ANNALES DE L'INSTITUT FOURIER

GEORGES GRAS
MARIE-NICOLE GRAS

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

Annales de l'institut Fourier, tome 25, n° 1 (1975), p. 1-22
<http://www.numdam.org/item?id=AIF_1975__25_1_1_0>

Ann. Inst. Fourier, Grenoble
25, 1 (1975), 1-22

SIGNATURE DES UNITÉS CYCLOTOMIQUES ET PARITÉ DU NOMBRE DE CLASSES DES EXTENSIONS CYCLIQUES DE Q DE DEGRÉ PREMIER IMPAIR

par Georges GRAS et Marie-Nicole GRAS

INTRODUCTION

Soit K une extension cyclique de Q de degré premier impair l. Un théorème de Armitage et Fröhlich ([2], résultat IV) permet de déduire la propriété suivante (redémontrée indépendamment ici dans le chapitre III) : "Soit F le groupe des unités cyclotomiques de norme 1 de K. Si l'ordre f de 2 modulo l est *pair*, alors une condition nécessaire et suffisante pour que le nombre de classes au sens ordinaire h de K soit pair est qu'il existe dans $F \setminus F^2$ une unité totalement positive" ; ce résultat a déjà été énoncé dans des cas particuliers : [4] pour $l = 3$ et [1] lorsque 2 est racine primitive modulo l.

Il ne semble pas qu'on ait établi de critères semblables dans le cas où f est *impair* (i.e. dans le cas où le théorème de Armitage et Fröhlich n'est pas valable). Nous nous proposons de montrer que, dans tous les cas, la seule connaissance de la signature des unités cyclotomiques de K permet de décider de la parité de h. Ce résultat proviendra essentiellement d'une propriété élémentaire des unités cyclotomiques des corps cyclotomiques que nous établissons dans le chapitre II.

I. GENERALITES

1. Plongement de K dans un corps cyclotomique.

Si m est le conducteur de K, alors K est contenu dans le sous-corps réel maximal $\mathbf{Q}_0^{(m)}$ du corps cyclotomique $\mathbf{Q}^{(m)}$; m est soit produit de nombres premiers distincts congrus à 1 modulo l, soit de la forme $l^2 m_0$, m_0 produit de nombres premiers distincts congrus à 1 modulo l ([9], chap. III, § 3 et chap. IV, th. 9). Ainsi m est impair.

On notera Γ, Γ_0 et G les groupes de Galois des extensions $\mathbf{Q}^{(m)}/\mathbf{Q}$, $\mathbf{Q}_0^{(m)}/\mathbf{Q}$ et $\mathrm{K}/\mathbf{Q}$. On identifiera Γ à $(\mathbf{Z}/m\mathbf{Z})^*$ en notant σ_x, x premier à m défini modulo m, l'élément de Γ tel que $\xi^{\sigma_x} = \xi^x$, pour toute racine m^e de l'unité ξ. Pour simplifier, nous noterons encore par σ_x les éléments de Γ_0 ; σ_x et σ_{-x} représentent le même Q-automorphisme de $\mathbf{Q}_0^{(m)}$.

2. Formule analytique du nombre de classes.

Dans [5] (chap. II), Hasse a donné une interprétation arithmétique du nombre de classes au sens ordinaire des extensions abéliennes réelles de Q, faisant intervenir le groupe des unités cyclotomiques de ces extensions. Soit ζ une racine primitive m^e de l'unité ; alors, dans notre cas, le groupe des unités cyclotomiques de $\mathbf{Q}_0^{(m)}$ est engendré par les unités $\epsilon_a = \dfrac{\zeta^a - \zeta^{-a}}{\zeta - \zeta^{-1}}$, $a \in \mathbf{Z}$, a premier à m, et le groupe F′ des unités cyclotomiques de K est engendré par les unités $\eta_a = \mathrm{N}_{\mathbf{Q}_0^{(m)}/\mathrm{K}}\, \epsilon_a$. La formule est alors, dans le cas particulier d'une extension K/Q cyclique de degré premier l : $h = \mathcal{R}'/\mathcal{R}$ où $\mathcal{R}$ (resp. $\mathcal{R}'$) est le régulateur du groupe des unités E′ de K (resp. du groupe des unités cyclotomiques F′ de K).

PROPOSITION I1. — *Soit* E *(resp.* F*) le groupe des unités de* K *(resp. des unités cyclotomiques de* K*) de norme absolue* 1. *Alors on a* $h = (\mathrm{E} : \mathrm{F})$.

Démonstration. — On a $\mathcal{R}'/\mathcal{R} = (E'/\{-1, +1\} : F'/T)$ où T est le sous-groupe de torsion de F' ; comme l est impair, on a

$$N_{K/Q} E' = \{-1, +1\} \quad \text{et} \quad E'/\{-1, +1\}$$

est isomorphe à E ; de même F'/T sera isomorphe à F si on montre que $T = N_{K/Q} F'$. Or F' est un G-module : on a en effet la relation $\epsilon_a^{\sigma_b} = \epsilon_{ab}\epsilon_b^{-1}$ dans $Q_0^{(m)}$ qui conduit à $\eta_a^{\sigma_b} = \eta_{ab}\eta_b^{-1}$ dans K ; donc si $-1 \in N_{K/Q} F'$, on a $-1 \in F'$ soit $-1 \in T$ et inversement.

Nous noterons enfin $\bar{E} = E/E^2$, $\bar{F} = F/F^2$ et nous désignerons par q l'homomorphisme canonique $F \to \bar{F}$ ($\bar{E}$ et $\bar{F}$ sont des $\mathbf{F}_2$-espaces vectoriels de dimension $l - 1$).

3. Structure du groupe des unités de K.

On a le résultat général suivant connu : "Soit L une extension galoisienne réelle de Q de groupe de Galois Λ. Soit E_L le groupe des unités de L modulo la torsion, considéré comme $\mathbf{Z}[\Lambda]$-module, et soit F_L un sous-module de E_L de même Z-rang que E_L ; alors si p est un nombre premier ne divisant pas l'ordre de Λ, F_L/F_L^p est isomorphe à l'algèbre $\mathbf{F}_p[\Lambda]/(\nu)$, où ν est la norme $\sum_{\tau \in \Lambda} \tau$".

Nous appliquerons ce résultat à $\bar{E}$ et $\bar{F}$; en ce qui concerne F on a :

PROPOSITION I2. — *Soit a un entier premier à m tel que $\sigma_a \notin \mathrm{Gal}\ (Q^{(m)}/K)$ et soit η celle des deux unités η_a et $-\eta_a$ qui est de norme 1. Alors η engendre* F *sur* $\mathbf{Z}[G]$.

Démonstration. — D'après la proposition I1, on a $F = F'/T$ où T est le sous-groupe de torsion de F' ; il suffit donc de montrer que pour tout b premier à m, on a $\eta_b = \pm \eta_a^{\omega}$, avec $\omega \in \mathbf{Z}[G]$, ce qui est immédiat d'après [5], p. 24-25.

Choisissons une fois pour toutes un entier a vérifiant les conditions de la proposition I2 et notons η le générateur correspondant de F ; alors $q(\eta)$ est une base du $\mathbf{F}_2[G]/(\nu)$-module $\bar{F}$, où $\nu = \sum_{\tau \in G} \tau$.

