ACTA ARITHMETICA
XLVI (1986)

Lien algébrique entre les deux facteurs de la formule analytique du nombre de classes dans les corps abéliens

par

BERNARD ORIAT (Besançon)

La formule analytique donnant le nombre de classes d'idéaux d'un corps de nombres abélien est obtenue en étudiant la fonction ζ de Dedekind. Elle se scinde en deux formules: en effet ce nombre de classes se trouve exprimé comme produit de deux entiers (ou facteurs) mesurant l'un, le nombre de classes réelles, l'autre le nombre de classes relatives du corps de nombres considéré [7]. Nous montrons ici, que sous certaines hypothèses, nous pouvons établir un lien algébrique entre ces deux formules. Nous généralisons ainsi un résultat de K. Iwasawa [10], établi pour les corps cyclotomiques $\boldsymbol{Q}^{(p)}$ seulement. Nous utilisons les unités cyclotomiques introduites par H. W. Leopoldt dans [12] et la décomposition du groupe des p-classes d'idéaux en composantes associées aux caractères p-adiques du groupe de Galois.

1. Enoncé des résultats. Soit p un nombre premier impair. Soit χ un caractère de conducteur f_χ et d'ordre g_χ. Nous supposons χ pair et différent du caractère unité. Soit K_χ le corps cyclique associé à χ. Précisons ce que nous voulons dire par là: Soit $\boldsymbol{Q}^{(f_\chi)}$ le corps cyclotomique obtenu en ajoutant à $\boldsymbol{Q}$, corps des rationnels, les racines $(f_\chi)^{\text{ème}}$ de l'unité et soit $(\boldsymbol{Z}/f_\chi\boldsymbol{Z})^*$ le groupe multiplicatif formé par les classes d'entiers modulo f_χ, premiers à f_χ. Si nous notons $(\cdot, \boldsymbol{Q}^{(f_\chi)})$ le symbole d'Artin attaché à $\boldsymbol{Q}^{(f_\chi)}$, ce groupe s'identifie par l'application de réciprocité $a \to (a, \boldsymbol{Q}^{(f_\chi)})$ au groupe de Galois de l'extension $\boldsymbol{Q}^{(f_\chi)}/\boldsymbol{Q}$. Le caractère χ est un homomorphisme de $(\boldsymbol{Z}/f_\chi\boldsymbol{Z})^*$ sur le groupe des racines $(g_\chi)^{\text{ème}}$ de l'unité. Le sous-corps de $\boldsymbol{Q}^{(f_\chi)}$, laissé fixe par les éléments de $\operatorname{Ker}\chi$ est K_χ. C'est un corps réel, différent de $\boldsymbol{Q}$ et l'extension $K_\chi/\boldsymbol{Q}$ est cyclique de degré g_χ.

Désignons par K le corps composé de K_χ et $\boldsymbol{Q}^{(p)}$, c'est-à-dire le corps obtenu en ajoutant à K_χ les racines $p^{\text{ème}}$ de l'unité. Nous notons G le groupe de Galois de $K/\boldsymbol{Q}$.

Le caractère χ peut aussi être considéré comme un caractère de $\operatorname{Gal}(K_\chi/\boldsymbol{Q})$ et d'une façon plus générale comme un caractère du groupe de

Galois de toute extension abélienne L/Q telle que L contienne K_χ; par exemple K/Q. Dans la suite, ces entités ne seront pas distinguées.

Nous faisons l'hypothèse suivante:

HYPOTHÈSE A. *L'ordre g_χ de χ est premier à p.*

Nous désignons par $\varkappa_\chi$ la χ-composante rationnelle du p-groupe des classes de K. Rappelons sa définition: soit $Q(\chi)$ le corps obtenu en ajoutant à Q les valeurs de χ, c'est-à-dire $Q(\chi) = Q^{(g_\chi)}$. Le caractère rationnel associé à χ est $\mathrm{Tr}_{Q(\chi)/Q}(\chi)$ et l'idempotent associé est

$$\varrho_\chi = \mathrm{Tr}_{Q(\chi)/Q}\left(\frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})\sigma\right).$$

C'est un élément de $Z_p[G]$. Si $\varkappa$ est le p-groupe des classes d'idéaux de K, $\varkappa$ est un $Z_p[G]$-module et $\varkappa_\chi$ est défini comme étant $\varkappa^{\varrho_\chi}$.

Nous désignons par E_χ le groupe des χ-unités propres et F_χ le groupe des χ-unités cyclotomiques [12] ou [14]. Notons $(E_\chi/F_\chi)_p$ la p-composante du groupe quotient E_χ/F_χ. Rappelons que l'interprétation faite par H. W. Leopoldt du premier facteur de la formule analytique montre que les ordres des groupes introduits ci-dessus sont égaux:

$$|\varkappa_\chi| = |(E_\chi/F_\chi)_p|.$$

Dans la suite, nous utilisons des groupes de classes d'idéaux et d'unités associés non plus à un caractère rationnel mais à un caractère p-adique. Désignons par ϕ le caractère p-adique issu de χ. Si $Q_p(\chi)$ est le corps obtenu en ajoutant au corps p-adique Q_p les valeurs de χ, le caractère ϕ est donné par l'égalité: $\phi = \mathrm{Tr}_{Q_p(\chi)/Q_p}(\chi)$. Notons e_ϕ l'idempotent associé

$$e_\phi = \frac{1}{|G|}\sum_{\sigma\in G}\phi(\sigma^{-1})\sigma.$$

C'est un élément de $Z_p[G]$. De même que $\varkappa$, $(E_\chi/F_\chi)_p$ est un $Z_p[G]$-module. Nous posons:

$$\varkappa_\phi = \varkappa^{e_\phi} \quad \text{et} \quad (E_\chi/F_\chi)_\phi = (E_\chi/F_\chi)_p^{e_\phi}.$$

Plusieurs auteurs ont proposé la conjecture suivante [11], [4]:

CONJECTURE. *Les groupes ainsi définis ont même ordre:*

$$|\varkappa_\phi| = |(E_\chi/F_\chi)_\phi|.$$

Cette conjecture a été démontrée partiellement par A. Wiles, pour $K = Q^{(p)}$ seulement [17].

Désignons par ω l'homomorphisme de G dans le groupe multiplicatif de Q_p ainsi défini: $\zeta^\sigma = \zeta^{\omega(\sigma)}$ pour tout σ de G. Cet homomorphisme est un caractère p-adique. Considérons désormais que χ est à valeurs dans $Q_p(\chi)^*$, groupe multiplicatif de $Q_p(\chi)$. Nous pouvons alors définir le reflet de χ, noté

$\bar\chi$, par l'égalité $\bar\chi = \omega\chi^{-1}$ [13]. De même que nous avons associé à χ les quantités ϱ_χ et $\varkappa_\chi$, nous pouvons associer à $\bar\chi$, de la même façon, $\varrho_{\bar\chi}$ et $\varkappa_{\bar\chi}$. L'ordre de la $\bar\chi$-composante rationnelle $\varkappa_{\bar\chi}$ de $\varkappa$ s'exprime à l'aide de nombres de Bernoulli. Rappelons leur définition. Si ψ est un caractère de conducteur f_ψ, on pose $B_\psi = f_\psi^{-1}\sum a\psi(a)$; cette somme est étendue aux entiers premiers à f_ψ et compris entre 1 et f_ψ. Le nombre B_ψ appartient au corps $Q(\psi)$. Si ψ est Q-équivalent à $\bar\chi$, c'est-à-dire si ψ est de la forme $\bar\chi^u$, u entier premier à l'ordre de $\bar\chi$, alors B_ψ appartient à $Q(\bar\chi)$ et le produit $\prod_{\psi\sim\bar\chi} B_{\psi^{-1}}$ étendu aux caractères ψ Q_p-équivalents à $\bar\chi$ est un élément de Z. Nous désignons par $(\prod_{\psi\sim\bar\chi} B_{\psi^{-1}})_p$ sa p-composante. Le deuxième facteur de la formule analytique peut s'interpréter comme l'égalité [4]:

$$|\varkappa_{\bar\chi}| = (\prod_{\psi\sim\chi} B_{\psi^{-1}})_p.$$

Comme ω est un caractère p-adique, l'involution $\chi\to\bar\chi$ peut être étendue aux caractères p-adiques. Nous désignons par $\bar\phi$ le caractère p-adique issu de $\bar\chi$. On a donc:

$$\bar\phi = \mathrm{Tr}_{Q_p(\bar\chi)/Q_p}(\bar\chi) = \omega\phi^{-1}.$$

Soit ψ un caractère Q_p-équivalent à $\bar\chi$, c'est-à-dire tel que $\psi = \bar\chi^{p^u}$, pour un certain entier u. Nous notons $\psi|\bar\phi$ cette relation. Le nombre de Bernoulli $B_{\psi^{-1}}$ peut être considéré comme un élément de $Q_p(\bar\chi)$ et le produit $\prod_{\psi|\bar\phi} B_{\psi^{-1}}$, étendu aux caractères ψ Q_p-équivalents à $\bar\chi$, comme un élément de Z_p. Nous notons $(\prod_{\psi|\bar\phi} B_{\psi^{-1}})_p$ la plus grande puissance de p divisant ce produit. Cette quantité a été l'objet de la conjecture suivante [11], [4]:

CONJECTURE. *L'ordre de $\varkappa_{\bar\phi}$ est donné par l'égalité*:

$$|\varkappa_{\bar\phi}| = (\prod_{\psi|\bar\phi} B_{\psi^{-1}})_p.$$

Enonçons une autre hypothèse:

HYPOTHÈSE B. *Lorsque le conducteur f_χ de χ est premier à p, on suppose que le degré résiduel de p dans K/Q est différent de* 1.

Soit χ_0 le caractère de Dirichlet associé à χ, c'est-à-dire l'application définie sur $Z/f_\chi Z$ par $\chi_0(a) = \chi(a)$ si a est premier à f_χ et $\chi_0(a) = 0$ sinon. L'hypothèse B est équivalente à la condition: $\chi_0(p) \neq 1$.

L'objet du présent article est de démontrer la propriété suivante:

THÉORÈME. *On suppose que χ est un caractère pair et différent du caractère unité. On suppose qu'il vérifie les hypothèses* A *et* B *écrites ci-dessus. Soit ϕ le caractère p-adique issu de χ et soit $\bar\phi$ le reflet de ϕ.*

(i) *Si l'on suppose:* $\varkappa_\phi = \{1\}$ *et* $(E_\chi/F_\chi)_\phi = \{1\}$, *alors on démontre, à l'aide de considérations algébriques seulement, l'égalité:*

$$|\varkappa_{\bar\phi}| = \Big(\prod_{\psi|\bar\phi} B_{\psi-1}\Big)_p.$$

(ii) *Réciproquement, si l'on suppose* $|\varkappa_{\bar\phi}| = \big(\prod_{\psi|\bar\phi} B_{\psi-1}\big)_p$, *alors on démontre, à l'aide de considérations algébriques seulement, l'équivalence entre les deux conditions*

$$\varkappa_\phi = \{1\} \quad et \quad (E_\chi/F_\chi)_\phi = \{1\}.$$

2. Généralisation d'une formule explicite de H. Hasse. On désigne toujours par p un nombre premier impair. Soit n un entier naturel et soit $\Omega_n = Q_p^{(p^{n+1})}$ le corps obtenu en ajoutant à Q_p les racines $(p^{n+1})^{\text{ème}}$ de l'unité. Soient M/Q_p une extension finie non ramifiée de Q_p et M_n le corps composé de Q_p et Ω_n. Soient ζ_n une racine primitive $(p^{n+1})^{\text{ème}}$ de l'unité et ζ_n' une racine de l'unité appartenant à M_n et telle que $\zeta_n'^k = \zeta_n$ pour un entier k premier à p. Posons $\pi_n = 1-\zeta_n$ et $\pi_n' = 1-\zeta_n'$. Une uniformisante de M_n (et de Ω_n) est donc π_n. Notons $(\cdot,\cdot)_{M,n}$ le symbole de Hilbert (symbole de norme résiduelle) relatif à M_n et $(\cdot,\cdot)_n$ le symbole de Hilbert relatif à Ω_n. Dans [1], Artin et Hasse ont démontré la propriété suivante:

