SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

GEORGES GRAS

Signature des unités cyclotomiques et parité du nombre de classes des extensions cycliques de Q de degré premier impair

Séminaire de théorie des nombres de Grenoble, tome 3 (1973-1974), exp. n° 1, p. 1-10

<http://www.numdam.org/item?id=STNG_1973-1974__3__A1_0>

Séminaire de Théorie des Nombres

4 décembre 1973
Grenoble

SIGNATURE DES UNITES CYCLOTOMIQUES ET PARITE DU NOMBRE DE CLASSES DES EXTENSIONS CYCLIQUES DE $\mathbb{Q}$ DE DEGRE PREMIER IMPAIR.

par Georges GRAS

1. INTRODUCTION.

Cet exposé résume un travail en commun de Marie-Nicole GRAS et moi-même ([3]) .

2. CLASSES AU SENS LARGE ET CLASSES AU SENS RESTREINT.

Si $\mathcal{H}$ (resp. $\mathcal{H}'$) est le 2-groupe des classes au sens restreint (resp. ordinaire) d'un corps de nombres K , on a, pour "comparer" $\mathcal{H}$ et $\mathcal{H}'$, le procédé suivant :

Soit $S : K^* \to \mathbb{F}_2^r$ l'homomorphisme signature défini par $S(\alpha) = (s(\alpha^{\sigma_1}),\ldots,s(\alpha^{\sigma_r}))$, $s(\alpha^{\sigma_i}) = 0$ ou 1 selon que α^{σ_i} est positif ou non ($\sigma_1,\ldots,\sigma_r$ désignant les r plongements réels de K dans $\mathbb{C}$) . Soit E_o le groupe des unités de K . On a alors la suite exacte :

$$1 \to S(K^*)/S(E_o) \to \mathcal{H} \xrightarrow{j} \mathcal{H}' \to 1 ,$$

où l'homomorphisme j est défini (avec des notations évidentes) par :

$$j(cl(\mathfrak{a})) = cl'(\mathfrak{a}) .$$

Le noyau de j est constitué des classes de la forme $cl(\alpha A_K)$, $\alpha \in K^*$; l'application qui à $cl(\alpha A_K)$ associe la classe de $S(\alpha)$ modulo $S(E_o)$ permet d'identifier $S(K^*)/S(E_o)$ à $Ker(j)$.

Lorsque $S(K^*) = S(E_o)$, on a $\mathcal{H} = \mathcal{H}'$; si au contraire $S(E_o)$ est réduit à $S(-1)$ (on peut trouver un système d'unités fondamentales totalement positives), le noyau est maximum mais on ne sait pas a priori comment se répartit la "différence" lorsqu'on passe du sens large au sens restreint : augmentation du rang ou augmentation de l'ordre des classes ? Si ρ et ρ' sont les rangs respectifs de $\mathcal{H}$ et $\mathcal{H}'$, l'évaluation de $\rho-\rho'$ permet de caractériser ce phénomène.

Pour comparer ρ et ρ' on introduit l'ensemble suivant :

$$M = \{\alpha \in K^* \ , \ K(\sqrt{\alpha})/K \text{ non ramifiée pour les idéaux premiers}\} \ ;$$

on a alors $K(\sqrt{\alpha})/K$ non ramifiée partout (i.e. y compris pour les places à l'infini) si et seulement si α et totalement positif $(S(\alpha) = (0))$ donc si on désigne par $M^+ = M \cap Ker\ S$:

$$M^+ = \{\alpha \in K^* \ , \ K(\sqrt{\alpha})/K \text{ non ramifiée partout}\} \ .$$

On a alors, grâce au corps de classes et à la théorie de Kummer :

$$\dim_{\mathbb{F}_2}(M/K^{*2}) = \rho \quad \text{et} \quad \dim_{\mathbb{F}_2}(M^+/K^{*2}) = \rho' \ .$$

PROPOSITION. <u>On a</u> $\rho - \rho' = \dim_{\mathbb{F}_2}(S(M))$.

En effet, on a la suite exacte d'espaces vectoriels sur $\mathbb{F}_2$:

$$1 \to M^+/K^{*2} \to M/K^{*2} \xrightarrow{S} S(K^*) \ .$$

On a alors les résultats suivants :

THEOREME 1 (Armitage - Fröhlich). <u>On a</u> $0 \leq \rho-\rho' \leq [r/2]$.

Se reporter à [2] et [4] pour la démonstration.