4. Bases normales d'entiers de K.

On sait ([7], théorème 132) que lorsque l'extension K/Q est modérément ramifiée (i.e. l ne divise pas m), les l conjugués du nombre $\theta = \mathrm{Tr}_{\mathbf{Q}(m)/\mathrm{K}}\,\zeta$ constituent une **Z**-base normale de l'anneau des entiers A de K ; lorsque l est ramifié dans K, on a une **Z**-base quasi-normale ([8]) formée de 1 et de $l-1$ conjugués de θ (dans ce dernier cas, les conjugués de θ sont liés par "l'unique" relation $\mathrm{Tr}_{\mathrm{K}/\mathbf{Q}}\theta = 0$).

5. Propriétés de l'algèbre $\mathfrak{A} = \mathbf{F}_2[\mathrm{G}]/(v)$.

Comme G est cyclique d'ordre l premier impair, l'algèbre $\mathfrak{A}$ est semi-simple et on a le résultat immédiat suivant ([3]) :

PROPOSITION 13. — *L'algèbre $\mathfrak{A}$ possède un système de $g = \dfrac{l-1}{f}$ idempotents orthogonaux irréductibles, f étant l'ordre de 2 modulo l.*

Nous noterons $\bar{e}_1, \ldots, \bar{e}_g$ les idempotents de $\mathfrak{A}$ et $e_1, \ldots, e_g$ des représentants dans $\mathbf{Z}[\mathrm{G}]$ de ces idempotents. Si $g = 1$, l'unique idempotent de $\mathfrak{A}$ est $\bar{e} = 1$.

Si $\mathfrak{M}$ est un $\mathfrak{A}$-module, nous noterons multiplicativement (resp. exponentiellement) l'opération de $\mathfrak{A}$, si la loi de groupe dans $\mathfrak{M}$ est notée additivement (resp. multiplicativement).

Remarque 11. — Tout $\mathfrak{A}$-module de type fini est somme directe de $\mathfrak{A}$-modules simples et l'ensemble des $\mathfrak{A}$-modules simples non isomorphes deux à deux est constitué des g sous-modules simples de $\mathfrak{A}$ qui sont de la forme $e_i\mathfrak{A}$, $i = 1, 2, \ldots, g$ ([3]). En particulier, $\bar{\mathrm{E}}$ et $\bar{\mathrm{F}}$, étant isomorphes à $\mathfrak{A}$, se décomposent de façon unique sous la forme :

$$\bar{\mathrm{E}} = \bigoplus_{i=1}^{g} \bar{\mathrm{E}}^{\bar{e}_i}\ ,\quad \bar{\mathrm{F}} = \bigoplus_{i=1}^{g} \bar{\mathrm{F}}^{\bar{e}_i} = \bigoplus_{i=1}^{g} q(\eta)^{\bar{e}_i\mathfrak{A}}$$

Les idempotents $\bar{e}_i$, $i = 1, 2, \ldots, g$, peuvent se calculer facilement et ils possèdent la propriété suivante qui nous sera utile ([2] p. 97).

PROPOSITION I4. — *Soit ψ l'automorphisme de $\mathfrak{A}$ induit par l'application $\tau \to \tau^{-1}$ de G dans G. Si f est pair, alors ψ opère trivialement sur l'ensemble des idempotents ; si f est impair, alors ψ opere sans point fixe sur cet ensemble.*

6. Théorie du Corps de classes et théorie de Kummer.

Soient L une extension galoisienne réelle de Q, de groupe de Galois Λ et A_L l'anneau des entiers de L (les résultats de ce paragraphe seront appliqués ultérieurement à $L = Q_0^{(m)}$ ou $L = K$).

a) *L'homomorphisme signature.* On notera $S_L : L^* \to F_2^{[L:Q]}$, l'homomorphisme signature défini par $S_L(\alpha) = (s(\alpha^\tau))_{\tau \in \Lambda}$, s désignant la fonction "signe", c'est-à-dire que $s(\alpha^\tau) = 0$ (resp. 1) si α^τ est positif (resp. négatif). Les éléments de $\operatorname{Ker} S_L$ seront dits totalement positifs. Pour tout sous-groupe Ω de L^* on notera $\Omega_+ = \Omega \cap \ker S_L$.

On peut munir $S_L(L^*)$ d'une structure de Λ-module en posant $\tau(S_L(\alpha)) = S_L(\alpha^\tau)$ pour tout $\tau \in \Lambda$. Ainsi S_L est un homomorphisme de Λ-modules.

b) *Théorie du corps de classes.* On rappelle qu'une condition nécessaire et suffisante pour que le nombre de classes au sens ordinaire de L soit pair est qu'il existe $\alpha \in L^*$, $\alpha \notin L^{*2}$ tel que l'extension $L(\sqrt{\alpha})/L$ soit non ramifiée en toute place finie ou non de L (c'est-à-dire que α soit totalement positif et $L(\sqrt{\alpha})/L$ non ramifiée pour les idéaux premiers).

c) *Théorie de Kummer.* On sait que si l'extension $L(\sqrt{\alpha})/L$ est non ramifiée pour les idéaux, c'est que αA_L est le carré d'un idéal et que α vérifie certaines congruences que nous appellerons congruences de Kummer ([6]). Donnons les dans le cas particulier où 2 n'est pas ramifié dans L/Q ; en supposant α premier à (2) (cas auquel on peut toujours se ramener si αA_L est le carré d'un idéal), on a :

PROPOSITION I5. — *On suppose 2 non ramifié dans L/Q ; α premier à (2) vérifie les congruences de Kummer si et seulement si pour tout idéal $\mathfrak{p}$ au-dessus de (2) dans L, il existe $\xi_\mathfrak{p} \in L$ tel que $\alpha \equiv \xi_\mathfrak{p}^2$ modulo $\mathfrak{p}^2$.*

d) *Définition de l'homomorphisme* $\overline{\varphi}_L$. On suppose toujours 2 non ramifié dans L/Q. Soit C un sous-Λ-module du groupe des unités de L. Soit $\alpha \in C$; il existe un entier n impair (par exemple $2^\gamma - 1$, où γ est le degré résiduel de 2 dans L/Q) tel que α^n soit congru à 1 modulo (2). On écrit alors $\alpha^n = 1 + 2\beta$, $\beta \in A_L$; on vérifie que l'image de β dans $A_L/(2)$ ne dépend pas du choix de n et que, aux carrés d'éléments de C, correspond O dans $A_L/(2)$. On note alors $\overline{\varphi}_L(\alpha)$ l'image de β dans le Λ-module $A_L/(2)$.

PROPOSITION I6. — *L'application* $\varphi_L : C \to A_L/(2)$ *est un homomorphisme de* Λ*-modules dont le noyau est le sous-module* C_0 *de* C *formé des unités qui vérifient les congruences de Kummer.*

C'est une simple traduction des définitions et de la proposition I5.