PROPOSITION 2.1. *Si* α *est une unité principale de* Ω_n, *alors on a l'égalité:*

$$(\pi_n, \alpha)_n = \zeta_n^a,$$

avec

$$a = -\frac{1}{p^{n+1}} \operatorname{Tr}_{\Omega_n/Q_p}\Big(\frac{\zeta_n}{\pi_n}\log\alpha\Big).$$

Nous utilisons dans la suite une formule analogue dans M_n:

PROPOSITION 2.2. *Si* α *est une unité principale de* M_n, *alors on a l'égalité:*

$$(\pi_n', \alpha)_{M,n} = \zeta_n^{a'},$$

avec

$$a' = -\frac{1}{kp^{n+1}} \operatorname{Tr}_{M_n/Q_p}\Big(\frac{\zeta_n'}{\pi_n'}\log\alpha\Big).$$

La démonstration de cette proposition peut être obtenue en reprenant les arguments de Artin et Hasse, exposés dans [1]. On peut également vérifier que les calculs effectués par Iwasawa dans Ω_n [9], peuvent être repris dans le corps M_n. On écrit ainsi une formule explicite donnant $(\beta, \alpha)_{M,n}$ à condition que β soit norme dans M_m/M_n, pour m assez grand. Comme π_n' est norme de π_m', l'application à π_n' de cette formule permet d'obtenir la proposition énoncée ci-dessus. Le détail de ce calcul est écrit dans [15]. Remarquons aussi que Coleman a généralisé dans [2] les formules explicites d'Iwasawa.

3. Résultats fondamentaux utilisés dans la démonstration. Soit M un $Z_p[G]$-module. Le sous-module $M_\phi = M^{e_\phi}$ de M est la ϕ-composante de M. Désignons par G_χ le groupe de Galois de K_χ/Q, c'est-à-dire $G_\chi = G/\operatorname{Ker}\chi$. C'est un groupe cyclique d'ordre g_χ. Comme $\sigma e_\phi = e_\phi$ pour tout σ de $\operatorname{Ker}\chi$, M_ϕ est naturellement un G_χ-module (cette situation s'applique en particulier à $\varkappa$, p-groupe des classes d'idéaux de K, dont $\varkappa_\phi$ est la ϕ-composante). Considérons l'anneau des entiers de $Q_p(\chi)$, noté $Z_p[\chi]$ et l'application V_χ de $Z_p[G_\chi]$ dans $Z_p[\chi]$ qui prolonge Z_p-linéairement χ. Ainsi V_χ est défini par:

$$V_\chi\Big(\sum_{\sigma\in G_\chi} a_\sigma\sigma\Big) = \sum_{\sigma\in G_\chi} a_\sigma\chi(\sigma).$$

Nous ne distinguons pas χ (resp. ϕ) en tant que caractère de G ou en tant que caractère de G_χ. Ainsi e_ϕ désigne encore la projection de e_ϕ sur $Z_p[G_\chi]$. Nous aurons donc, suivant le contexte:

$$e_\phi = \frac{1}{g}\sum_{\sigma\in G}\phi(\sigma^{-1})\sigma \quad \text{ou} \quad e_\phi = \frac{1}{g_\chi}\sum_{\sigma\in G_\chi}\phi(\sigma^{-1})\sigma.$$

L'image de e_ϕ par V_χ est 1. Plus précisément, la restriction de V_χ à l'idéal $e_\phi Z_p[G_\chi]$ engendré par e_ϕ est un isomorphisme d'anneaux de $e_\phi Z_p[G_\chi]$ sur $Z_p[\chi]$. Ainsi la ϕ-composante de M est un $Z_p[\chi]$-module. En vertu de l'hypothèse A, cet anneau possède un seul idéal maximal engendré par p. Si l'on suppose M fini, alors M_ϕ est isomorphe à une somme directe de $Z_p[\chi]$-modules de la forme $Z_p[\chi]/p^m Z_p[\chi]$. Le nombre de modules de ce type, non nuls, qui interviennent dans cette somme directe est le ϕ-rang de M.

Relativement à $\bar\chi$, les notations et notions suivantes peuvent être définies pareillement: $g_{\bar\chi}$, $f_{\bar\chi}$, $K_{\bar\chi}$, $G_{\bar\chi}$, $e_{\bar\phi}$, $V_{\bar\chi}$, $Z_p[\bar\chi]$, $\bar\phi$-composante, $\bar\phi$-rang. Nous notons f le PPCM de p et f_χ. C'est donc le conducteur de K. C'est aussi le PPCM de p et $f_{\bar\chi}$. On pose aussi $f' = f/p$. En vertu de l'hypothèse A, cet entier est premier à p.

Annulation de $\varkappa_{\bar\phi}$. Le théorème d'annulation de Stickelberger [16], [3], peut se traduire, pour $\varkappa_{\bar\phi}$, en termes de $Z_p[\bar\chi]$-module:

PROPOSITION 3.1. *Le nombre de Bernoulli* $B_{\bar\chi-1}$ *appartient à* $Z_p[\bar\chi]$ *et annule* $\varkappa_{\bar\phi}$.

Démonstration. L'appartenance de $B_{\bar\chi-1}$ à $Z_p[\bar\chi]$ résulte de l'hypothèse A et se démontre à l'aide d'un calcul élémentaire. Notons $(\cdot, K_{\bar\chi})$ le symbole d'Artin relatif à $K_{\bar\chi}$. Désignons par $S_{\bar\chi}$ la somme

$$S_\chi = f_\chi^{-1}\sum a(a, K_\chi)^{-1},$$

étendue aux entiers a premiers à $f_{\bar\chi}$, compris entre 1 et $f_{\bar\chi}$. Rappelons que l'idéal de Stickelberger $S_{\bar\chi}Z_p[G_{\bar\chi}]\cap Z_p[G_{\bar\chi}]$ annule le p-groupe des classes de $K_{\bar\chi}$. Il annule donc également $\varkappa_{\bar\phi}$. Pour appliquer ce résultat, considérons la

quantité $e_{\bar\phi} S_{\bar\chi}$. Décomposons l'idempotent $e_{\bar\phi}$ en somme d'idempotents associés aux caractères ψ Q_p-équivalents à $\bar\chi$. Nous avons donc

$$e_{\bar\phi} = \sum_{\psi|\bar\phi} e_\psi \quad \text{avec} \quad e_\psi = \frac{1}{g_{\bar\chi}} \sum_{\sigma\in G_{\bar\chi}} \psi(\sigma^{-1})\sigma$$

et on vérifie l'égalité

$$e_{\bar\phi} S_{\bar\chi} = \sum_{\psi|\bar\phi} B_{\psi^{-1}} e_\psi.$$

Ceci montre que $e_{\bar\phi} S_{\bar\chi}$ est un élément de l'idéal de Stickelberger. D'autre part, l'image de $e_{\bar\phi} S_{\bar\chi}$ par $V_{\bar\chi}$ est $B_{\bar\chi^{-1}}$. Ainsi, $B_{\bar\chi^{-1}}$ annule $\varkappa_{\bar\phi}$.

Remarque. Les nombres de Bernoulli qui interviennent dans le produit $\prod_{\psi|\bar\phi} B_{\psi^{-1}}$ sont les conjugués de $B_{\bar\chi^{-1}}$ dans l'extension $Q_p(\bar\chi)/Q_p$. Soient n la p-valuation de $B_{\bar\chi^{-1}}$ et d le degré de $Q_p(\bar\chi)/Q_p$. L'expression $\left(\prod_{\psi|\bar\phi} B_{\psi^{-1}}\right)_p$ est donc égale à p^{nd}.

Structure de groupes d'idéaux principaux. Nous désignons toujours par ζ une racine primitive $p^{\text{ième}}$ de 1. Soit $\pi = 1-\zeta$. Cet élément engendre dans $Q^{(p)}$ l'idéal premier au-dessus de p. En vertu de l'hypothèse A, cet idéal n'est pas ramifié dans K. Soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ les idéaux de K au-dessus de p. Les décompositions des idéaux de K engendrés par p et π sont donc: $(\pi) = \mathfrak{p}_1 \ldots \mathfrak{p}_g$ et $(p) = (\mathfrak{p}_1 \ldots \mathfrak{p}_g)^{p-1}$. Pour tout entier i, notons K_{π^i} l'ensemble des x de K tels que: quelque soit j de 1 à g, $x \equiv 1 \bmod (\mathfrak{p}_j^i)$. Il est clair que les K_{π^i} sont des G-modules multiplicatifs. Nous désignons par O_K le localisé en p de l'anneau des entiers de K, c'est-à-dire l'ensemble des éléments x de K dont les $\mathfrak{p}_j$-valuations sont positives.

Proposition 3.2. *Le quotient K_π/K_{π^p} est un $F_p[G]$-module et son $\bar\phi$-rang est* 1.

Démonstration. Soit $\pi^i O_K$ l'idéal de O_K engendré par π^i. Pour tout i un isomorphisme de $F_p[G]$-modules:

$$\pi^i O_K/\pi^{i+1} O_K \simeq K_{\pi^i}/K_{\pi^{i+1}}$$

est obtenu en faisant correspondre à la classe de $\lambda\pi^i$ modulo $\pi^{i+1} O_K$, la classe de $1+\lambda\pi^i$ modulo $K_{\pi^{i+1}}$. Comme l'algèbre $F_p[G]$ est semi-simple, on déduit de ces isomorphismes que K_π/K_{π^p} et O_K/pO_K sont deux $F_p[G]$-modules isomorphes. D'autre part, l'extension K/Q est modérément ramifiée. Si O_Q désigne le localisé en p de Z, O_K est isomorphe, en tant que $O_Q[G]$-module, à $O_Q[G]$. On en déduit que O_K/pO_K est isomorphe, en tant que $F_p[G]$-module, à $F_p[G]$. D'où le résultat annoncé.

Proposition 3.3. *Les deux $F_p[G]$-modules K_π/K_{π^2} et $K_{\pi^p}/K_{\pi^{p+1}}$ sont isomorphes. Leur $\bar\phi$-rang est égal à* 1 *ou* 0 *suivant que le conducteur f_χ de χ est premier à p ou non.*

Démonstration. En utilisant l'isomorphisme présenté au début de la démonstration précédente, on constate que K_π/K_{π^2}, $K_{\pi^p}/K_{\pi^{p+1}}$ et $\pi O_K/\pi^2 O_K$ sont des $F_p[G]$-modules isomorphes. Décomposons G en produit direct $G = G'G''$ de deux sous-groupes $G' = \mathrm{Gal}(K/Q^{(p)})$ et $G'' = \mathrm{Gal}(K/K \cap Q^{(f')})$. Ce dernier sous-groupe est donc isomorphe à $\mathrm{Gal}(Q^{(p)}/Q)$. En tant que $F_p[G']$-module, $\pi O_K/\pi^2 O_K$ est isomorphe à $O_K/\pi O_K$. Soit $O^{(p)}$ le localisé en p de l'anneau des entiers de $Q^{(p)}$. Considéré comme G'-module, O_K est isomorphe à $O^{(p)}[G']$. On en déduit que $O_K/\pi O_K$ est isomorphe, en tant que $F_p[G']$-module, à $F_p[G']$. Il en est également ainsi de $\pi O_K/\pi^2 O_K$. Examinons maintenant la structure de G''-module de $\pi O_K/\pi^2 O_K$. Nous avons $\pi = 1-\zeta$ et $\zeta^\sigma = \zeta^{\omega(\sigma)}$ pour tout σ de G. On en déduit la congruence $\pi^\sigma \equiv \omega(\sigma)\pi \bmod (\pi^2)$, pour tout σ de G. D'autre part, on a aussi $x^\sigma \equiv x \bmod (\pi)$, pour tout x de O_K et tout σ de G''. On en déduit: $(\pi x)^\sigma \equiv \omega(\sigma)\pi x \bmod (\pi^2)$ pour tout x de O_K et tout σ de G''. Cette congruence précise donc l'action de G'' sur $\pi O_K/\pi^2 O_K$. Comme l'action de G' est également connue, on peut calculer explicitement les valeurs du caractère γ de $\pi O_K/\pi^2 O_K$. Soient σ un élément de G et $\sigma = \sigma'\sigma''$ sa décomposition en produit d'un élément σ' de G' et d'un élément σ'' de G''; on obtient: $\gamma(\sigma) = \omega(\sigma'')|G'|$ si $\sigma' = 1$ et $\gamma(\sigma) = 0$ si $\sigma' \neq 1$. Le $\bar\phi$-rang de $\pi O_K/\pi^2 O_K$ est le nombre de fois qu'apparaît $\bar\chi$ dans la décomposition de γ en somme de caractères irréductibles; c'est-à-dire $(1/|G|)\sum_{\tau\in G} \gamma(\tau)\bar\chi(\tau^{-1})$. Cette quantité est égale à $(1/|G''|)\sum_{\tau\in G''} \chi(\tau)$ et vaut 1 ou 0 suivant que K_χ soit inclus dans $Q^{(f')}$ ou non. On en déduit le résultat annoncé.