THEOREME 2 (généralisation d'une démonstration de Serre). Si $K/\mathbb{Q}$ est galoisienne et si $\mathrm{Gal}(K/\mathbb{Q})$ est un ℓ-groupe où ℓ est un nombre premier impair tel que l'ordre f de 2 modulo ℓ soit pair alors on a $\rho = \rho'$.

On reprend le principe de la démontration de Serre (des cas particuliers sont démontrés dans [2] et [4]) : on introduit le produit suivant défini sur $K^* \times K^*$:

$$B(a,b) = \prod_{i=1}^{r} (a,b)_{\infty_i} ,$$

produit des symboles de Hilbert relatifs aux r places à l'infini. On vérifie que $B(a,b)$ ne dépend que de $S(a)$ et $S(b)$. La formule du produit :

$$B(a,b) . \prod_{\mathfrak{p}\,\text{premier}} (a,b)_{\mathfrak{p}} = 1$$

permet, en calculant les $(a,b)_{\mathfrak{p}}$, de vérifier que $B(a,b) = 1$ dès que $(a,b) \in M \times M$.

En passant à la notation additive et compte-tenu de ce qui précède, on peut considérer B comme une forme bilinéaire définie sur $S(K^*) \times S(K^*)$ à valeurs dans $\mathbb{F}_2$ et non dégénérée. Pour B , $S(M)$ est un sous-espace totalement isotrope.

Jusque là le raisonnement est valable pour un corps de nombres K quelconque. Dans l'hypothèse du théorème 2, alors $S(M)$ est muni canoniquement d'une structure de G-module, avec $G = \mathrm{Gal}(K/\mathbb{Q})$. Or la recherche des sous-modules totalement isotropes est relativement facile :

On vérifie que $S(K^*) \simeq \mathbb{F}_2[G]$; les propriétés de B (en particulier la description des sous-modules totalement isotropes pour B) se ramène exclusivement à des propriétés du groupe G , les propriétés arithmétiques de K n'intervenant pas du tout (cela explique bien l'échec de la méthode quand l'hypothèse f pair n'est pas vérifiée).

On démontre, en considérant les sous-modules simples de $\mathbb{F}_2[G]$, qu'il n'y a pas de sous-modules isotropes pour B autres que (0) lorsque

f est pair, d'où $\rho = \rho'$. Mais la méthode échoue totalement dans le cas où f est impair car, dans ce cas, il y a toujours des sous-espaces totalement isotropes (cf. [4]) et on est pratiquement ramené au résultat du théorème 1.

Un autre intérêt du cas $\rho = \rho'$ est le suivant :

3. CRITERE DE PARITE DE h LORSQUE $\rho = \rho'$.

Soit $K/\mathbb{Q}$ cyclique de degré ℓ . Si h est le nombre de classes au sens ordinaire de K , on sait d'après Hasse ([5]), que h s'interprète comme l'indice du groupe des unités cyclotomiques de K dans le groupe des unités de K ; et de façon précise, on a $h = (E : F)$ où E est le groupe des unités de norme 1 de K et F le groupe des unités cyclotomiques de norme 1 de K (c'est la formule analytique du nombre de classes qui conduit à cette interprétation).

Critère. Si $\rho = \rho'$ alors une condition nécessaire et suffisante pour que h soit pair est que $F_+ \neq F^2$ ($F_+ = F \cap \mathrm{Ker}\, S$).

Démonstration : Si h est pair, il existe $\varepsilon \in E$ telle que $\eta = \varepsilon^2 \in F \setminus F^2$ donc $\eta \in F_+ \setminus F^2$.

Si $F_+ \neq F^2$ et si on suppose h impair alors F_+/F^2 s'identifie à E_+/E^2 ; or l'hypothèse $E_+/E^2 \neq (1)$ conduit immédiatement à $S(K^*)/S(E_o) \neq (1)$, soit $\mathfrak{A}$ non trivial, d'après la suite exacte du § 2 ; mais $\rho = \rho'$ entraîne $\rho' \neq 0$, d'où une contradiction.

Ce critère redonne les cas connus : $\ell = 3$ et le cas où 2 est racine primitive ([1]).

Lorsque f est impair, il n'y a pas de raisons d'avoir $\rho = \rho'$ et d'ailleurs le critère précédent est faux, comme le montre l'exemple suivant :

Exemple. Soit $\ell = 7$ (f=3) ; les sous-modules complètement isotropes sont de dimensions 0,3,6 ([4]) et on peut donc avoir $\rho - \rho' = 0,3$ ou 6 . Pour le sous-corps de degré 7 de $\mathbb{Q}^{(29)}$, on a $F_+ \neq F^2$ ($\dim_{\mathbb{F}_2}(F_+/F^2) = 3$) et pourtant, bien que $\rho = 3$, on a $\rho' = 0$ (h impair).