DEFINITIONS I1. — *Si* L = K *et si* C *est égal à* F, *nous noterons* $\overline{\varphi}$ *l'homomorphisme de* G*-modules* $F \to A/(2)$ *défini ci-dessus. Soit* $F_0 = \operatorname{Ker} \overline{\varphi}$; *alors* F_0 *est constitué des unités de* F *qui vérifient les congruences de Kummer ; on a donc* $F^2 \subset F_0$ et F_0/F^2 *s'identifie à l'image* $q(F_0)$ *de* F_0 *dans* $\overline{F}$, *que nous noterons* $\overline{F}_0$. *Soit maintenant* $F_+ = F \cap \operatorname{Ker} S$, *où* $S = S_K$ *est la signature dans* K ; *on a aussi* $F^2 \subset F_+$ *et* F_+/F^2 *s'identifie à* $q(F_+)$ que nous noterons $\overline{F}_+$ (*on vérifie que* $(F_0 \cap F_+)/F^2$ *est égal à* $\overline{F}_0 \cap \overline{F}_+$ *et que* $\overline{F}_+$ et $\overline{F}_0$ *sont des sous-*$\mathfrak{A}$*-modules de* $\overline{F}$). *Les images* $\overline{\varphi}(F)$ *et* S(F) *sont des* $\mathbf{F}_2[G]$*-modules annulés par* ν, *par conséquent ce sont des* $\mathfrak{A}$*-modules engendrés respectivement par* $\overline{\varphi}(\eta)$ *et* $S(\eta)$.

On a alors le résultat suivant :

PROPOSITION I7. — *On a* $\overline{F}_0 = \underset{i \in I}{\oplus} \overline{F}^{\overline{e}_i}$, *où* I *est l'ensemble des indices* $i \in \{1, 2, \ldots, g\}$ *pour lesquels* $\overline{e}_i \overline{\varphi}(\eta) = O$ *et on a* $\overline{F}_+ = \underset{j \in J}{\oplus} \overline{F}^{\overline{e}_j}$, *où* J *est l'ensemble des indices* $j \in \{1, 2, \ldots, g\}$ *pour lesquels* $\overline{e}_j S(\eta) = 0$.

Démonstration. — On sait (remarque I2) que tout sous-$\mathfrak{A}$-module de $\overline{F}$ est de la forme indiquée. On a $\overline{F}^{\overline{e}_i} = q(\eta)^{\overline{e}_i \mathfrak{A}}$ et $\overline{F}^{\overline{e}_i}$ est engendré par $q(\eta^{e_i})$, e_i étant un représentant de $\overline{e}_i$ dans $\mathbf{Z}[G]$. Il en résulte que $\overline{F}^{\overline{e}_i}$ est contenu dans $\overline{F}_0$ si et seulement si $\overline{\varphi}(\eta^{e_i}) = O$ (prop. I6), donc si et seulement si $\overline{e}_i \overline{\varphi}(\eta) = O$ dans $\overline{\varphi}(F)$. La seconde assertion est aussi immédiate.

On a alors le critère suivant de parité de h :

PROPOSITION I8. — *Une condition nécessaire et suffisante pour que le nombre de classes h au sens ordinaire de* K *soit pair est que* $\overline{F}_+ \cap \overline{F}_0$ *ne soit pas réduit à* (1).

Démonstration. — Si h est pair, alors l'indice (E : F) est pair (prop. I1) et il existe $v \in E$, $v \notin F$, tel que $v^2 \in F$; or $v^2 \notin F^2$: en effet, $v^2 = w^2$, $w \in F$, conduit à $v = \pm w$, soit $v = w$ puisque v et w sont de norme 1, ce qui est absurde. On a donc $q(v^2) \in \overline{F}_+ \cap \overline{F}_0$, avec $q(v^2) \neq 1$.

Inversement, soit $u \in F_0 \cap F_+$, $u \notin F^2$; si u n'est pas un carré dans K^*, alors l'extension $K(\sqrt{u})/K$ est quadratique et non ramifiée en toute place finie ou non et h est alors pair (§ 6, b)) ; si u est un carré dans K^*, alors u est un carré dans E et $h = (E : F)$ est pair.

Remarque I2. — La proposition précédente montre que la connaissance de $S(\eta)$ et de $\overline{\varphi}(\eta)$ permet de décider de la parité de h. Dans les chapitres II et III, nous montrons que l'expression de $\overline{\varphi}(\eta)$ se déduit de celle de $S(\eta)$, les conséquences de cette relation sont étudiées à la fin du chapitre III.

II. DEMONSTRATION D'UNE PROPRIETE DES UNITES CYCLOTOMIQUES

Dans ce chapitre, nous allons établir une propriété des unités cyclotomiques de $Q_0^{(m)}$ pour m impair quelconque. Cette propriété conduira (dans le chapitre III) au calcul de $\overline{\varphi}(\eta)$ que nous avons en vue.

1. Préliminaires.

Nous faisons le choix suivant d'une racine primitive m^e de l'unité : $\zeta = \exp(i\pi/m + i\pi)$, et nous posons $y_i = \zeta^i + \zeta^{-i}$ pour tout $i \in \mathbf{Z}$. Comme précédemment, ϵ_a, a premier à m, désigne l'unité cyclotomique de $Q_0^{(m)}$: $\epsilon_a = \dfrac{\zeta^a - \zeta^{-a}}{\zeta - \zeta^{-1}}$.

Le corps $L = Q_0^{(m)}$ vérifie les hypothèses du chapitre I (§ 6, d) ; on peut donc définir $\overline{\varphi}_L(\epsilon_a)$. Nous noterons φ_a un représentant de $\overline{\varphi}_L(\epsilon_a)$ dans l'anneau des entiers de $Q_0^{(m)}$.

PROPOSITION III. – *On a* $\varphi_a \equiv \dfrac{y_a + y_{a-1} + y_1}{y_1 y_a}$ modulo (2).

Démonstration. – On remarque d'abord que y_i, pour i premier à m, est premier à (2).

Calculons $\epsilon_a^{2^\gamma - 1}$, où γ est le degré résiduel de 2 dans $Q_0^{(m)}$. On remarque que si x et y sont des entiers quelconques de $Q^{(m)}$, on a $(x + y)^{2^\gamma} \equiv x^{2^\gamma} + y^{2^\gamma} + 2x^{2^{\gamma-1}} y^{2^{\gamma-1}}$ modulo (4), d'où ici, compte tenu du fait que $2^\gamma - 1 \equiv 0 \bmod m$:

$$\epsilon_a^{2^\gamma} \equiv \frac{\zeta^a + \zeta^{-a} + 2}{\zeta + \zeta^{-1} + 2} = \frac{\zeta^a - \zeta^{-a} + 2(1 + \zeta^{-a})}{\zeta - \zeta^{-1} + 2(1 + \zeta^{-1})} \bmod (4) ;$$

on en déduit

$$\epsilon_a^{2^\gamma - 1} \equiv \left(1 + 2\frac{1 + \zeta^a}{\zeta^a + \zeta^{-a}}\right)\left(1 + 2\frac{1 + \zeta^{-1}}{\zeta + \zeta^{-1}}\right) \equiv$$

$$\equiv 1 + 2\frac{y_a + y_{a-1} + y_1}{y_a y_1} \bmod (4) ;$$

d'où φ_a modulo (2).

Remarque III. – On a $\epsilon_{-a} = -\epsilon_a$, d'où

$$(\epsilon_{-a})^{2^\gamma - 1} = -\epsilon_a^{2^\gamma - 1} \equiv -(1 + 2\varphi_a) \bmod (4),$$

soit $\epsilon_{-a}^{2^\gamma - 1} \equiv 1 + 2(1 + \varphi_a) \bmod (4)$ et $\varphi_{-a} \equiv 1 + \varphi_a \bmod (2)$.