Pour tout entier i désignons par P_i l'ensemble des idéaux de K engendrés par les éléments de K_{π^i}.

Proposition 3.4. *En associant à tout x de K_π l'idéal engendré par x, on définit un isomorphisme de $F_p[G]$-modules de K_π/K_{π^p} sur P_1/P_p. Le $\bar\phi$-rang de P_1/P_p est égal à* 1.

Lemme 3.5. *Soit O_K^* l'ensemble des éléments inversibles de O_K. Alors K_π est un sous-groupe de O_K^* d'indice premier à p.*

Démonstration. Le groupe quotient O_K^*/K_π est isomorphe à $(O_K/\pi O_K)^*$, groupe multiplicatif des éléments inversibles de l'anneau $O_K/\pi O_K$. Nous avons des isomorphismes:

$$O_K/\pi O_K \cong \bigoplus_{1\leqslant j\leqslant g} O_K/\mathfrak{p}_j \quad \text{et} \quad O_K^*/K_\pi \cong \bigoplus_{1\leqslant j\leqslant g} (O_K/\mathfrak{p}_j)^*$$

où $(O_K/\mathfrak{p}_j)^*$ est le groupe multiplicatif du corps $O_K/\mathfrak{p}_j$. Ce groupe est d'ordre premier à p; d'où le résultat énoncé dans le lemme.

Soit E le groupe des unités de K. A partir de l'application de K_π dans P_1 associant à x l'idéal engendré par x, on forme une suite exacte:

$$1 \to ((E\cap K_\pi)/(E\cap K_{\pi^p}))_{\bar\phi} \to (K_\pi/K_{\pi^p})_{\bar\phi} \to (P_1/P_p)_{\bar\phi} \to 1.$$

D'autre part, on déduit de l'inclusion $(K_\pi)^p \subset K_{\pi^p}$, l'existence d'une suite exacte:

$$\big((E\cap K_\pi)/(E\cap K_\pi)^p\big)_{\bar\phi} \to \big((E\cap K_\pi)/(E\cap K_{\pi^p})\big)_{\bar\phi} \to 1.$$

Du lemme précédent, on déduit que l'indice $(E: E\cap K_\pi)$ est premier à p. En conséquence l'injection canonique induit un isomorphisme:

$$(E\cap K_\pi)/(E\cap K_\pi)^p \cong E/E^p.$$

Le caractère $\bar\chi$ est impair et différent de ω; le théorème de Dirichlet montre alors que la $\bar\phi$-composante de E/E^p est réduite à $\{1\}$. En conséquence les $\bar\phi$-composantes de K_π/K_{π^p} et P_1/P_p sont isomorphes. La valeur du $\bar\phi$-rang de P_1/P_p se déduit donc de la proposition 3.2.

Spiegelungssatz. Rappelons le résultat écrit par H. W. Leopoldt en [13]:

PROPOSITION 3.6. *Le ϕ-rang de $\varkappa_\phi$ et le $\bar\phi$-rang de $\varkappa_{\bar\phi}$ sont liés par les inégalités*:

$$\dim_\phi \varkappa_\phi \leqslant \dim_{\bar\phi} \varkappa_{\bar\phi} \leqslant \dim_\phi \varkappa_\phi + 1.$$

Démonstration. Soit N l'extension abélienne d'exposant p, maximale, non ramifiée de K. L'application de réciprocité d'Artin induit un isomorphisme de G-modules entre $\varkappa/\varkappa^p$ et $\mathrm{Gal}(N/K)$ (l'opération de G sur ce dernier groupe est la conjugaison). L'extension N/K est une extension de Kummer. Soit W son radical; c'est l'ensemble des éléments non nuls de N, dont la puissance $p^{\text{ème}}$ appartient à N. La théorie élémentaire de Kummer montre l'existence d'un isomorphisme de groupes entre W/K^* et $\mathrm{Gal}(N/K)$. Dans cet isomorphisme la ϕ-composante (resp. $\bar\phi$-composante) de W/K^* correspond à la $\bar\phi$-composante (resp. ϕ-composante) de $\mathrm{Gal}(N/K)$.

Soit $\mathscr{L}$ l'application de W/K^* dans $\varkappa^{(p)}$, ensemble des éléments de $\varkappa$ annulés par p, ainsi définie: Si w appartient à W, alors w^p appartient à K et comme l'extension $K(w)/K$ est non ramifiée, w^p engendre un idéal qui est la puissance $p^{\text{ème}}$ d'un idéal $\mathfrak{a}$ de K. On définit $\mathscr{L}(wK^*)$ comme étant la classe de l'idéal $\mathfrak{a}$. Il est clair que $\mathscr{L}$ est un $F_p[G]$-homomorphisme. Si wK^* appartient au noyau de $\mathscr{L}$, alors il existe un élément x de K et une unité ε de K telle que $w^p = a^p\varepsilon$. En faisant correspondre à wK^* la classe de ε modulo E^p, on définit un $F_p[G]$-homomorphisme injectif de $\mathrm{Ker}\,\mathscr{L}$ dans E/E^p. Le ϕ-rang de E/E^p est égal à 1 et le $\bar\phi$-rang de E/E^p est nul. On en déduit que le ϕ-rang de $\mathrm{Ker}\,\mathscr{L}$ est inférieur à 1 et que le $\bar\phi$-rang de $\mathrm{Ker}\,\mathscr{L}$ est nul. En considérant les restrictions de $\mathscr{L}$ à la ϕ-composante et la $\bar\phi$-composante de W/K^*, on obtient les inégalités annoncées.

Pour démontrer le point (ii) du théorème, il est nécessaire de préciser cette proposition. Soit I le groupe des idéaux $\mathfrak{a}$ de K pour lesquels il existe une puissance de p, p^u, telle que $\mathfrak{a}^{p^u}$ appartienne à P_1. Si P_0 est le groupe des idéaux principaux de K, premiers à p, on déduit du lemme 3.5 que l'indice

$(P_0: P_1)$ est premier à p. Il s'en suit que l'injection canonique de I dans le groupe des idéaux de K induit un isomorphisme de I/P_1 sur $\varkappa$, groupe des p-classes d'idéaux de K.

PROPOSITION 3.7. *Le ϕ-rang de $\varkappa_\phi$ et le $\bar\phi$-rang de I/P_p sont liés par la relation*:

$$1 + \dim_\phi(\varkappa_\phi) = \dim_{\bar\phi}(I/P_p).$$

Démonstration. Introduisons W_1 ensemble des x de N, tels que x^p appartienne à K_π. Cet ensemble W_1 est inclus dans W et l'injection canonique de W_1 dans W induit un isomorphisme de W_1/K_π sur W/K^*: en effet, soit w un élément de W. Il existe un élément x de K^* tel que pour tout idéal $\mathfrak{P}$ de N au-dessus de p, les $\mathfrak{P}$-valuations de w et x soient égales. Nous avons alors: $wK^* = wx^{-1}K^*$ et $(wx^{-1})^p$ appartient à O_K^*. On déduit du lemme 3.5 que wK^* peut être représenté par un élément de W_1. Le même lemme permet de montrer l'égalité $W_1 \cap K^* = K_\pi$.

Définissons une application $\mathscr{L}_1$ de W_1/K_π dans I/P_1 de la même façon que $\mathscr{L}$; si w appartient à W_1, alors w^p appartient à K_π et w^p engendre un idéal de la forme $\mathfrak{a}^p$, $\mathfrak{a}$ étant un idéal de K. L'image de wK_π par $\mathscr{L}_1$ est $\mathfrak{a}P_1$. Notons $\mathscr{U}$ la surjection canonique de I/P_p sur I/P_1 et notons $(I/P_p)^{(p)}$ l'ensemble des éléments de I/P_p annulés par p. Montrons que l'on a l'égalité:

$$\mathscr{L}_1\big((W_1/K_\pi)_{\bar\phi}\big) = \mathscr{U}\big((I/P_p)^{(p)}_{\bar\phi}\big).$$

Soit w un élément de W_1. Comme l'extension $K(w)/K$ est non ramifiée, w^p vérifie les conditions ([8], § 39): il existe des éléments x_j de K tels que $w^p \equiv x_j^p \bmod \mathfrak{p}_j^p$ pour $1 \leqslant j \leqslant g$. Mais comme w^p appartient à K_π, x_j^p vérifie la congruence $x_j^p \equiv 1 \bmod(\mathfrak{p}_j)$. D'où l'on déduit $x_j \equiv 1 \bmod(\mathfrak{p}_j)$ et $x_j^p \equiv 1 \bmod(\mathfrak{p}_j^p)$. Finalement, w^p appartient à K_{π^p} et $\mathscr{L}_1(wK_\pi)$ appartient à $\mathscr{U}\big((I/P)^{(p)}\big)$. Réciproquement, si $\mathfrak{a}$ est un idéal de I tel que $\mathfrak{a}P_p$ appartienne à $(I/P_p)^{(p)}_{\bar\phi}$, alors $\mathfrak{a}^p$ est un idéal principal engendré par un élément a de K_{π^p}. Posons $w = \sqrt[p]{a}$. L'extension $K(\sqrt[p]{a})/K$ est non ramifiée. Donc w appartient à W_1 et $\mathscr{L}_1\big((wK_\pi)_{\bar\phi}\big) = \mathscr{U}(\mathfrak{a}P_p)$.

Le résultat énoncé se déduit de l'égalité démontrée plus haut: comme $(E/E^p)_{\bar\phi}$ est réduit à $\{1\}$, la restriction de $\mathscr{L}_1$ à $(W_1/K_\pi)_{\bar\phi}$ est injective et on a donc:

$$\dim_\phi(\varkappa_\phi) = \dim_\phi \mathscr{L}_1\big((W_1/K_\pi)_{\bar\phi}\big).$$

D'autre part, le noyau de $\mathscr{U}$, P_1/P_p, est inclus dans $(I/P_p)^{(p)}$ et son $\bar\phi$-rang est 1 (Proposition 3.4). En conséquence on a la relation:

$$\dim_{\bar\phi}(I/P_p)^{(p)}_{\bar\phi} = 1 + \dim_{\bar\phi} \mathscr{U}\big((I/P_p)^{(p)}_{\bar\phi}\big).$$

Enfin il est clair que I/P_p et $(I/P_p)^{(p)}$ ont même $\bar\phi$-rang.