On peut se demander si à défaut de critère de parité, dans le cas f impair, il n'est pas possible de décider numériquement (et sans calculer h évidemment) de cette parité.

On a en effet le procédé général suivant :

4. CRITERE GENERAL DE PARITE DE h .

Toujours dans le cas $K/\mathbb{Q}$ cyclique de degré premier $\ell \neq 2$, on utilise la théorie de Kummer :

Critère général. Soient $\overline{F}_+ = F_+/F^2$, $\overline{F}_o = F_o/F^2$ où $F_o = \{\eta \in F$, η vérifie les congruences de Kummer$\}$ (autrement dit $F_o = F \cap M$). Alors une condition nécessaire et suffisante pour que h soit pair est que :

$$\overline{F}_+ \cap \overline{F}_o \neq (1) \quad \text{(i.e. } F_+ \cap F_o \neq F^2\text{)}.$$

Démonstration : Si h est pair alors il existe $\varepsilon \in E\backslash F$ telle que $\eta = \varepsilon^2 \in F\backslash F^2$ alors $\eta \in F_+ \cap F_o \backslash F^2$.

Inversement si $\eta \in F_+ \cap F_o \backslash F^2$ alors ou bien $\eta \in E^2$ et $h = (E:F)$ est pair, ou bien $\eta \notin E^2$ (donc $\eta \notin K^{*2}$) et $K(\sqrt{\alpha})/K$ est non ramifiée partout, soit h pair encore.

D'un point de vue numérique, la détermination de F_+ et F_o est assez facile, F étant parfaitement connu. Par exemple, dans le cas $\ell = 7$, $\overline{F}_+$ et $\overline{F}_o$ étant des sous-modules de $\overline{F}$, il y a 4 possibilités pour chacun d'eux : on a $\overline{F} \simeq \mathbb{F}_2[G]/(\nu) = \mathcal{A}$ où $\nu = \sum_{\sigma \in G} \sigma$ et l'algèbre $\mathcal{A}$ possède

2 idempotents, d'où les sous-modules : $\overline{F}, \overline{F}_1, \overline{F}_2, (1)$ (avec $\dim_{\mathbb{F}_2}(\overline{F}_1) = \dim_{\mathbb{F}_2}(\overline{F}_2) = 3$ et $\overline{F} = \overline{F}_1 \oplus \overline{F}_2$). Il y a donc a priori 16 possibilités pour le couple $(\overline{F}_+, \overline{F}_o)$; or dans tous les exemples numériques traités seuls les 4 suivants se sont produits :

$\overline{F}_+$	(1)	$\overline{F}$	$\overline{F}_1$	$\overline{F}_2$
$\overline{F}_o$	(1)	$\overline{F}$	$\overline{F}_2$	$\overline{F}_1$

Ces résultats suggèrent que $\overline{F}_o$ et $\overline{F}_1$ ne sont pas indépendants.

5. ETUDE DE F_+ ET F_o ([3]).

Comme $\overline{F}_+$ est facile à déterminer, considérons $\overline{F}_o$.

Dans $K/\mathbb{Q}$, F est engendré sur G par :

$$\eta' = N_{\mathbb{Q}_o^{(m)}/K} \varepsilon'_a$$

où m est le conducteur de K , ε'_a est de la forme :

$$\varepsilon'_a = \frac{\zeta^a - \zeta^{-a}}{\zeta - \zeta^{-1}}$$

pour a convenable et ζ racine primitive m^e de l'unité.

Comme 2 est non ramifié dans $\mathbb{Q}^{(m)}$, les congruences de Kummer sont, pour une unité ε de $\mathbb{Q}_o^{(m)}$: ε vérifie les congruences de Kummer si et seulement si pour tout $\mathfrak{p}$ divisant (2) il existe $\xi_{\mathfrak{p}} \in \mathbb{Q}_o^{(m)}$ tel que $\varepsilon \equiv \xi_{\mathfrak{p}}^2 \mod \mathfrak{p}^2$.

Soit $n = 2^\gamma - 1$, γ = degré résiduel de 2 dans $\mathbb{Q}_o^{(m)}$, alors il revient au même d'écrire :

$\varepsilon^n \equiv 1 \mod \mathfrak{p}^2$ pour tout $\mathfrak{p}$ divisant (2) soit

$\varepsilon^n \equiv 1 \mod (4)$.