2. Propriété fondamentale de φ_a.

L'entier a étant défini modulo m, on choisit dans ce paragraphe $a < m$.

On note $A_m = \{0, 1, \ldots, m - 1\}$, $A_m^* = \{1, 2, \ldots, m - 1\}$, $B_a = A_m^* - \{a\}$ et $B_{m-a} = A_m^* - \{m - a\}$.

Soit $R_m : \mathbf{Z} \to A_m$ la fonction résidu modulo m ; soient :

$$X = \left\{ x \in A_m^* \ , \ R_m\left(\frac{x}{a}\right) + x \equiv 1 \bmod (2) \right\},$$

$$\bar{X} = \left\{ x \in A_m^* \ , \ R_m\left(\frac{x}{a}\right) + x \equiv 0 \bmod (2) \right\},$$

Si $\pi : A_m^* \to A_m^*$ est la symétrie définie par $\pi(x) = m - x$, alors les ensembles X et $\bar{X}$ sont globalement invariants par π et sans point fixe ; enfin A_m^* est réunion disjointe de X et $\bar{X}$.

a) *Autre expression de* φ_a. On a le résultat suivant :

THEOREME II1. – *Quel que soit a premier à m, on a la relation :* $\varphi_a \equiv \sum_{x \in X} \zeta^x \bmod (2)$, *où*

$$X = \left\{ x \in \mathbf{Z} \ , \ 0 < x < m \ , \ R_m\left(\frac{x}{a}\right) + x \equiv 1 \bmod (2) \right\}.$$

La démonstration de ce théorème nécessite trois lemmes préliminaires. On suppose d'abord *a impair.*

LEMME II1. – *Soit* $x \in X$ (*resp.* $\bar{X}$). *Alors* :

(i) $x < m - a$ *entraîne* $x + a \in X$ (*resp.* $\bar{X}$) ;

(ii) $x > m - a$ *entraîne* $x + a - m \in \bar{X}$ (*resp.* X).

On remarque d'abord que si $u, v \in \mathbf{Z}$, v premier à m et $u + v \not\equiv 0 \bmod m$, alors on a la relation $R_m\left(\frac{u+v}{v}\right) = R_m\left(\frac{u}{v}\right) + 1$.

Dans le cas (i), on aura $x + a \in A_m^*$ et

$$R_m\left(\frac{x+a}{a}\right) + x + a = R_m\left(\frac{x}{a}\right) + 1 + x + a \equiv R_m\left(\frac{x}{a}\right) + x \bmod (2),$$

d'où $x + a \in X$ (resp. $\bar{X}$) si $x \in X$ (resp. $\bar{X}$).

Dans le cas (ii), on aura

$$x + a - m \in A_m^* \quad \text{et} \quad R_m\left(\frac{x + a - m}{a}\right) + x + a - m = R_m\left(\frac{x}{a}\right) +$$

$$1 + x + a - m \equiv R_m\left(\frac{x}{a}\right) + x + 1 \bmod (2),$$

d'où

$$x + a - m \in \bar{X} \text{ (resp. X)} \quad \text{si} \quad x \in X \text{ (resp. } \bar{X}).$$

D'où le lemme.

Soit maintenant $r \in B_a$; alors l'équation $r = R_m(x + a)$ admet une solution unique x_r dans B_{m-a}. On a d'ailleurs : $x_r = r - a$ (resp. $m + r - a$) si $r > a$ (resp. $r < a$).

On considère alors les ensembles suivants :

$$U_1 = \{a + 1, a + 2, \ldots, m - 1\},$$

$$U_2 = \{1, 2, \ldots, a - 1\}\ , \ X_i = X \cap U_i$$

et $$\bar{X}_i = \bar{X} \cap U_i \quad \text{pour} \quad i = 1, 2.$$

Ces quatre derniers ensembles constituent une famille de parties disjointes dont la réunion est B_a.

LEMME II2. – *Si* $r \in X_1$ *(resp.* $\bar{X}_1$, X_2 , $\bar{X}_2$) *alors* $x_r \in X$ *(resp.* $\bar{X}$, $\bar{X}$, X).

Ce lemme est en fait une conséquence du lemme II1 ; en effet :

(i) Supposons $r \in U_1$; alors $r > a$ et $x_r = r - a$, d'où $x_r < m - a$. Si $r \in X$ (resp. $\bar{X}$) alors $x_r \in X$ (resp. $\bar{X}$) ; en effet : $x_r \in \bar{X}$ (resp. X) entraîne (lemme II1) : $x_r + a = r \in \bar{X}$ (resp. X), ce qui est absurde.

(ii) Supposons $r \in U_2$: alors $r < a$ et $x_r = r - a + m$, d'où $x_r > m - a$. Si $r \in X$ (resp. $\bar{X}$) alors $x_r \in \bar{X}$ (resp. X) ; en effet : $x_r \in X$ (resp. $\bar{X}$) entraîne (lemme II1) : $x_r + a - m = r \in \bar{X}$ (resp. X), ce qui est absurde.

LEMME II3. – *Soit* U *une partie de* A_m^*. *Soient*

$$U^+ = \{x \in U\ ,\ \pi(x) \in U\} \quad \textit{et} \quad U^- = \{x \in U\ ,\ \pi(x) \notin U\}\ ;$$

alors

$$\sum_{x\in U} y_x \equiv \sum_{x\in\pi(U)} y_x \equiv \sum_{x\in U^-} y_x \bmod (2).$$

En effet, on remarque que $y_x = y_{\pi(x)}$ pour tout $x \in A_m^*$; le lemme résulte alors du fait que U est réunion disjointe de U^+ et U^- et que $\sum_{x\in U^+} y_x \equiv O \bmod (2)$.

Soit alors $X_0 = \left\{x \in X,\ x < \frac{m}{2}\right\}$ (X est donc réunion disjointe de X_0 et de $\pi(X_0)$) ; considérons $P = \sum_{x\in X} \zeta^x$; le théorème sera démontré si l'on montre que $y_1 y_a P \equiv y_a + y_{a-1} + y_1 \bmod (2)$. On a

$$P = \sum_{x\in X_0} y_x \quad \text{et} \quad y_a P = \sum_{x\in X_0} (y_{a+x} + y_{a-x}) = \sum_{x\in X} y_{a+x} =$$

$$= \sum_{x\in X} y_{R_m(a+x)}.$$

On peut donc écrire cette somme $\sum_{\substack{r\in B_a \\ x_r\in X}} y_r$ (les cas $R_m(x + a) = O$ et $R_m(x + a) = a$ n'ayant pas lieu car $m - a \in \bar{X}$, $O \notin X$ et $m \notin X$). On a donc $y_a P = \sum_{r\in U} y_r$ où $U = \{r \in B_a, x_r \in X\}$; le lemme II2 montre que $U = X_1 \cup \bar{X}_2$, d'où

$$y_a P = \sum_{r\in X_1\cup\bar{X}_2} y_r = \sum_{r\in X_1} y_r + \sum_{r\in\bar{X}_2} y_r = \sum_{r\in X_1^-} y_r + \sum_{r\in\bar{X}_2^-} y_r$$

(lemme II3). Si $a < \frac{m}{2}$, alors $X_1^- = \{r \in X, r > m - a\}$ car $m - a \notin X$

et $\bar{X}_2^- = \{r \in \bar{X}, r < a\}$ d'où $\pi(X_1^-) = \{r \in X, r < a\}$

et $\pi(X_1^-) \cup \bar{X}_2^- = \{r \in A_m^*, r < a\}$,

d'où $y_a P \equiv y_1 + y_2 + \cdots + y_{a-1} \bmod (2)$.