4. Une formule explicite pour le symbole de puissance résiduelle. Nous désignons par $(\cdot)$ le symbole de puissance résiduelle attaché à K et p. Rappelons qu'il s'agit d'une racine $p^{\text{ème}}$ de l'unité définie par

$$\left(\frac{\beta}{\mathfrak{a}}\right)\sqrt[p]{\beta} = \left(\sqrt[p]{\beta}\right)^{(\mathfrak{a},K(\sqrt[p]{\beta})/K)},$$

β étant un élément de K, $\mathfrak{a}$ un idéal de K non ramifié dans $K(\sqrt[p]{\beta})/K$ et $(\mathfrak{a}, K(\sqrt[p]{\beta})/K)$ le symbole d'Artin. Comme $K_{\pi^{p+1}}$ est l'ensemble des éléments p-hyperprimaires de K, ce symbole est défini sur le produit des $Z_p[G]$-modules: $E/E^p \times I/P_{p+1}$. Il vérifie, pour tout σ de G, tout ε de E, et tout $\mathfrak{a}$ de I, les relations

$$\left(\frac{\varepsilon^\sigma}{\mathfrak{a}^\sigma}\right) = \left(\frac{\varepsilon}{\mathfrak{a}}\right)^\sigma \quad \text{et} \quad \left(\frac{\varepsilon^{\mu_\phi}}{\mathfrak{a}}\right) = \left(\frac{\varepsilon}{\mathfrak{a}^{\mu_{\bar\phi}}}\right),$$

μ_ϕ (resp. $\mu_{\bar\phi}$) désignant un élément de $Z[G]$ tel que $\mu_\phi \equiv e_\phi$ (resp. $\mu_{\bar\phi} \equiv e_{\bar\phi}) \bmod (p)$.

Soit n un entier positif. Nous noterons $(\cdot)_n$ le symbole de puissance résiduelle attaché au corps cyclotomique $Q^{(fp^n)}$ et à l'entier p^{n+1}. Fixons quelques notations concernant des racines de l'unité dans ce corps: On désigne par ζ_n une racine primitive $(p^{n+1})^{\text{ème}}$ de l'unité telle que $\zeta_n^{p^n} = \zeta$. On désigne par ζ_n' une racine de l'unité telle que $\zeta_n'^{f'} = \zeta_n$ et on pose $\zeta' = \zeta_n'^{p^n}$. Cette quantité est une racine $f^{\text{ème}}$ de l'unité et verifie $\zeta'^{f'} = \zeta$. Posons encore: $\pi' = 1-\zeta'$, $\pi_n = 1-\zeta_n$ et $\pi_n' = 1-\zeta_n'$. La démonstration écrite ci-après utilise essentiellement un calcul explicite du symbole $\left(\frac{\pi_n'}{\alpha}\right)_n$, α étant un élément de K_π.

Rappelons que $\left(\frac{\pi_n'}{\alpha}\right)_n$ s'exprime en vertu d'une formule classique, comme le produit des symboles de Hilbert (π_n', α) relatifs aux complétés de $Q^{(fp^n)}$ en les différents idéaux premiers de ce corps au-dessus de p. Utilisant la valeur explicite de ces symboles de Hilbert donnée par la proposition 2.2 et la relation élémentaire:

$$\mathrm{Tr}_{Q^{(fp^n)}/Q^{(f)}}\left(\frac{\zeta_n'}{\pi_n'}\right) = p^n\frac{\zeta'}{\pi'}$$

on obtient la formule

$$\left(\frac{\pi_n'}{\alpha}\right)_n = \prod_{\mathfrak{P}} \zeta_n^{a(\mathfrak{P})},$$

avec

$$a(\mathfrak{P}) = -\frac{1}{f}\mathrm{Tr}_{\mathfrak{P}}\left(\frac{\zeta'}{\pi'}\log_{\mathfrak{P}}(\alpha)\right).$$

Ce produit est étendu aux idéaux $\mathfrak{P}$ de $Q^{(f)}$ au-dessus de p. L'expression $\mathrm{Tr}_{\mathfrak{P}}$ désigne la trace dans l'extension $Q^{(f)}/Q$ complétée en $\mathfrak{P}$ et $\log_{\mathfrak{P}}$ le logarithme dans le complété de $Q^{(f)}$ pour le même idéal.

Pour globaliser ce résultat, introduisons la fonction L_n définie sur K_π, à valeurs dans K et ainsi définie:

$$L_n(\beta) = -\sum_{1 \leq m \leq p^{n+2}} \frac{(1-\beta)^m}{m}.$$

LEMME 4.1. *Pour tout β appartenant à K_π et tout idéal $\mathfrak{P}$ premier de $Q^{(f)}$ au-dessus de p, on a:*

(i) $L_n(\beta^\sigma) = L_n(\beta)^\sigma$ *pour tout* σ *de* G,

(ii) $L_n(\beta) \equiv \log_{\mathfrak{P}}(\beta) \bmod (\mathfrak{P}^{p^{n+1}})$,

(iii) $\frac{1}{f}\mathrm{Tr}_{\mathfrak{P}}\left(\frac{\zeta'}{\pi'}L_n(\beta)\right) \equiv \frac{1}{f}\mathrm{Tr}_{\mathfrak{P}}\left(\frac{\zeta'}{\pi'}\log_{\mathfrak{P}}(\beta)\right) \bmod (p^{n+1})$.

Démonstration. L'assertion (i) est évidente. Pour démontrer les deux autres, vérifions que si m est supérieur à p^{n+2}, alors la $\mathfrak{P}$-valuation de $(1-\beta)^m/m$ est supérieure à $(n+1)(p-1)+3$. Posons $m = p^e l$ avec l premier à p. La $\mathfrak{P}$-valuation considérée est $m-e(p-1)$. Lorsque e est inférieur à $n+2$, l'inégalité cherchée résulte de la relation $p^{n+2} \geqslant (2n+3)(p-1)+3$, valable pour $n \geqslant 0$. Lorsque e est supérieur à $n+2$, on peut montrer à l'aide d'une récurrence sur e, l'inégalité: $p^e \geqslant (n+1+e)(p-1)+3$. On en déduit (ii) et (iii).

La somme des traces locales, lorsque $\mathfrak{P}$ parcourt les idéaux premiers de $Q^{(f)}$ au-dessus de p étant égale à la trace globale, on déduit du lemme la formule suivante:

PROPOSITION 4.2. *Soit α un élément de K_π. Le symbole de puissance résiduelle relatif à $Q^{(fp^n)}$ et à l'entier p^{n+1} est donné par:*

$$\left(\frac{\pi_n'}{\alpha}\right)_n = \zeta_n^a,$$

avec

$$a = -\frac{1}{f}\mathrm{Tr}_{Q^{(f)}/Q}\left(\frac{\zeta'}{\pi'}L_n(\alpha)\right).$$

5. Démonstration du théorème. On conserve les notations introduites précédemment en 1, 3 et 4. Posons de plus $\theta = N_{Q^{(f)}/K}(\pi')$. Désignons par $\mu_\phi = \sum_{\sigma\in G} a_\sigma \sigma$ un élément de $Z[G]$ tel que $\mu_\phi \equiv e_\phi \bmod (p)$ et tel que $\sum_{\sigma\in G} a_\sigma = 0$.

PROPOSITION 5.1. *On suppose que le caractère χ vérifie les hypothèses* A *et* B. *La ϕ-composante de $(E_\chi/F_\chi)_p$, notée $(E_\chi/F_\chi)_\phi$, est réduite à $\{1\}$ si et seulement si θ^{μ_ϕ} n'appartient pas à K^p.*

Démonstration. Rappelons que E_χ/E_χ^p est un $F_p[G]$-module de ϕ-rang égal à 1. La condition $(E_\chi/F_\chi)_\phi = \{1\}$ équivaut donc à la condition

$(F_\chi E_\chi^p/E_\chi^p)_\phi \neq \{1\}$. Introduisons $\theta_\chi = N_{\mathbf{Q}(f_\chi)/K_\chi}(1-\zeta_\chi)$, ζ_χ étant une racine primitive de l'unité d'ordre f_χ. Posons $D_\chi = \prod_{l|g_\chi}(1-\sigma_\chi^{g_\chi/l})$; dans cette expression σ_χ désigne un générateur de G_χ et l parcourt l'ensemble des nombres premiers divisant g_χ. Il découle de la définition de F_χ, [12] ou [14], que $(F_\chi E_\chi^p/E_\chi^p)$ est engendré, en tant que $F_p[G]$-module, par $\theta_\chi^{D_\chi}$. La ϕ-composante de ce module est donc engendré par $\theta_\chi^{\mu_\phi D_\chi}$. La condition $(E_\chi/F_\chi)_\phi = \{1\}$ équivaut donc à la condition: $\theta_\chi^{\mu_\phi D_\chi}$ n'appartient pas à E_χ^p. Remarquons encore que l'intersection $K_\chi^p \cap E_\chi$ est égale à E_χ^p. Ainsi dans l'énoncé de cette dernière condition on peut remplacer E_χ^p par K_χ^p.

Examinons d'autre part la condition: θ^{μ_ϕ} n'appartient pas à K^p. Pour tout σ de $\mathrm{Gal}(K/K_\chi)$, on a $\sigma e_\phi = e_\phi$. On en déduit $\sigma\mu_\phi \equiv \mu_\phi \bmod(p)$. Si $b = [K:K_\chi]$, le rapport $N_{K/K_\chi}(\theta^{\mu_\phi})/\theta^{b\mu_\phi}$ appartient à K^p. Ainsi, la condition θ^{μ_ϕ} n'appartient pas à K^p est équivalente à: $N_{K/K_\chi}(\theta^{\mu_\phi})$ n'appartient pas à K_χ^p.

Il reste donc à démontrer l'équivalence entre les deux conditions:

(i) $\theta_\chi^{\mu_\phi D_\chi}$ appartient à K_χ^p.

(ii) $N_{K/K_\chi}(\theta^{\mu_\phi})$ appartient à K_χ^p.

Distinguons deux cas: supposons d'abord que p divise f_χ. On a alors $f = f_\chi$ et on peut choisir $\zeta_\chi = \zeta'$. Considérons l'application V_χ introduite dans le paragraphe 3. L'image de D_χ par V_χ est $\prod_{l|g_\chi}(1-\varepsilon_l)$; dans ce produit l parcourt les diviseurs premiers de g_χ et ε_l est une racine primitive $l^{\text{ème}}$ de l'unité. Cette quantité est donc une unité de $\mathbf{Z}_p[\chi]$ et il s'en suit que $e_\phi D_\chi$ est un élément inversible de l'anneau $e_\phi \mathbf{Z}_p[G_\chi]$. Le quotient K_χ/K_χ^p est un $\mathbf{Z}_p[G_\chi]$-module et la condition $\theta_\chi^{\mu_\phi D_\chi}$ appartient à K_χ^p équivaut donc à: $\theta_\chi^{\mu_\phi}$ appartient à K_χ^p. Enfin, il découle de la définition de θ_χ l'égalité $N_{K/K_\chi}(\theta) = \theta_\chi$. Ceci termine la démonstration dans le premier cas.

Supposons maintenant que p ne divise pas f_χ. On a alors $pf_\chi = f$ et on peut choisir $\zeta'^p = \zeta_\chi$. Ecrivons une relation de Bezout entre f_χ et p sous la forme $1+vf_\chi = \lambda p$. En décomposant le polynôme $X^p - \zeta'^p$ sur $\mathbf{Q}^{(f)}$, on obtient:

$$N_{\mathbf{Q}^{(f)}/\mathbf{Q}^{(f_\chi)}}(1-\zeta') = (1-\zeta'^p)/(1-\zeta'^{\lambda p})$$

et comme $K \cap \mathbf{Q}^{(f_\chi)} = K_\chi$, on en déduit:

$$N_{K/K_\chi}(\theta) = N_{\mathbf{Q}^{(f)}/K_\chi}\big((1-\zeta'^p)/(1-\zeta'^{\lambda p})\big).$$

Soit σ_0 l'automorphisme de $K_\chi/\mathbf{Q}$ défini à l'aide du symbole d'Artin par $\sigma_0 = (\lambda, K_\chi)$. L'égalité précédente peut encore s'écrire $N_{K/K_\chi}(\theta) = \theta_\chi^{1-\sigma_0}$. Considérons l'application V_χ. Comme dans le cas précédent l'image de D_χ par V_χ est une unité de $\mathbf{Z}_p[\chi]$. D'autre part, on déduit de l'hypothèse B que σ_0 est différent de l'identité. Ainsi $V_\chi(1-\sigma_0) = 1-\chi(\sigma_0)$ est aussi une unité $\mathbf{Z}_p[\chi]$. Les deux conditions: $\theta_\chi^{\mu_\phi(1-\sigma_0)}$ appartient à K_χ^p, d'une part, et $\theta_\chi^{\mu_\phi D_\chi}$ appartient à K_χ^p, d'autre part, sont donc équivalentes. Cela termine la démonstration.