On est donc ramené à l'étude de $\varepsilon_a = \varepsilon'^n_a$ modulo (4) . On a une première réduction :

Soit $\varepsilon'_a = \dfrac{\zeta^a - \zeta^{-a}}{\zeta - \zeta^{-1}}$; $(\zeta - \zeta^{-1})^2 \equiv \zeta^2 + \zeta^{-2} + 2 \mod (4)$ et plus généralement $(\zeta-\zeta^{-1})^{2^\gamma} \equiv \zeta^{2^\gamma} + \zeta^{-2^\gamma} + 2 \mod (4)$ et comme $2^\gamma \equiv 1 \mod m$, on a facilement

$$\varepsilon_a \equiv 1 + 2\,\frac{Y_a + Y_{a-1} + Y_1}{Y_1 Y_a} \mod (4) ,$$

où $Y_i = \zeta^i + \zeta^{-i}$; le terme $\varphi_a = \dfrac{Y_a + Y_{a-1} + Y_1}{Y_1 Y_a}$ résume les propriétés congruentielles de ε_a donc de $\eta = N_{\Phi_o^{(m)}/K}\,\varepsilon_a = \eta'^n$, car on a :

$$\eta \equiv 1 + 2\,\mathrm{Tr}_{\Phi_o^{(m)}/K}(\varphi_a) \mod (4)$$

$$\equiv 1 + 2\varphi \quad \text{où} \quad \varphi = \mathrm{Tr}_{\Phi_o^{(m)}/K}(\varphi_a) ,$$

et on peut considérer φ comme élément de $A_K/(2)$. Si $\omega = \sum_{\sigma \in G} a_\sigma \sigma \in \mathbb{Z}[G]$ alors à η^ω correspond $\omega\varphi$ de la façon suivante :

$$\eta^\omega = \overline{\prod_{\sigma \in G} (\eta^\sigma)^{a_\sigma}} \equiv 1 + 2 \sum_{\sigma \in G} a_\sigma \varphi^\sigma \mod (4) .$$

On peut donc écrire, en désignant par e_i les idempotents de $\mathfrak{a} = \mathbb{F}_2[G]/(\nu)$:

$\overline{F}_o = \oplus_i \overline{F}^{e_i}$ pour les i tels que η^{e_i} vérifie les congruences de Kummer, soit $e_i\varphi \equiv 0 \mod (2)$;

$\overline{F}_+ = \oplus_j \overline{F}^{e_j}$ pour les j tels que η^{e_i} soit totalement positive, soit $e_i S(\eta) = 0$.

Le calcul des $e_i\varphi$ se présente mal car φ est un quotient d'entiers de $\Phi_o^{(m)}$. Il faut donc exprimer φ_a sur la base des ζ^k dans $\Phi^{(m)}$ et alors $\mathrm{Tr}_{\Phi_o^{(m)}/K}\varphi_a = \varphi$ s'écrira sur la base (quasi) normale formée par $\theta = \mathrm{Tr}_{\Phi^{(m)}/K}(\zeta)$ et ses conjugués.

THEOREME 1. Quel que soit a premier à m on a :

$$\varphi_a \equiv \sum_{x\in X} \zeta^x \mod(2) ,$$

où $X = \{x\in\mathbb{Z} , 0<x<m , R_m(\frac{x}{a})+x \equiv 1 \mod(2)\}$ et où R_m désigne la fonction résidu positif modulo m .

Cette formule (démontrée dans [3]) va établir un lien avec la signature en raison de la remarque suivante :

Si on prend $\zeta = e^{i\frac{\pi}{m}+i\pi}$ alors :

$$\frac{\zeta^r-\zeta^{-r}}{\zeta^x-\zeta^{-x}} = \frac{\operatorname{Sin} r(\frac{\pi}{m}+\pi)}{\operatorname{Sin} x(\frac{\pi}{m}+\pi)} = (-1)^{r+x}\,\frac{\sin\frac{\pi}{m}r}{\sin\frac{\pi}{m}x}$$

qui est du signe de $(-1)^{r+x}$; ce signe est négatif si et seulement si $r+x \equiv 1 \mod(2)$ soit $x\in X$. On aboutit alors au résultat suivant (dans K) :

THEOREME 2. On a $\varphi \equiv \sum_{\tau\in G} s(\eta^\tau)\theta^{\sigma_a\tau}$ modulo (2) .