Si $a > \frac{m}{2}$, alors

$$X_1^- = \{r \in X\ ,\ r > a\} \quad \text{et} \quad X_2^- = \{r \in \overline{X}\ ,\ r \leqslant m - a\}\ ;$$

on aura

$$\pi(X_1^-) \cup \overline{X}_2^- = \{r \in A_m^*\ ,\ r \leqslant m - a\} \quad \text{et} \quad y_a P = \sum_{r \leqslant m-a} y_r,$$

or
$$\sum_{r=a}^{m-a} y_r \equiv 0 \bmod (2)$$

d'où $y_a P \equiv \sum_{r=m-a+1}^{m-1} y_r \equiv y_1 + y_2 + \cdots + y_{a-1} \bmod (2)$.

Finalement $y_1 y_a P \equiv \sum_{r=1}^{a-1} (y_{r+1} + y_{r-1}) \equiv y_1 + y_{a-1} + y_a \bmod (2)$, ce qui démontre le théorème pour a impair.

Si a est pair, on considère $a' = m - a$ qui est impair ; alors dans ce cas on aura $\varphi_{a'} = \sum_{x \in X'} \zeta^x$ où $X' = \left\{x \in A_m^*\ ,\ R_m\left(-\frac{x}{a}\right) + x \equiv 1 \bmod (2)\right\}$; mais on a

$$R_m\left(-\frac{x}{a}\right) + x = m - R_m\left(\frac{x}{a}\right) + x \equiv R_m\left(\frac{x}{a}\right) + x + 1 \bmod (2),$$

d'où $X' = \overline{X}$ et

$$\sum_{x \in X'} \zeta^x = \sum_{x \in \overline{X}} \zeta^x = 1 + \sum_{x \in X} \zeta^x$$

puisque $\sum_{x \in A_m} \zeta^x = 0$ et que $X \cup \overline{X} = A_m^*$. D'après la remarque II1, on a $\varphi_{a'} \equiv 1 + \varphi_a \bmod (2)$, d'où $\varphi_a \equiv \sum_{x \in X} \zeta^x \bmod (2)$, ce qui achève la démonstration du théorème.

b) *Expression de φ_a au moyen de la signature de certaines unités associées à ϵ_a.* On notera d un diviseur de m supposé différent de m ; on note $d' = m/d$.

Soit a premier à m. Pour tout diviseur d de m, $d \neq m$, on pose $\epsilon_{a,d} = \dfrac{\zeta^{da} - \zeta^{-da}}{\zeta^{d} - \zeta^{-d}}$; c'est une unité de $Q_0^{(d')}$.

Notons Γ_d (resp. $\Gamma_{0,d}$) les groupes de Galois des extensions $Q^{(d')}/Q$ (resp. $Q_0^{(d')}/Q$) pour tout diviseur d de m différent de m. On a le résultat suivant :

THEOREME II2. — *Pour tout a premier à m, on a :*

$$\varphi_a \equiv \sum_{\substack{d|m \\ d\neq m}} \sum_{\sigma\in\Gamma_{0,d}} s(\epsilon_{a,d}^{\sigma})\, y_{ad}^{\sigma} \text{ modulo } (2).$$

Démontrons d'abord trois lemmes.

LEMME II.4. — *Soit $x \in A_m^*$; alors il existe deux entiers uniques d_x et u_x, d_x divisant m, $d_x \neq m$, u_x premier à $d'_x = m/d_x$ et tels que $x = d_x u_x$.*

Il suffit de prendre pour d_x le p.g.c.d. de x et m et pour u_x l'entier x/d_x. La vérification des propriétés de d_x et u_x est alors immédiate.

LEMME II5. — *Pour tout diviseur $d \neq m$, on pose*

$$\Gamma'_d = \{x \in A_m^*,\ d_x = d\} ;$$

alors :

(i) *pour d fixé, l'application $x \to \sigma_{u_x}$ définit une bijection de Γ'_d sur Γ_d.*

(ii) *A_m^* est réunion disjointe des Γ'_d.*

On constate que Γ'_d est l'ensemble des du, $du \in A_m^*$, u premier à d' ; donc u parcourt l'ensemble des nombres compris entre O et d' qui sont premiers à d', ce qui établit (i). La deuxième partie du lemme provient de l'existence et de l'unicité de la décomposition $x = d_x u_x$ du lemme II4.

LEMME II.6. — *Soit $x \in A_m^*$; alors $s\left(\dfrac{\zeta^{ax} - \zeta^{-ax}}{\zeta^{x} - \zeta^{-x}}\right) = 1$ si et seulement si $R_m(ax) \in X$.*

On a $s\left(\frac{\zeta^{ax}-\zeta^{-ax}}{\zeta^{x}-\zeta^{-x}}\right) = s\left(\frac{\zeta^{r}-\zeta^{-r}}{\zeta^{x}-\zeta^{-x}}\right)$ où l'on a posé $r = \mathrm{R}_m(ax)$.

On a alors, compte tenu du fait que $\zeta = \exp(i\pi/m + i\pi)$ (chap. II, § 1) :

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

qui est du signe de $(-1)^{r+x}$ et on aura $s\left(\frac{\zeta^{r}-\zeta^{-r}}{\zeta^{x}-\zeta^{-x}}\right) = 1$ si et seulement si $r + x \equiv 1 \bmod (2)$; mais $r + x = \mathrm{R}_m(ax) + x = r + \mathrm{R}_m\left(\frac{r}{a}\right)$, d'où le lemme.

Démonstration du théorème. – Le théorème II1 montre que $\varphi_a \equiv \sum_{x\in X} \zeta^{x} \bmod (2)$, ce qui peut s'écrire $\varphi_a \equiv \sum_{\substack{x\in A_m^* \\ \mathrm{R}_m(ax)\in X}} \zeta^{ax} \bmod (2)$ car, lorsque x parcourt A_m^*, $\mathrm{R}_m(ax)$ parcourt aussi A_m^*. D'après le lemme II6, on aura $\varphi_a \equiv \sum_{x\in A_m^*} s\left(\frac{\zeta^{ax}-\zeta^{-ax}}{\zeta^{x}-\zeta^{-x}}\right)\zeta^{ax} \bmod (2)$ et d'après le lemme II5,

$$\varphi_a \equiv \sum_{\substack{d\mid m \\ d\neq m}} \sum_{x\in\Gamma_d'} s\left(\frac{\zeta^{ax}-\zeta^{-ax}}{\zeta^{x}-\zeta^{-x}}\right)\zeta^{ax} \equiv \sum_{\substack{d\mid m \\ d\neq m}} \sum_{\sigma\in\Gamma_d} s\left(\frac{\zeta^{ad}-\zeta^{-ad}}{\zeta^{d}-\zeta^{-d}}\right)\zeta^{ad\sigma} \equiv$$

$$\equiv \sum_{\substack{d\mid m \\ d\neq m}} \sum_{\sigma\in\Gamma_d'} s(\epsilon_{a,d}^{\sigma})\,\zeta^{ad\sigma} \bmod (2).$$

Il en résulte que

$$\varphi_a \equiv \sum_{\substack{d\mid m \\ d\neq m}} \sum_{\sigma\in\Gamma_{0,d}} s(\epsilon_{a,d}^{\sigma})\,(\zeta^{ad}+\zeta^{-ad})^{\sigma} \quad \text{soit}$$

$$\varphi_a \equiv \sum_{\substack{d\mid m \\ d\neq m}} \sum_{\sigma\in\Gamma_{0,d}} s(\epsilon_{a,d}^{\sigma})\,y_{ad}^{\sigma} \bmod (2).$$

Dans le dernier chapitre, nous allons étudier les conséquences de cette formule en ce qui concerne le calcul de $\overline{\varphi}(\eta)$.