PROPOSITION 5.2. *Soit $\mathfrak{a}$ un idéal de K appartenant à I et tel que $\mathfrak{a}P_{p+1}$ appartienne à la $\bar{\phi}$-composante de I/P_{p+1}. Soit n la p-valuation de $B_{\bar{\chi}^{-1}}$. Soit α appartenant à K_π tel que αK_{π^p} appartienne à la $\bar{\phi}$-composante de K_π/K_{π^p} et tel que l'idéal engendré par α soit $\mathfrak{a}^{p^n}$.*

(i) *Si α appartient à K_{π^p}, alors le symbole de puissance résiduelle vérifie* $\left(\frac{\theta^{\mu_\phi}}{\mathfrak{a}}\right) = 1$.

(ii) *Réciproquement, si α n'appartient pas à K_{π^p}, alors il existe σ appartenant à G tel que* $\left(\frac{\theta^{\mu_\phi}}{\mathfrak{a}^\sigma}\right) \neq 1$.

Remarque. La condition $\sum_{\sigma\in G} a_\sigma = 0$ vérifiée par μ_ϕ implique que θ^{μ_ϕ} est une unité de K, même si le conducteur f_χ de χ est égal à p.

Démonstration. L'existence de α vérifiant les conditions indiquées résulte des propositions 3.1 et 3.4. Pour tout entier n, désignons par G_n le groupe de Galois de $\mathbf{Q}^{(f p^n)}/\mathbf{Q}$. Notons encore μ_ϕ un relèvement de μ_ϕ dans $\mathbf{Z}[G_n]$. En vertu des propriétés classiques du symbole de puissance résiduelle et de l'égalité $N_{\mathbf{Q}^{(f p^n)}/\mathbf{Q}^{(f)}}(\pi'_n) = \pi'$, nous avons:

$$\left(\frac{\theta^{\mu_\phi}}{\mathfrak{a}}\right) = \left(\frac{\pi'^{\mu_\phi}}{\mathfrak{a}}\right)_0 = \left(\frac{\pi'^{\mu_\phi}_n}{\mathfrak{a}}\right)_n^{p^n} = \left(\frac{\pi'^{\mu_\phi}_n}{\mathfrak{a}}\right)_n.$$

Le reste de la démonstration a pour objet le calcul de ce symbole, à partir de la formule donnée par la proposition 4.2. Les exposants de ζ_n qui vont intervenir, seront considérés comme des éléments de $\mathbf{Z}_p \otimes \mathbf{Z}$ (nous écrivons $\otimes$ pour $\otimes_{\mathbf{Z}}$). Cet anneau est un sous-anneau de la $\mathbf{Q}_p[G_0]$-algèbre $\mathbf{Q}_p \otimes \mathbf{Q}^{(f)}$. Elle-même est un sous-anneau de la $\mathbf{Q}_p(\bar{\chi})[G_0]$-algèbre $\mathbf{Q}_p(\bar{\chi}) \otimes \mathbf{Q}^{(f)}$. Sur cette algèbre, il est clair que l'action de $\mathbf{Q}_p(\bar{\chi})$ est donnée par $\varepsilon'(\varepsilon \otimes \beta) = (\varepsilon'\varepsilon) \otimes \beta$ et que l'action de G_0 est donnée par $\sigma(\varepsilon \otimes \beta) = \varepsilon \otimes \beta^\sigma$. Précisons encore que β^σ et $\sigma(\beta)$ ont la même signification; le groupe G_0 agit sur $\mathbf{Q}^{(f)}$ additivement et multiplicativement et les deux structures de G_0-modules interviennent. Les deux notations seront donc utilisées.

Si ψ est un caractère de conducteur f_ψ divisant f, nous désignerons par ψ_0^{-1} le caractère de Dirichlet associé à ψ^{-1}: c'est l'application définie par $\psi_0^{-1}(a) = \psi^{-1}(a)$ si a est premier à f_ψ et $\psi_0^{-1}(a) = 0$ sinon. L'indicateur d'Euler est noté φ.

LEMME 5.3. *Soit α un élément de K_π. Si ψ est un caractère $\mathbf{Q}_p$-équivalent à $\bar{\chi}$, on note e_ψ et $e_{\psi^{-1}}$ les idempotents associés à ψ et ψ^{-1}, c'est-à-dire*

$$e_\psi = \frac{1}{|G_0|}\sum_{\sigma\in G_0}\psi(\sigma^{-1})\sigma \quad \text{et} \quad e_{\psi^{-1}} = \frac{1}{|G_0|}\sum_{\sigma\in G_0}\psi(\sigma)\sigma.$$

Pour tout entier n, on a l'égalité:

$$\left(\frac{\pi_n'^{\mu}\phi}{\alpha}\right)_n = \zeta_n^a,$$

avec

$$a = \frac{\varphi(f)}{f}\sum_{\psi|\bar{\phi}}(1-p\psi_0^{-1}(p))B_{\psi^{-1}}e_{\psi^{-1}}(1\otimes\zeta')e_{\psi}(1\otimes L_n(\alpha)).$$

Démonstration. Soit σ un élément de G. On note de la même façon un prolongement de σ à $\mathbb{Q}^{(fp^n)}$. En vertu de la proposition 4.2, nous avons:

$$\left(\frac{\pi_n'^{\sigma}}{\alpha}\right)_n = \left(\frac{\pi_n'}{\alpha^{\sigma^{-1}}}\right)_n^{\sigma} = \left(\frac{\pi_n'}{\alpha^{\sigma^{-1}}}\right)_n^{\omega(\sigma)} = \zeta_n^b,$$

avec

$$b = -\frac{\omega(\sigma)}{f}\otimes \mathrm{Tr}_{\mathbb{Q}(f)/\mathbb{Q}}\left(\frac{\zeta'}{\pi'}L_n(\alpha^{\sigma^{-1}})\right) = -\frac{\omega(\sigma)}{f}\otimes \mathrm{Tr}_{\mathbb{Q}(f)/\mathbb{Q}}\left(\sigma\left(\frac{\zeta'}{\pi'}\right)L_n(\alpha)\right).$$

Nous en déduisons:

$$\left(\frac{\pi_n'^{\mu}\phi}{\alpha}\right) = \zeta_n^c,$$

avec

$$c = -\frac{1}{f}\mathrm{Tr}_{\mathbb{Q}(f)/\mathbb{Q}}\left(e_{\bar{\phi}^{-1}}\left(1\otimes\frac{\zeta'}{\pi'}\right)(1\otimes L_n(\alpha))\right).$$

Dans cette expression $\bar{\phi}^{-1}$ désigne le caractère $\bar{\phi}^{-1}=\omega^{-1}\phi$ et $e_{\bar{\phi}^{-1}}$ l'idempotent:

$$e_{\bar{\phi}^{-1}} = \frac{1}{|G_0|}\sum_{\sigma\in G_0}\omega(\sigma)\phi(\sigma^{-1})\sigma.$$

Décomposons cet idempotent sur l'algèbre $\mathbb{Q}_p(\bar{\chi})[G_0]$. Nous obtenons $e_{\bar{\phi}^{-1}} = \sum_{\psi|\bar{\phi}} e_{\psi^{-1}}$. On en déduit:

$$\mathrm{Tr}_{\mathbb{Q}(f)/\mathbb{Q}}\left(e_{\psi^{-1}}\left(1\otimes\frac{\zeta'}{\pi'}\right)(1\otimes L_n(\alpha))\right)$$

$$= \sum_{\sigma\in G_0}\sigma e_{\psi^{-1}}\left(1\otimes\frac{\zeta'}{\pi'}\right)(1\otimes L_n(\alpha)) = \sum_{\sigma\in G_0}\psi^{-1}(\sigma)e_{\psi^{-1}}\left(1\otimes\frac{\zeta'}{\pi'}\right)\sigma(1\otimes L_n(\alpha))$$

$$= \varphi(f)e_{\psi^{-1}}\left(1\otimes\frac{\zeta'}{\pi'}\right)e_{\psi}(1\otimes L_n(\alpha)).$$

Nous obtenons ainsi:

$$\left(\frac{\pi_n'^{\mu}\phi}{\alpha}\right)_n = \zeta_n^d,$$

avec

$$d = -\frac{\varphi(f)}{f}\sum_{\psi|\bar{\phi}}e_{\chi^{-1}}\left(1\otimes\frac{\zeta'}{\pi'}\right)e_{\psi}(1\otimes L_n(\alpha))$$

et il reste à transformer $e_{\psi^{-1}}\left(1\otimes\frac{\zeta'}{\pi'}\right)$. Nous avons

$$\frac{\zeta'}{\pi'} = -1+\frac{1}{\pi'} \quad \text{et} \quad \frac{1}{\pi'} = -\frac{1}{f}\sum_{1\leq a\leq f-1}a\zeta'^{a}.$$

D'où

$$e_{\psi^{-1}}\left(1\otimes\frac{\zeta'}{\pi'}\right) = -\frac{1}{f}\sum_{1\leq a\leq f-1}ae_{\psi^{-1}}(1\otimes\zeta'^{a}).$$

Supposons que le conducteur de $\bar{\chi}$, soit divisible par p. On a alors $f = f_{\bar{\chi}}$. Si a est premier à f, on a l'égalité:

$$e_{\psi^{-1}}(1\otimes\zeta'^{a}) = \psi^{-1}(a)e_{\psi^{-1}}(1\otimes\zeta').$$

Si a n'est pas premier à f, il existe un élément σ de G_0 tel que $\zeta'^{a\sigma}=\zeta'^{a}$ et tel que $\psi(\sigma)\neq 1$. De l'égalité

$$e_{\psi^{-1}}(1\otimes\zeta'^{a}) = \psi^{-1}(\sigma)e_{\psi^{-1}}(1\otimes\zeta'^{a}),$$

on déduit

$$e_{\psi^{-1}}(1\otimes\zeta'^{a}) = 0.$$

Nous obtenons ainsi:

$$e_{\psi^{-1}}\left(1\otimes\frac{\zeta'}{\pi'}\right) = -\frac{1}{f}\sum_{1\leq a\leq f-1}a\psi_0^{-1}(a)e_{\psi^{-1}}(1\otimes\zeta') = -B_{\psi^{-1}}e_{\psi^{-1}}(1\otimes\zeta').$$

Cela termine la démonstration du lemme dans le cas où $f = f_{\bar{\chi}}$.