On rappelle que $s(\eta^\tau) = 1$ (resp. 0) si $\eta^\tau < 0$ (resp. >0) , que σ_a est la restriction à K du $\mathbb{Q}$-automorphisme $\zeta \to \zeta^a$ de $\mathbb{Q}^{(m)}$ et enfin que $\theta = \operatorname{Tr}_{\mathbb{Q}^{(m)}/K}(\zeta)$.

On peut dire que les coefficients des conjugués de θ sont les "composantes" de la signature de η .

6. COROLLAIRES.

On déduit du théorème 2 les résultats suivants :

THEOREME 3. Si $\overline{F}_+ = \bigoplus_{i\in I} \overline{F}^{e_i}$ alors $\overline{F}_o = \bigoplus_{i\in I} \overline{F}^{\psi(e_i)}$, où $\psi : \mathcal{A} \to \mathcal{A}$ est l'automorphisme induit par $\sigma \to \sigma^{-1}$ dans G (ψ opère sur l'ensemble des idempotents).

Remarques. L'opération ψ se rencontrait déjà dans la démonstration d'Armitage-Fröhlich-Serre ([2]) ; le calcul de $\overline{F}_o$ se déduit donc de celui de $\overline{F}_+$; donc la détermination de $\overline{F}_+ \cap \overline{F}_o$ ne dépend que de $\overline{F}_+$.

COROLLAIRE 1. On a $\dim_{\mathbb{F}_2}(\overline{F}_o) = \dim_{\mathbb{F}_2}(\overline{F}_+)$.

COROLLAIRE 2. Si f est pair on a $\psi(e) = e$ pour tout idempotent de $\mathcal{A}$, d'où h est pair si et seulement si $\overline{F}_+ \neq (1)$ (on retrouve le critère qui se déduit du fait que $\rho = \rho'$).

COROLLAIRE 3. Si f est impair, une condition nécessaire et suffisante pour que h soit pair est qu'il existe un idempotent e de $\mathcal{A}$ tel que η^e et $\eta^{\psi(e)}$ soient totalement positives.

COROLLAIRE 4. Si $\mathcal{A}$ possède exactement 2 idempotents e et e' et si f est impair alors on a $\psi(e) = e'$ et h est pair si et seulement si η est totalement positive.

En effet, on a les cas suivants :

$\overline{F}_+ = (1)$, alors $\overline{F}_o = (1)$, h impair ;

$\overline{F}_+ = \overline{F}^e$, alors $\overline{F}_o = \overline{F}^{\psi(e)} = \overline{F}^{e'}$ et $\overline{F}_+ \cap \overline{F}_o = (1)$, h impair ;

$\overline{F}_+ = \overline{F}^{e'}$, même résultat ;

$\overline{F}_+ = \overline{F}$, alors $\overline{F}_o = \overline{F}$ et h est pair (c'est le seul cas).

Ce corollaire s'applique notamment pour $\ell = 7$ où les deux idempotents sont :

$$e = 1 + \tau + \tau^2 + \tau^4 \quad ; \quad e' = 1 + \tau^3 + \tau^5 + \tau^6 .$$

Critère portant sur la signature de η . Dans le cas général, il suffit de déterminer quels sont les idempotents e de $\mathcal{A}$ tels que η^e soit totalement positive, ce qui est facile.

7. CONCLUSION.

En conclusion citons les deux exemples suivant obtenus par ordinateur :

a) pour $\ell = 17$ $(f=8)$ et $p = 34\ 919$, le sous-corps de degré 17 de $\mathbb{Q}^{(p)}$ est tel que $\dim_{\mathbb{F}_2}(F_+/F^2) = 8$ et h est pair (alors nécessairement 2^8 divise h).

b) Un des 16 sous-corps (et un seul) de degré 17 sur $\mathbb{Q}$ de $\mathbb{Q}^{(m)}$ avec $m = 137.307$ (et connu par le sous-groupe de $(\mathbb{Z}/m\mathbb{Z})^*$ qui lui correspond) a un nombre de classes pair.

-o-o-

BIBLIOGRAPHIE

[1] ADACHI (N.) - On the class number of an absolutely cyclic number field of prime degree.

Proc. Japan Acad., 45 (1969).

[2] ARMITAGE (J.V.) and FRÖHLICH (A.) - Class numbers and unit signatures.

Mathematika, 14 (1967), 94-98.

[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).

[4] GRAS (M.N.) - Nombre de classes et signature des unités.

Séminaire de théorie des nombres, Grenoble, novembre 1971.

[5] HASSE (H.) - Über die Klassenzahl abelscher Zahlkörpern.

Berlin (1952).

-o-o-