III. APPLICATION DES RESULTATS PRECEDENT A L'ETUDE DE F_+ ET F_0

Soit K une extension cyclique de degré premier l impair de $\mathbf{Q}$, de conducteur m et de groupe de Galois G. On rappelle que le groupe F des unités cyclotomiques de norme 1 de K admet pour générateur, sur $\mathbf{Z}[G]$, $\eta = \pm \eta_a$, a convenable et $N_{K/Q}(\eta) = +1$ (chap. I, prop. I2). Notons $\theta = \mathrm{Tr}_{Q^{(m)}/K} \zeta$ avec $\zeta = \exp(i\pi/m + i\pi)$ (chap. I, § 3), S la signature dans K (chap. I, § 6) et φ un représentant de $\overline{\varphi}(\eta)$ dans A.

1. Propriété fondamentale de φ.

On a le résultat suivant qui est l'analogue pour K du théorème II2 :

THEOREME III1. — *On a la relation* : $\varphi \equiv \sum_{\tau \in G} s(\eta^\tau)\, \theta^{\sigma_a \tau}$ modulo (2).

Démontrons d'abord trois lemmes.

LEMME III1. — *Soit d un diviseur de m distinct de 1 et m et soit*

$$T_d = \sum_{\sigma \in \Gamma_{0,d}} s(\epsilon^\sigma_{a,d})\, \mathrm{Tr}_{Q_0^{(m)}/K}\, y^\sigma_{ad} \ ;$$

on pose $\quad L = Q_0^{(d')} K, \quad n = [Q_0^{(m)} : L],$

$$t = \mathrm{Tr}_{Q_0^{(d')}/Q}\, y_d \quad \textit{et} \quad s = s(N_{Q_0^{(d')}/Q} \epsilon_{a,d}).$$

Alors $T_d \equiv n\, t\, s \bmod (2)$ *et* $n = \dfrac{\Phi(m)}{l\Phi(d')}$ *où* Φ *est l'indicateur d'Euler.*

On a $\mathrm{Tr}_{\mathbf{Q}_0^{(m)}/\mathbf{K}} y_d = \mathrm{Tr}_{\mathbf{Q}_0^{(m)}/\mathbf{L}} (\mathrm{Tr}_{\mathbf{L}/\mathbf{K}} y_d)$; mais K/Q et $\mathbf{Q}_0^{(d')}/\mathbf{Q}$ sont linéairement disjointes, d'où $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}} (y_d) = \mathrm{Tr}_{\mathbf{Q}_0^{(d')}/\mathbf{Q}} (y_d) = t$ et $\mathrm{Tr}_{\mathbf{Q}_0^{(m)}/\mathbf{K}} y_{ad}^{\tau} = nt$. On a alors

$$\mathrm{T}_d \equiv nt \sum_{\sigma \in \Gamma_{0,d}} s(\epsilon_{a,d}^{\sigma}) \equiv nts\,(\mathrm{N}_{\mathbf{Q}_0^{(d')}/\mathbf{Q}} \epsilon_{a,d}) \equiv nts \bmod (2).$$

Le calcul de n est immédiat.

LEMME III2. — *Soit μ un nombre impair composé divisible par un nombre premier p tel que p^2 ne divise pas μ et soit ξ une racine primitive $\mu^{\text{ème}}$ de l'unité ; alors, pour tout a premier à μ, l'unité* $\dfrac{\zeta^a - \zeta^{-a}}{\zeta - \zeta^{-1}}$ *de* $\mathbf{Q}_0^{(\mu)}$ *est de norme absolue* 1.

On vérifie sans difficultés que si $\lambda = \dfrac{\mu}{p}$ alors la norme dans $\mathbf{Q}_0^{(\mu)}/\mathbf{Q}_0^{(\lambda)}$ de $\dfrac{\xi^a - \xi^{-a}}{\xi - \xi^{-1}}$ est de la forme $\left(\dfrac{w^a - w^{-a}}{w - w^{-1}}\right)^{1-\sigma}$, où $w = \xi^p$, $\sigma \in \Gamma_0$; d'où le lemme.

LEMME III3. — *Soit ξ une racine primitive $l^{2\,\text{ème}}$ de l'unité, l impair, et soit a premier à l ; alors* $\mathrm{N}_{\mathbf{Q}_0^{(l^2)}/\mathbf{Q}_0^{(l)}} \dfrac{\xi^a - \xi^{-a}}{\xi - \xi^{-1}} = \dfrac{\xi_0^a - \xi_0^{-a}}{\xi_0 - \xi_0^{-1}}$ *où* $\xi_0 = \xi^l$.

Fin de la démonstration du théorème. — Définissons l'entier γ égal à 1 (resp. O) si $\eta = -\mathrm{N}_{\mathbf{Q}_0^{(m)}/\mathbf{K}} \epsilon_a$ (resp. $\mathrm{N}_{\mathbf{Q}_0^{(m)}/\mathbf{K}} \epsilon_a$) ; alors d'après la proposition I6, la remarque II1 et le théorème II2, on aura

$$\varphi \equiv \gamma + \mathrm{Tr}_{\mathbf{Q}_0^{(m)}/\mathbf{K}} \varphi_a \equiv \gamma + \sum_{\substack{d \mid m \\ d \neq m}} \mathrm{T}_d \bmod (2),$$

où

$$\mathrm{T}_d = \sum_{\sigma \in \Gamma_{0,d}} s(\epsilon_{a,d}^{\sigma})\, \mathrm{Tr}_{\mathbf{Q}_0^{(m)}/\mathbf{K}} (y_{ad}^{\sigma}).$$

On distingue alors trois cas selon que m est premier, égal à l^2 ou divisible par au moins deux nombres premiers distincts :

(i) m est premier ; alors $\varphi \equiv \gamma + T_1 \bmod (2)$;

(ii) m est égal à l^2 ; alors $\varphi \equiv \gamma + T_1 + T_l \bmod (2)$; le lemme III3 montre que $\epsilon_{a,l} = N_{Q_0^{(l^2)}/Q_0^{(l)}} \epsilon_{a,1}$, par conséquent, on aura $\gamma = 1$ si et seulement si $\epsilon_{a,l}$ est de norme absolue -1. On a, en appliquant le lemme III1 à $d = d' = l$: $s = \gamma$, $n = 1$, $t = 1$, d'où $T_l \equiv \gamma \bmod (2)$ et $\varphi \equiv T_1 \bmod (2)$.