Supposons maintenant que $f_{\bar{\chi}}$ ne soit pas égal à f. On a alors $f_{\bar{\chi}} = f'$. Comme précédemment, on a

$$e_{\psi^{-1}}(1\otimes\zeta'^{a}) = \psi^{-1}(a)e_{\psi^{-1}}(1\otimes\zeta')$$

lorsque a est premier à f. Si a et f ont pour PGCD p et si $a' = a/p$, on a:

$$e_{\psi^{-1}}(1\otimes\zeta'^{a}) = \psi^{-1}(a')e_{\psi^{-1}}(1\otimes\zeta'^{p}).$$

Si enfin l'entier a n'est pas premier à f', on a

$$e_{\psi^{-1}}(1\otimes\zeta'^{a}) = 0.$$

On obtient ainsi:

$$e_{\psi^{-1}}\left(1\otimes\frac{\zeta'}{\pi'}\right)=\left(-\frac{1}{f}\sum_{\substack{1\leqslant a\leqslant f\\(a,f)=1}}a\psi^{-1}(a)\right)e_{\psi^{-1}}(1\otimes\zeta')$$
$$-\left(\frac{1}{f'}\sum_{\substack{1\leqslant a\leqslant f'\\(a,f')=1}}a\psi^{-1}(a)\right)e_{\psi^{-1}}(1\otimes\zeta'^{p}).$$

Avec la dernière somme apparaît le nombre de Bernoulli $B_{\psi^{-1}}$. Quant à l'autre somme, on peut, à l'aide d'un calcul élémentaire, l'exprimer ainsi (L.II.10 [5]):

$$\frac{1}{f}\sum a\psi^{-1}(a)=\left(1-\psi_0^{-1}(p)\right)B_{\psi^{-1}}.$$

Considérons enfin $e_{\psi^{-1}}(1\otimes\zeta'^{p})$: Soit $1=up+vf'$ une relation de Bezout entre p et f'. Nous avons alors $\mathrm{Tr}_{\boldsymbol{Q}^{(f)}/\boldsymbol{Q}^{(f')}}(\zeta')=-\zeta'^{pu}$ et on en déduit:

$$e_{\psi^{-1}}(1\otimes\zeta')=-\frac{1}{p-1}e_{\psi^{-1}}(1\otimes\zeta'^{pu})=-\frac{1}{p-1}\psi^{-1}(u)\,e_{\psi^{-1}}(1\otimes\zeta'^{p}).$$

D'où la relation

$$e_{\psi^{-1}}(1\otimes\zeta'^{p})=-(p-1)\psi_0^{-1}(p)\,e_{\psi^{-1}}(1\otimes\zeta').$$

Finalement nous avons démontré (dans les deux cas) la relation:

$$e_{\psi^{-1}}\left(1\otimes\frac{\zeta'}{\pi'}\right)=-\left(1-p\psi_0^{-1}(p)\right)B_{\psi^{-1}}\,e_{\psi^{-1}}(1\otimes\zeta').$$

Ceci termine la démonstration du lemme 5.3.

Nous pouvons maintenant justifier le point (i) de la proposition 5.2. Soit $A^{(f)}$ l'anneau des entiers de $\boldsymbol{Q}^{(f)}$. Nous appliquons le lemme précédent en donnant à n la valeur de la p-valuation de $B_{\bar{\chi}^{-1}}$. Supposons que α appartienne à K_{π^p}. On en déduit, à l'aide du lemme 4.1 (ii) la congruence $L_n(\alpha)\equiv 0 \bmod(\pi^p)$ et, dans l'anneau $\boldsymbol{Z}_p[\bar{\chi}]\otimes A^{(f)}$, la congruence:

$$e_\psi\left(1\otimes L_n(\alpha)\right)\equiv 0 \bmod(1\otimes\pi^p).$$

D'autre part, $\varphi(f)\,e_{\psi^{-1}}(1\otimes\zeta')$ appartient à $\boldsymbol{Z}_p[\bar{\chi}]\otimes A^{(f)}$. Nous avons donc:

$$\frac{\varphi(f)}{f}\sum_{\psi|\phi}\left(1-p\psi_0^{-1}(p)\right)B_{\psi^{-1}}\,e_{\psi^{-1}}(1\otimes\zeta')\,e_\psi\left(1\otimes L_n(\alpha)\right)\equiv 0 \bmod(p^n\otimes\pi).$$

Mais cette expression se trouve en fait dans $\boldsymbol{Z}_p\otimes\boldsymbol{Z}$. Elle est donc congrue à 0 modulo p^{n+1} et le symbole $\left(\frac{\theta^{\mu}\phi}{\mathfrak{a}}\right)$ est égal à 1.

Pour établir le point (ii) de la proposition 5.2, il est nécessaire de faire encore des calculs.

LEMME 5.4. *Soit ψ un caractère $\boldsymbol{Q}_p$-équivalent à $\bar{\chi}$. Alors on a:*

$$e_{\psi^{-1}}(1\otimes\zeta')\,e_\psi(1\otimes\zeta')=-\left(f/\varphi(f)^2\right)(1\otimes 1)$$

ou $-\left(f/p\varphi(f)^2\right)(1\otimes 1)$ suivant que le conducteur de $\bar{\chi}$, $f_{\bar{\chi}}$, soit divisible par p ou non.

Démonstration. Soit δ un caractère de conducteur f_δ divisant $f_{\bar{\chi}}$. Considérons le comme un homomorphisme de $(\boldsymbol{Z}/f_\delta\boldsymbol{Z})^*$ dans le groupe des racines $f_\delta^{\text{ème}}$ de l'unité. Soit ξ une racine d'ordre f_δ de l'unité. Posons

$$\mathscr{G}(\delta,\xi)=\sum\delta(a)\otimes\xi^a,$$

cette somme étant étendue aux éléments a de $(\boldsymbol{Z}/f_\delta\boldsymbol{Z})^*$. Cet élément de $\boldsymbol{Q}_p(\bar{\chi})\otimes\boldsymbol{Q}^{(f)}$ est une somme de Gauss. Les propriétés que nous allons utiliser sont classiques. A toute décomposition de f_δ en produit de deux entiers premiers entre eux f_1 et f_2, correspond une décomposition de $(\boldsymbol{Z}/f_\delta\boldsymbol{Z})^*$ en produit direct de $(\boldsymbol{Z}/f_1\boldsymbol{Z})^*$ et $(\boldsymbol{Z}/f_2\boldsymbol{Z})^*$, une décomposition du caractère δ en produit de deux caractères δ_1 et δ_2, de conducteurs respectifs f_1 et f_2, et enfin une décomposition de ξ en produit de deux racines ξ_1 et ξ_2, d'ordres respectifs f_1 et f_2. La quantité $\mathscr{G}(\delta,\xi)$ est alors le produit de $\mathscr{G}(\delta_1,\xi_1)$ et $\mathscr{G}(\delta_2,\xi_2)$. L'étude de $\mathscr{G}(\delta,\xi)$ se trouve ainsi ramenée au cas où f_δ est une puissance d'un nombre premier. Supposons donc un instant que f_δ soit la forme l^p, l premier et calculons le produit $\mathscr{G}(\delta,\xi)\,\mathscr{G}(\delta^{-1},\xi)$. Il se met sous la forme:

$$\sum_a\sum_b\delta(ab^{-1})\otimes\xi^{a+b}=\sum_c\delta(c)\otimes\sum_b\xi^{b(c+1)},$$

les sommes étant étendues au groupe $(\boldsymbol{Z}/f_\delta\boldsymbol{Z})^*$. La dernière somme est la trace de ξ^{c+1} dans l'extension $\boldsymbol{Q}^{(l^p)}/\boldsymbol{Q}$. Cette trace est égale 0, ou $-l^{p-1}$ ou l^p-l^{p-1} suivant les valeurs de c. Nous obtenons ainsi

$$\mathscr{G}(\delta,\xi)\,\mathscr{G}(\delta^{-1},\xi)=\delta(-1)\,l^n(1\otimes 1).$$

Revenons au cas général, où f_δ est un diviseur de f. Grâce à la propriété de décomposition énoncée plus haut, nous obtenons:

$$\mathscr{G}(\delta,\xi)\,\mathscr{G}(\delta^{-1},\xi)=\delta(-1)\,f_\delta(1\otimes 1).$$

Supposons que le conducteur de $\bar{\chi}$ soit égal à f. On a la relation

$$\varphi(f)\,e_{\psi^{-1}}(1\otimes\zeta')=\mathscr{G}(\psi,\zeta')$$

et une relation analogue en remplaçant ψ par ψ^{-1}. On en déduit le premier des résultats annoncés.

Supposons maintenant que le conducteur de $\bar{\chi}$ soit premier à f. Ce conducteur est alors égal à f' et on a l'égalité:

$$\varphi(f')\,e_{\psi^{-1}}(1\otimes\zeta'^{p})=\mathscr{G}(\psi,\zeta'^{p});$$

de même en remplaçant ψ par ψ^{-1}. D'autre part, une relation liant $e_{\psi^{-1}}(1\otimes\zeta'^{p})$ et $e_{\psi^{-1}}(1\otimes\zeta')$ a été établie à la fin de la démonstration du lemme 5.3. On en déduit la seconde des égalités annoncées.

LEMME 5.5. *Soit ψ un caractère Q_p-équivalent à $\bar\chi$. La quantité $\varphi(f)e_\psi(1\otimes\zeta')$ appartient à l'anneau $\mathbf{Z}_p[\bar\chi]\otimes A^{(f)}$. Si p divise le conducteur de $\bar\chi$, alors on a, dans cet anneau, la congruence*

$$\varphi(f)e_\psi(1\otimes\zeta')\equiv 0 \bmod (1\otimes\pi).$$

Démonstration. Décomposons le caractère $\bar\chi$ de la façon suivante $\bar\chi=\omega^i\delta$, avec δ caractère de conducteur premier à p et i entier tel que $0\leqslant i\leqslant p-2$. Si p divise $f_{\bar\chi}$, l'entier i n'est pas nul. La propriété de décomposition de $\mathscr{G}(\psi^{-1},\zeta')$ énoncée dans la démonstration du lemme précédent montre que, pour obtenir le résultat annoncé, il suffit de vérifier les congruences:

$$\mathscr{G}(\omega^{-i},\zeta)\equiv 0 \bmod (1\otimes\pi) \quad \text{pour} \quad 1\leqslant i\leqslant p-2.$$

Mais nous avons (les sommes étant étendues aux entiers a entre 1 et $p-1$):

$$\mathscr{G}(\omega^{-i},\zeta)=\sum\omega^{-i}(a)\otimes\zeta^a=\sum\omega^{-i}(a)\otimes(\zeta^a-1)\equiv 0 \bmod (1\otimes\pi).$$

Remarque. En s'appuyant sur un calcul classique de sommes de Gauss liant $\mathscr{G}(\omega^{-1},\zeta)$, $\mathscr{G}(\omega^{-i},\zeta)$, $\mathscr{G}(\omega^{-i-1},\zeta)$, on montrerait les congruences plus précises: $\mathscr{G}(\omega^{-i},\zeta)\equiv 0 \bmod (1\otimes\pi^i)$. On en déduirait pour $1\leqslant i\leqslant p-2$, le résultat:

$$\varphi(f)e_\psi(1\otimes\zeta')\equiv 0 \bmod (1\otimes\pi^i).$$

Mais une telle précision ne nous a pas paru utile à cette démonstration.

Notons $H_{\bar\chi}$ le groupe de Galois de $Q_p(\bar\chi)/Q_p$. Les caractères Q_p-équivalents à $\bar\chi$ sont de la forme $\tau\circ\bar\chi$, τ parcourant $H_{\bar\chi}$. L'algèbre $Q_p(\bar\chi)\otimes Q^{(f)}$ est aussi un module sur $H_{\bar\chi}$: on pose $\tau(\varepsilon\otimes x)=\varepsilon^\tau\otimes x$ avec ε dans $Q_p(\bar\chi)$, τ dans $H_{\bar\chi}$ et x dans $Q^{(f)}$.

