), 39-50.

-:-:-:-

Georges GRAS
Université de Besançon
U. E. R. de Sciences
Exactes et Naturelles
Département de
Mathématiques
Route de Gray - La Bouloie
25030 BESANÇON Cedex