(iii) m est divisible par deux nombres premiers distincts ; d'après le lemme III2, on aura $\gamma = 0$:

α) Si d et d' sont premiers entre eux, $d \neq 1$, alors

$$n = \frac{\Phi(d)}{l\,\Phi(d')} = \frac{\Phi(d)}{l}$$

est pair.

β) Si d et d' ne sont pas premiers entre eux, alors nécessairement on a $m = l^2 m_0$ (m_0 est donc premier à l, $m_0 \neq 1$), $d = l\delta$, $d' = l\delta'$ avec $\delta\delta' = m_0$; alors $n = \Phi(\delta)$ sera pair sauf dans le cas $\delta = 1$, soit $d = l$ et $d' = lm_0$. Supposons $d' = lm_0$; alors d'après le lemme III2, l'unité $\epsilon_{a,d} \in Q_0^{(d')}$ est de norme absolue 1, donc $s = 0$ et on a $\varphi \equiv T_1 \bmod (2)$ dans tous les cas.

Calculons maintenant T_1 : on a ici $\Gamma_{0,1} = \Gamma_0$, $\epsilon_{a,1} = \epsilon_a$ et $y_1 = \zeta + \zeta^{-1}$;

$$T_1 = \sum_{\sigma \in \Gamma_0} s(\epsilon_a^\sigma)\, \mathrm{Tr}_{Q_0^{(m)}/K}(y_1^{\sigma_a \sigma}) = \sum_{\sigma \in \Gamma_0} s(\epsilon_a^\sigma)\, \theta^{\sigma_a \sigma}.$$

Soient $\tau_1, \tau_2, \ldots, \tau_l$ des éléments de Γ_0 représentant les classes de Γ_0 modulo $H_0 = \mathrm{Gal}(Q_0^{(m)}/K)$; alors

$$T_1 = \sum_{i=1}^{l} \sum_{\sigma' \in H_0} s(\epsilon_a^{\tau_i \sigma'})\, \theta^{\sigma_a \tau_i \sigma'} = \sum_{i=1}^{l} \sum_{\sigma' \in H_0} s(\epsilon_a^{\tau_i \sigma'})\, \theta^{\sigma_a \tau_i} \quad ;$$

$$\text{or} \sum_{\sigma' \in H_0} s(\epsilon_a^{\tau_i \sigma'}) = s(N_{Q_0^{(m)}/K} \epsilon_a^{\tau_i}) = s(\pm \eta^{\tau_i}) \equiv \gamma + s(\eta^{\tau_i}) \bmod (2) \quad ;$$

d'où

$$T_1 \equiv \sum_{\tau\in G} (\gamma + s(\eta^\tau))\,\theta^{\sigma_a\tau} \equiv \gamma\Big(\sum_{\tau\in G}\theta^\tau\Big)^{\sigma_a} + \sum_{\tau\in G} s(\eta^\tau)\,\theta^{\sigma_a\tau} \bmod (2).$$

On sait que lorsque l ne divise pas m, $\sum_{\tau\in G}\theta^\tau \equiv 1 \bmod (2)$ et que lorsque l divise m, cette même somme est nulle (chap. I, § 4) ; d'où :

– lorsque l ne divise pas m, on a $T_1 \equiv \gamma + \sum_{\tau\in G} s(\eta^\tau)\,\theta^{\sigma_a\tau} \bmod (2)$,

– lorsque l divise m, on a $T_1 \equiv \sum_{\tau\in G} s(\eta^\tau)\,\theta^{\sigma_a\tau} \bmod (2)$.

Le théorème en résulte alors dans tous les cas :

Cas (i) : $\varphi \equiv \gamma + T_1 \equiv \gamma + \gamma + \sum_{\tau\in G} s(\eta^\tau)\,\theta^{\sigma_a\tau} \bmod (2)$,

Cas (ii) : $\varphi \equiv T_1 \equiv \sum_{\tau\in G} s(\eta^\tau)\,\theta^{\sigma_a\tau} \bmod (2)$,

Cas (iii) : $\varphi \equiv T_1 \equiv \sum_{\tau\in G} s(\eta^\tau)\,\theta^{\sigma_a\tau} \bmod (2)$, car, ici, $\gamma = 0$.

2. Application à l'étude de $\overline{F}_+$ et $\overline{F}_0$.

Les définitions de $\overline{F}_0$ et $\overline{F}_+$ ont été données dans le chapitre I, § 6, d), Définition I1.

On a le résultat suivant :

THEOREME III2. – *Si* $\overline{F}_+ = \bigoplus_{i\in I} \overline{F}^{\overline{e}_i}$, *alors* $\overline{F}_0 = \bigoplus_{i\in I} \overline{F}^{\psi(\overline{e}_i)}$, *où* ψ *est l'automorphisme de* $\mathfrak{A}$ *induit par l'application* $\tau \to \tau^{-1}$ *de* G *dans* G.

Montrons d'abord le lemme suivant :

LEMME III4. – *Soit* $\omega \in \mathbf{Z}[G]$ *tel que* $\nu\omega \equiv O \bmod 2\,\mathbf{Z}[G]$; *alors la relation* $\omega \cdot \theta \equiv O \bmod (2)$ *entraîne* $\omega \equiv O \bmod 2\,\mathbf{Z}[G]$.

Si θ définit une **Z**-base normale d'entiers de K le lemme est évident (sans l'hypothèse sur ω). Dans le cas contraire, on sait que $\mathrm{Tr}_{K/Q}\,\theta = O$ et que 1 et $l-1$ conjugués distincts de θ constituent une **Z**-base d'entiers de K (chap. I, § 4). Ecrivons

$$\omega = \sum_{\tau \in G} a_\tau\,\tau = \sum_{\tau \neq 1} (a_\tau - a_1)\,\tau + a_1\nu\ ;$$

alors $\omega\theta = \sum_{\tau \neq 1} (a_\tau - a_1)\,\theta^\tau$ et $\omega\theta \equiv O \bmod (2)$ entraîne $a_\tau \equiv a_1 \bmod (2)$ pour tout $\tau \in G$, soit $\omega \equiv a_1\,\nu \bmod (2)\,\mathbf{Z}[G]$. L'hypothèse $\nu\omega \equiv O \bmod 2\,\mathbf{Z}[G]$ entraîne $a_1\nu^2 = la_1\,\nu \equiv O \bmod 2\,\mathbf{Z}[G]$, d'où $a_1 \equiv O \bmod (2)$ et le lemme en résulte.

Démonstration du théorème. – Soit $\bar{e}$ un idempotent de $\mathfrak{A}$ et soit e un représentant de $\bar{e}$ dans $\mathbf{Z}[G]$. D'après la proposition I7, on a $\bar{F}^{\bar{e}} \subset \bar{F}_0$ si et seulement si $\bar{e}\bar{\varphi}(\eta) = O$, donc si et seulement si $e\varphi \equiv O \bmod (2)$, car $\nu\varphi \equiv O \bmod (2)$.