LEMME 5.6. *Soit ψ un caractère Q_p-équivalent à $\bar\chi$ et soit n un entier. Pour tout α de K_π, il existe $\alpha_{\psi,n}$ appartenant à $Q_p(\bar\chi)$ tel que:*

$$e_\psi\big(1\otimes L_n(\alpha)\big)=\alpha_{\psi,n}e_\psi(1\otimes\zeta').$$

De plus, pour tout τ de $H_{\bar\chi}$ et tout σ de G, on a les relations:

$$\alpha_{\tau\circ\psi,n}=(\alpha_{\psi,n})^\tau \quad \text{et} \quad (\alpha^\sigma)_{\psi,n}=\psi(\sigma)\alpha_{\psi,n}.$$

Démonstration. L'existence d'une base normale dans l'extension $Q^{(f)}/Q$ implique que $Q_p(\bar\chi)\otimes Q^{(f)}$ est isomorphe à $Q_p(\bar\chi)[G_0]$ en tant que $Q_p(\bar\chi)[G_0]$-module. Ainsi $e_\psi\,Q_p(\bar\chi)\otimes Q^{(f)}$ est isomorphe à l'idéal simple de $Q_p(\bar\chi)[G_0]$ engendré par e_ψ. C'est donc un $Q_p(\bar\chi)$-espace vectoriel de dimension 1. Comme $e_\psi(1\otimes\zeta')$ est non nul (Lemme 5.4) il forme une $Q_p(\bar\chi)$-base de cet espace vectoriel. Ainsi se trouve démontrée l'existence de $\alpha_{\psi,n}$. En transformant la relation définissant $\alpha_{\psi,n}$ par l'élément τ de $H_{\bar\chi}$, on obtient:

$$e_{\tau\circ\psi}\big(1\otimes L_n(\alpha)\big)=(\alpha_{\psi,n})^\tau e_{\tau\circ\psi}(1\otimes\zeta').$$

En multipliant la même relation par $\psi(\sigma)$, on obtient:

$$e_\psi\big(1\otimes L_n(\alpha^\sigma)\big)=\psi(\sigma)\alpha_{\psi,n}e_\psi(1\otimes\zeta').$$

Ceci démontre les deux relations annoncées.

Revenons maintenant à la démonstration de la proposition 5.2. Il reste à justifier le point (ii). Nous désignons par n la p-valuation de $B_{\bar\chi^{-1}}$. Soit σ un élément de G. Le calcul effectué au début de la démonstration à l'aide du lemme 5.3 est repris. Nous avons donc:

$$\binom{0^{\mu_\phi}}{\alpha^\sigma}=\binom{\pi_n'^{\mu_\phi}}{\alpha^\sigma}=\zeta_n^a,$$

avec

$$a=\frac{\varphi(f)}{f}\sum_{\psi|\bar\phi}\big(1-p\psi_0^{-1}(p)\big)B_{\psi^{-1}}e_{\psi^{-1}}(1\otimes\zeta')e_\psi\big(1\otimes L_n(\alpha^\sigma)\big).$$

Les lemmes démontrés ci-dessus vont permettre d'exprimer l'exposant de ζ_n comme une trace dans $Q_p(\bar\chi)/Q_p$. Distinguons plusieurs cas:

Supposons d'abord que le conducteur de $\bar\chi$ soit divisible par p. Dans ce cas $\psi_0^{-1}(p)=0$ et on déduit des lemmes 5.4 et 5.6 l'égalité:

$$\binom{\pi_n'^{\mu_\phi}}{\alpha^\sigma}=\zeta_n^s,$$

avec

$$s=-\frac{1}{\varphi(f)}\sum_{\psi|\bar\phi}B_{\psi^{-1}}\psi(\sigma)\alpha_{\psi,n}.$$

La $\bar\phi$-composante de K_π/K_{π^p} contient αK_{π^p}. Soit $\mu_{\bar\phi}$ un élément de $\mathbf{Z}[G]$ tel que $\mu_{\bar\phi}\equiv e_{\bar\phi} \bmod (p)$. Comme le rapport $\alpha^{\mu_{\bar\phi}}/\alpha$ appartient à K_{π^p}, nous avons, pour tout $\mathfrak{P}$, $\mu_{\bar\phi}\log_{\mathfrak{P}}\alpha\equiv\log_{\mathfrak{P}}\alpha \bmod (\mathfrak{P}^p)$. On en déduit (lemme 4.1 ii)

$$\mu_{\bar\phi}L_n(\alpha)\equiv L_n(\alpha) \bmod (\pi^p) \quad \text{et} \quad e_{\bar\phi}\big(1\otimes L_n(\alpha)\big)\equiv 1\otimes L_n(\alpha) \bmod (1\otimes\pi^p).$$

Par hypothèse α n'appartient pas K_{π^p}. Pour transporter cette propriété à $L_n(\alpha)$ distinguons deux cas: supposons d'abord que le conducteur de χ soit (comme le conducteur de $\bar\chi$) divisible par p. On déduit alors de la proposition 3.3 que α appartient à K_{π^2}. Un calcul simple démontre la congruence

$$L_n(\alpha)\equiv-\sum_{1\leqslant k\leqslant p-1}(1-\alpha)^k/k \bmod (\pi^{p+1})$$

et on obtient $L_n(\alpha) \not\equiv 0 \bmod(\pi^p)$. Dans l'anneau $Z_p[\bar{\chi}] \otimes A^{(f)}$ cela se traduit par $1 \otimes L_n(\alpha) \not\equiv 0 \bmod(1 \otimes \pi^p)$. Nous avons donc $e_{\bar{\phi}}(1 \otimes L_n(\alpha)) \not\equiv 0 \bmod(1 \otimes \pi^p)$. On en déduit l'existence d'un caractère ψ Q_p-équivalent à $\bar{\chi}$ et tel que $e_\psi(1 \otimes L_n(\alpha)) \not\equiv 0 \bmod(1 \otimes \pi^p)$. Utilisons les lemmes 5.5 et 5.6. Nous obtenons $\varphi(f)^{-1}\alpha_{\psi,n} \not\equiv 0 \bmod(p)$. En d'autres termes: la quantité $\varphi(f)^{-1}p^{-n-1}B_{\psi^{-1}}\alpha_{\psi,n}$ n'appartient pas à $Z_p[\bar{\chi}]$. Mais l'extension $Q_p(\bar{\chi})/Q_p$ n'est pas ramifiée et sa codifférente est 1. Ainsi l'idéal

$$\varphi(f)^{-1}p^{-n-1}\operatorname{Tr}_{Q_p(\bar{\chi})/Q_p}(B_{\psi^{-1}}\alpha_{\psi,n}Z_p[\bar{\chi}])$$

n'est pas inclus dans Z_p. Mais l'ensemble des $\psi(\sigma)$, lorsque σ parcourt G, est un système de générateurs de $Z_p[\bar{\chi}]$ considéré comme Z_p-module. Il existe donc un σ dans G tel que

$$\varphi(f)^{-1}p^{-n-1}\operatorname{Tr}_{Q_p(\bar{\chi})/Q_p}(B_{\psi^{-1}}\psi(\sigma)\alpha_{\psi,n})$$

n'appartienne pas à Z_p. Cette trace est égale à la somme

$$\sum_{\tau \in H_{\bar{\chi}}} \tau(B_{\psi^{-1}})(\tau \circ \psi)(\sigma)\tau(\alpha_{\psi,n}).$$

Mais nous avons $\tau(B_{\psi^{-1}}) = B_{\tau\psi^{-1}}$ et en vertu du lemme 5.6, nous pouvons écrire cette somme $\sum_{\tau \in H_{\bar{\chi}}} B_{\tau\psi^{-1}}(\tau \circ \psi)(\sigma)\alpha_{\tau\circ\psi,n}$. On reconnaît la somme qui intervient dans la formule donnant le symbole $\binom{\pi'^{\mu_\phi}_n}{\alpha^\sigma}$. Nous avons donc démontré, dans le cas où les conducteurs de χ et $\bar{\chi}$ sont divisibles par p, que le symbole $\binom{\theta^{\mu_\phi}}{\alpha^\sigma}$ est différent de 1.

Nous supposons maintenant que le conducteur de χ est premier à p. Dans ce cas, les propositions 3.2 et 3.3 montrent que la $\bar{\phi}$-composante de K_{π^2}/K_{π^p} est réduite $\{1\}$. On déduit de l'hypothèse: α n'appartient pas à K_{π^p} et de la condition: αK_{π^p} appartient à $(K_\pi/K_{\pi^p})_{\bar{\phi}}$, que α n'appartient pas à K_{π^2}. Un calcul élémentaire montre que l'on a maintenant la congruence $L_n(\alpha) \equiv \alpha - 1 + (\alpha-1)^p/p \bmod(\pi^2)$. Pour montrer que $L_n(\alpha)$ n'est pas congru à 0 modulo π^2, raisonnons par l'absurde: supposons donc un instant $L_n(\alpha) \equiv 0 \bmod(\pi^2)$. Nous aurions alors $\alpha - 1 + (\alpha-1)^p/p \equiv 0 \bmod(\pi^2)$. Cela équivaut à $1 + (\alpha-1)^{p-1}/p \equiv 0 \bmod(\pi)$. Comme on a la congruence $\pi^{p-1}/p \equiv -1 \bmod(\pi)$, nous aurions $1 \equiv ((\alpha-1)/\pi)^{p-1} \bmod(\pi)$. Soit $\mathfrak{p}$ un idéal de K au-dessus de p. La congruence $1 \equiv ((\alpha-1)/\pi)^{p-1} \bmod(\mathfrak{p})$ implique l'existence d'un élément x de Z tel que $(\alpha-1)/\pi \equiv x \bmod(\mathfrak{p})$. Nous aurions alors $\alpha \equiv 1 + x\pi \bmod(\mathfrak{p}^2)$. Notons D le groupe de décomposition de $\mathfrak{p}$ dans K. Soit σ un élément de D. Nous aurions aussi

$$\alpha^\sigma \equiv 1 + x\pi^\sigma \equiv (1 + x\pi)^{\omega(\sigma)} \bmod(\mathfrak{p}^2).$$

D'où la relation $\alpha^\sigma \equiv \alpha^{\omega(\sigma)} \bmod(\mathfrak{p}^2)$. Dans le G-module K_π/K_{π^2} cela se traduit par $(\alpha K_{\pi^2})^\sigma = (\alpha K_{\pi^2})^{\omega(\sigma)}$. D'autre part, nous avons aussi $(\alpha K_{\pi^2}) = (\alpha K_{\pi^2})^{e_{\bar{\phi}}}$. Désignons par R un système de représentants de G modulo D. Nous pouvons écrire $e_{\bar{\phi}}$ sous la forme:

$$e_{\bar{\phi}} = \frac{1}{|G|}\sum_{\sigma \in G}\bar{\phi}(\sigma^{-1})\sigma = \frac{1}{|G|}\sum_{\tau \in R}\sum_{\sigma \in D}\bar{\phi}(\sigma^{-1}\tau^{-1})\tau\sigma.$$

Nous obtenons alors:

$$(\alpha K_{\pi^2}) = (\alpha K_{\pi^2})^a,$$

avec

$$a = \frac{1}{|G|}\sum_{\tau \in R}\sum_{\sigma \in D}\bar{\phi}(\sigma^{-1}\tau^{-1})\omega(\sigma)\tau.$$

Montrons que la somme $\sum_{\sigma \in D}\bar{\phi}(\sigma^{-1}\tau^{-1})\omega(\sigma)$ est nulle. Cela revient à démontrer la même relation en remplaçant $\bar{\phi}$ par ψ, caractère Q_p-équivalent à $\bar{\chi}$. Un tel caractère est de la forme $\bar{\chi}^{p^\mu}$. Calculons:

$$\sum_{\sigma \in D}\bar{\chi}(\sigma^{-1})^{p^\mu}\omega(\sigma) = \sum_{\sigma \in D}(\bar{\chi}(\sigma^{-1})\omega(\sigma))^{p^\mu} = \sum_{\sigma \in D}\chi(\sigma)^{p^\mu} = \sum_{\sigma \in D}\chi(\sigma).$$

En vertu de l'hypothèse B, cette dernière somme est nulle. Nous démontrons ainsi que α appartient à K_{π^2}. C'est la contradiction cherchée. Nous avons donc $L_n(\alpha) \not\equiv 0 \bmod(\pi^2)$ et a fortiori $L_n(\alpha) \not\equiv 0 \bmod(\pi^p)$. Le reste de la démonstration est la même que dans le cas précédent.