Or $e\varphi = e\omega\theta^{\sigma_a}$ où $\omega = \sum_{\tau \in G} s(\eta^\tau)\,\tau$ et $e\varphi \equiv O \bmod (2)$ équivaut à $e\omega\theta \equiv O \bmod (2)$.

On a $e\omega\nu \equiv e\nu \sum_{\tau \in G} s(\eta^\tau) \equiv e\nu\, s(N_{K/Q}\,\eta) \equiv O \bmod (2)$ et le lemme III4 entraîne $e\omega \equiv O \bmod 2\,\mathbf{Z}[G]$.

Soit maintenant $c = (c_\tau)_{\tau \in G}$ la signature définie par $c_\tau = O$ pour tout $\tau \neq 1$ et $c_1 = 1$. On rappelle que $S(K^*)$ est un $\mathbf{F}_2[G]$-module, l'opération de G étant définie par $\tau\,(S(\alpha)) = S(\alpha^\tau)$ (chap. I, § 6, a)) et on vérifie facilement que c est une base de $S(K^*)$ sur $\mathbf{F}_2[G]$. On a alors $S(\eta) = \sum_{\tau \in G} s(\eta^\tau)\,\tau^{-1}c \equiv \psi(\omega) \cdot c$ où $\omega = \sum_{\tau \in G} s(\eta^\tau)\,\tau$. On a donc $\bar{F}^{\psi(\bar{e})} \subset \bar{F}_+$ si et seulement si

$$\psi(e)\,S(\eta) = \psi(e)\,\psi(\omega)\,c = \psi(e\omega)\,c = O$$

donc si et seulement si $e\omega \equiv O \bmod 2\,\mathbf{Z}[G]$.

On a donc montré que $\overline{F}^{\overline{e}} \subset \overline{F}_0$ si et seulement si $\overline{F}^{\psi(\overline{e})} \subset \overline{F}_+$, ce qui démontre le théorème.

COROLLAIRE III1. – *On a* $\dim \overline{F}_0 = \dim \overline{F}_+$.

Il suffit de vérifier que si $\overline{e}$ est un idempotent de $\mathfrak{A}$, alors $\overline{e}\,\mathfrak{A}$ et $\psi(\overline{e})\,\mathfrak{A}$ ont la même dimension sur $\mathbf{F}_2$, ce qui est immédiat.

COROLLAIRE III.2. – *Si l'ordre f de 2 modulo l est pair, alors* $\overline{F}_0 = \overline{F}_+$ *et une condition nécessaire et suffisante pour que h soit pair est que* $\overline{F}_+$ *ne soit pas réduit à* (1).

En effet, dans ce cas, les idempotents de $\mathfrak{A}$ sont invariants par ψ (prop. I4). Par exemple, f est pair pour $l = 3, 5, 11, 13, 17, 19, \ldots$

COROLLAIRE III3. – *Si f est impair, alors une condition nécessaire et suffisante pour que h soit pair est qu'il existe dans* $\overline{F}_+$ *un sous-module de la forme* $\overline{F}^{\overline{e}+\psi(\overline{e})}$, $\overline{e}$ *idempotent de* $\mathfrak{A}$.

En effet, $\overline{F}_0$ contiendra aussi $\overline{F}^{\overline{e}+\psi(\overline{e})}$.

COROLLAIRE III.4. – *Si f est impair, et si* $\dim \overline{F}_+ > \dfrac{l-1}{2}$, *alors h est pair.*

En effet, on a aussi $\dim \overline{F}_0 > \dfrac{l-1}{2}$ et $\overline{F}_+ \cap \overline{F}_0$ n'est pas réduit à (1).

COROLLAIRE III5. – *Si f est impair et si* $g = 2$, *alors h est pair si et seulement si l'unité cyclotomique* η *est totalement positive. Par exemple,* $g = 2$ *et f est impair pour* $l = 7, 23, 47, \ldots$

Dans ce cas, il y a deux idempotents $\overline{e}$ et $\overline{e}'$, et $\overline{e}' = \psi(\overline{e})$; donc, si on écarte les cas triviaux $\overline{F}_+ = (1)$ ou $\overline{F}_+ = \overline{F}$, on aura $\overline{F}_+ = \overline{F}^{e}$, par exemple, d'où $\overline{F}_0 = \overline{F}^{\psi(\overline{e})} = \overline{F}^{\overline{e}'}$ et $\overline{F}_+ \cap \overline{F}_0 = (1)$; h est impair.

COROLLAIRE III6. – *Soit* E *le groupe des unités de norme 1 de* K. *Soit* $\overline{E}_+$ *l'image dans* E/E^2 *du sous-groupe des unités totalement positives de* K :

(i) *Si f est pair, alors h est pair dès que* $\overline{E}_+$ *n'est pas réduit à* (1).

(ii) *Si f est impair, alors h est pair dès que* $\dim \overline{E}_+ > \frac{l-1}{2}$.

Dans le premier cas, si h était impair, on aurait $\overline{E}_+ \cong \overline{F}_+$, ce qui contredit le résultat du corollaire III2.

Dans le deuxième cas, h impair est contraire au corollaire III4.

Remarque III1. – Le corollaire III3 fournit un critère de parité très simple : ayant obtenu la signature de η par la méthode suggérée par le lemme II6, on regarde l'action des idempotents de $\mathfrak{A}$ sur cette signature : h est pair si et seulement si il existe un idempotent $\overline{e}$ tel que $\overline{e}$ et $\psi(\overline{e})$ annulent la signature de η.

Remarque III2. – Le nombre $l = 17$ est le plus petit nombre premier pour lequel la propriété : "h est pair si et seulement si η est totalement positive", est fausse. Citons, pour $l = 17$, deux exemples où l'on a h pair et η non totalement positive :

(i) K est l'unique corps de degré 17 de conducteur premier 34919;

(ii) K est le sous-corps de $\mathbf{Q}^{(m)}$ de degré 17, de conducteur $m = 137.307$, fixe par le sous-groupe de $\Gamma = \mathrm{Gal}(\mathbf{Q}^{(m)}/\mathbf{Q})$ engendré par Γ^{17} et par σ_{65}.

BIBLIOGRAPHIE

[1] N. ADACHI, On the class number of an absolutely cyclic number field of prime degree, *Proc. Japan Acad.*, 45 (1969).

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

[3] C. CURTIS et I. REINER, Representation theory of finite groups and associative algebras, *Interscience Pub.*, vol. XI (1962).

[4] M.N. GRAS, Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de Q, *J. für die reine und Angew. Math.* (à paraître).

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

[6] E. HECKE, Vorlesungen über die Theorie der algebraischen Zahlen, Chelsea Pub. Co.,(1948).

[7] D. HILBERT, Théorie des corps de nombres algébriques, trad. de T. Got et A. Levy, Hermann (1913).

[8] E. NOETHER, Normal basis bei Körpern ohne höhere Verzweigung, *J. für die reine und angew. Math.*, 167 (1932), 147-152.

[9] J.J. PAYAN, Contribution à l'étude des corps abéliens absolus de degré premier impair, *Annales de l'Institut Fourier* (1965), 133-199.

Manuscrit reçu le 24 avril 1974
Accepté par C. Chabauty.

Georges GRAS et Marie-Nicole GRAS,
Laboratoire de Mathématiques
Faculté des Sciences
25030 Besançon Cedex.