Il reste à décrire le cas où le conducteur de $\bar{\chi}$ serait premier à p. On déduit des lemmes 5.4 et 5.6 la formule:

$$\binom{\pi'^{\mu_\phi}}{\alpha^\sigma} = \zeta_n^t,$$

avec

$$t = -\frac{1}{p\varphi(f)}\sum_{\psi|\bar{\phi}}(1 - p\psi_0^{-1}(p))B_{\psi^{-1}}\psi(\sigma)\alpha_{\psi,n}.$$

Le conducteur de χ est divisible par p. Le début de la démonstration est le même: Les hypothèses faites sur α impliquent toujours les congruences: $\alpha \not\equiv 1 \bmod(\pi^2)$ et $e_{\bar{\phi}}(1 \otimes L_n(\alpha)) \not\equiv 0 \bmod(1 \otimes \pi^p)$. Il existe un caractère ψ Q_p-équivalent à $\bar{\chi}$ et tel que $e_\psi(1 \otimes L_n(\alpha)) \not\equiv 0 \bmod(1 \otimes \pi^p)$. Maintenant la quantité $\alpha_{\psi,n}$ vérifie la relation $\varphi(f)^{-1}\alpha_{\psi,n} \not\equiv 0 \bmod(p^2)$. Le reste de la démonstration suit le même principe que précédemment.

Fin de la démonstration. Essayons maintenant de justifier le théorème énoncé dans le paragraphe 1. On désigne par n la p-valuation de $B_{\bar{\chi}^{-1}}$. Supposons que $\varkappa_\phi$ soit réduit à $\{1\}$. La proposition 3.6 montre que le $\bar{\phi}$-rang de $\varkappa_{\bar{\phi}}$ est inférieur à 1. En tant que $Z_p[\bar{\chi}]$-module $\varkappa_{\bar{\phi}}$ est donc

isomorphe à un module de la forme $Z_p[\bar{\chi}]/p^m Z_p[\bar{\chi}]$. La proposition 3.1 montre l'inégalité $n \geqslant m$. En vertu de la remarque qui suit cette proposition nous avons donc obtenu l'inégalité:

$$|\varkappa_{\bar{\phi}}| \leqslant \Big(\prod_{\psi|\bar{\phi}} B_{\psi^{-1}}\Big)_p.$$

Remarquons que cette partie de la démonstration n'utilise que les résultats rappelés dans le paragraphe 3. Ces arguments avaient été mis en évidence en [4].

Supposons maintenant que $(E_\chi/F_\chi)_\phi$ soit réduit à $\{1\}$. La proposition 5.1 montre que θ^{μ_ϕ} n'appartient pas K^p. L'extension $K\big(\sqrt[p]{\theta^{\mu_\phi}}\big)/K$ a donc pour degré p. Il existe un idéal de K non ramifié et non décomposé dans cette extension. En d'autres termes, il existe un idéal $\mathfrak{a}$ appartenant à I et tel que le symbole $\left(\dfrac{\theta^{\mu_\phi}}{\mathfrak{a}}\right)$ soit différent de 1. En vertu des propriétés de ce symbole rappelées dans le paragraphe 4, on peut remplacer $\mathfrak{a}$ par un élément de $(\mathfrak{a}P_{p+1})^{e_{\bar{\phi}}}$ sans en changer la valeur. Notons encore $\mathfrak{a}$ cet idéal. La proposition 3.1 montre que $\mathfrak{a}^{p^n}$ appartient à P_1. Il existe un élément α de K_π qui engendre $\mathfrak{a}^{p^n}$. Compte tenu de la proposition 3.4 on peut supposer que αK_{π^p} appartient à la $\bar{\phi}$-composante de K_π/K_{π^p}. On déduit alors de la proposition 5.2 (i) que α n'appartient pas à K_{π^p}. Ceci montre que $\mathfrak{a}^{p^{n-1}}$ n'appartient pas à P_1: en effet, si cela était, $\mathfrak{a}^{p^n}$ appartiendrait à P_p et α appartiendrait à K_{π^p} (Proposition 3.4). Ainsi l'ordre de la classe de l'idéal $\mathfrak{a}$ dans I/P_1, isomorphe à $\varkappa$, est p^n et nous avons, en supposant $(E_\chi/F_\chi)_\phi$ réduit à $\{1\}$, démontré l'inégalité:

$$|\varkappa_{\bar{\phi}}| \geqslant \Big(\prod_{\psi|\bar{\phi}} B_{\psi^{-1}}\Big)_p.$$

Pour démontrer le point (ii) du théorème, supposons d'abord que l'on ait les égalités

$$|\varkappa_{\bar{\phi}}| = \Big(\prod_{\psi|\bar{\phi}} B_{\psi^{-1}}\Big)_p \quad \text{et} \quad |\varkappa_\phi| = 1.$$

La seconde hypothèse et la proposition 3.7 montrent que le $\bar{\phi}$-rang de $(I/P_p)_{\bar{\phi}}$ est 1. Désignons toujours par d le degré de $Q_p(\bar{\chi})/Q_p$. La première hypothèse montre que le groupe $(I/P_1)_{\bar{\phi}}$ est d'ordre p^{nd}. A l'aide de la proposition 3.4, on en déduit que l'ordre de $(I/P_p)_{\bar{\phi}}$ est $p^{(n+1)d}$. Ainsi la structure de $(I/P_p)_\phi$ en tant que $Z_p[\bar{\chi}]$-module est déterminée: ce module est isomorphe à $Z_p[\bar{\chi}]/p^{n+1}Z_p[\bar{\chi}]$. Il existe donc un idéal $\mathfrak{a}$, appartenant à I, tel que $\mathfrak{a}P_{p+1}$ appartienne à $(I/P_{p+1})_{\bar{\phi}}$ et tel que $\mathfrak{a}P_p$ soit un élément de $(I/P_p)_{\bar{\phi}}$ d'ordre p^{n+1}. En vertu des propositions 3.1 et 3.4 il existe un élément α de K_π qui engendre $\mathfrak{a}^{p^n}$ et tel que αK_{π^p} appartienne à $(K_\pi/K_{\pi^p})_{\bar{\phi}}$. Comme $\mathfrak{a}^{p^n}$ n'appartient pas à P_p, α n'appartient pas à K_{π^p} et la proposition 5.2 (ii) montre qu'il existe un σ dans G tel que le symbole $\left(\dfrac{\theta^{\mu_\phi}}{\mathfrak{a}^\sigma}\right)$ soit différent de 1. En conséquence θ^{μ_ϕ} n'appartient pas à K^p et la proposition 5.1 montre que $(E_\chi/F_\chi)_\phi$ est réduit à $\{1\}$.

Supposons maintenant que l'on ait les égalités

$$|\varkappa_{\bar{\phi}}| = \Big(\prod_{\psi|\bar{\phi}} B_{\psi^{-1}}\Big)_p \quad \text{et} \quad (E_\chi/F_\chi)_\phi = \{1\}.$$

Comme précédemment on déduit de la proposition 5.1 l'existence d'un idéal $\mathfrak{a}$ appartenant à I, tel que $\mathfrak{a}P_{p+1}$ appartienne à $(I/P_{p+1})_{\bar{\phi}}$ et tel que $\left(\dfrac{\theta^{\mu_\phi}}{\mathfrak{a}}\right)$ soit différent de 1. Les propositions 3.1 et 3.4 montrent qu'il existe α dans K_π tel que $\mathfrak{a}^{p^n}$ soit l'idéal engendré par α et tel que αK_{π^p} appartienne à $(K_\pi/K_{\pi^p})_{\bar{\phi}}$. En vertu de la proposition 5.2 (i), le nombre α n'appartient pas à K_{π^p}. Ainsi $\mathfrak{a}^{p^n}$ n'appartient pas à P_p et l'ordre de $\mathfrak{a}P_p$ dans I/P_p est p^{n+1}. D'autre part la première hypothèse précise l'ordre de $(I/P_1)_{\bar{\phi}}$, à savoir p^{nd}. L'ordre de $(I/P_p)_{\bar{\phi}}$ est donc $p^{(n+1)d}$. En conséquence le $\bar{\phi}$-rang de $(I/P_p)_{\bar{\phi}}$ est égal à 1. On déduit alors de la proposition 3.7 l'égalité $\varkappa_\phi = \{1\}$.

Bibliographie

[1] E. Artin und H. Hasse, *Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln*, Abh. Math. Sem. Univ. Hamburg 6 (1928), p. 146–162.

[2] R. F. Coleman, *The dilogarithm and the norm residue symbol*, Bull. Soc. Math. France 109 (1981), p. 373–402.

[3] R. Gillard, *Relations de Stickelberger*, Séminaire de théorie des nombres, Grenoble 1974.

[4] G. Gras, *Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés*, Ann. Inst. Fourier 27 (1977), p. 1–66.

[5] – *Application de la notion de φ-objet à l'étude du groupe des classes d'idéaux des extensions abéliennes*, Publ. Math. Fac. Sci. Besançon (1975–1976).

[6] H. Hasse, *Zum expliziten Reziprozitätsgesetz*, Abh. Math. Sem. Univ. Hamburg 6 (1929), p. 52–63.

[7] – *Über die Klassenzahl abelscher Zahlkörper*, Berlin 1952.

[8] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Akad. Verlag, Leipzig 1923.

[9] K. Iwasawa, *On explicit formulas for the norm residue symbol*, J. Math. Soc. Japan 20 (1–2) (1968), p. 151–165.

[10] – *A note on cyclotomic fields*, Invent. Math. 36 (1976), p. 115–123.

[11] S. Lang, *Units and class groups in number theory and algebraic geometry*, Bull. Amer. Math. Soc. 6 (1982), p. 253–316.

[12] H. W. Leopoldt, *Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, Abh. Deutsche Akad. Wiss. Berlin Math. 2 (1954), 48 pag.

[13] – *Zur Struktur der l-Klassengruppe galoischer Zahlkörper*, Journ. Reine Angew. Math. 199 (1958), p. 165–174.

[14] B. Oriat, *Sur l'article de H. W. Leopoldt intitulé: "Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper"*, Publ. Math. Fac. Sci. Besançon (1974–1975).
[15] — *Un calcul explicite*, à paraître Publ. Math. Fac. Sci. Besançon.
[16] L. Stickelberger, *Über eine Verallgemeinerung der Kreisteilung*, Math. Ann. 37 (1890), p. 321–387.
[17] A. Wiles, *Modular curves and the class group of* $Q(\zeta_p)$, Invent. Math. 58 (1980), p. 1–35.

E.R.A. C.N.R.S. 070654
MATHÉMATIQUES
FACULTÉ DES SCIENCES
F 25030 BESANÇON CEDEX

Reçu le 6.3.1984 (1410)

ACTA ARITHMETICA
XLVI (1986)

On primitive divisors of Mersenne numbers

by

CARL POMERANCE* (Athens, Ga.)

An interesting source of problems in number theory is to study the restriction of a familiar function to a special set of integers. For example, it is common in the literature to see papers which study the various divisor functions at polynomials evaluated at natural numbers or at primes. In his interesting paper [2], Erdös considered the divisor function

$$\sigma_{-1}(m) = \sum_{d|m} 1/d$$

restricted to Mersenne numbers; that is, numbers m of the form 2^n-1.

It is well known that

$$\sigma_{-1}(m) = O(\log\log m).$$

Thus letting $m = 2^n-1$, we trivially have

$$\sigma_{-1}(2^n-1) = O(\log n).$$

What Erdös proved in [2] is the surprisingly difficult result that the $\log n$ can be replaced with $\log\log n$:

$$\sigma_{-1}(2^n-1) = O(\log\log n).$$

It is not so hard to see that this result is best possible.

For d an odd natural number, let $l(d)$ denote the exponent to which 2 belongs modulo d. That is,

$$2^{l(d)} \equiv 1 \bmod d \quad \text{and} \quad 2^l \not\equiv 1 \bmod d \quad \text{for all } l,\ 1 \leqslant l < l(d).$$

Let

$$E(n) = \sum_{l(d)=n} 1/d.$$

* Research supported in part by an NSF grant.