

SUR LES INVARIANTS " LAMBDA " D'IWASAWA
DES CORPS ABELIENS

SUR LES INVARIANTS "LAMBDA" D'IWASAWA

DES CORPS ABELIENS

par Georges GRAS

(Besançon, E. R. A. au C. N. R. S. n°070654)

Cet article est un complément destiné, principalement, à la démonstration détaillée d'un résultat, que nous avons seulement cité dans [4] (th. 5.1) concernant des invariants du type invariants "lambda" d'Iwasawa, et aussi, à celle de formules de translation sur ces invariants (cf. [4], § 5), qui résultent de la théorie des fonctions L p-adiques ([10], [3]), formules qui ont été données indépendamment par Kida ([6], [7]), à partir de la théorie des genres.

Pour la commodité du lecteur, nous redonnons les définitions essentielles et réexpliquons les principaux arguments.

Dans la suite p est un nombre premier fixé.

Soit K un corps abélien sur \mathbb{Q} ; si K est réel, nous convenons d'associer à K le groupe fini $\mathcal{C}(K)$ qui est le \mathbb{Z}_p -module de torsion de la p-extension abélienne p-ramifiée maximale de K (cf. [4], § 1) ; si K est imaginaire, nous convenons d'associer à K le groupe $\mathcal{K}(K)$ des p-classes d'idéaux ordinaires relatives de K.

Rappelons les notations déjà utilisées dans [3] et [4] : on pose $q = p$ (resp. $q = 4$) si $p \neq 2$ (resp. $p = 2$), et on considère le caractère de Teichmüller θ défini comme l'unique caractère de Dirichlet modulo q tel que $a\theta^{-1}(a) \equiv 1 \pmod{q}$, pour tout a premier à p. On désigne par

$\mathbb{Q}_\infty = \bigcup_{n \geq 0} \mathbb{Q}_n$ ($[\mathbb{Q}_n : \mathbb{Q}] = p^n$) la \mathbb{Z}_p -extension cyclotomique de \mathbb{Q} , par

$K_\infty = \bigcup_{n \geq 0} K_n$ ($K_n = K\mathbb{Q}_n$) celle de K, et par $(\gamma_n)_{n \geq 0}$ une famille de

caractères de \mathbb{Q}_∞ , où γ_n est d'ordre p^n et où $\gamma_{n+1}^p = \gamma_n$. Soit ψ un caractère abélien de degré 1 ; on écrit $\psi = \psi_p \psi_o$ (ψ_p d'ordre puissance de p , ψ_o d'ordre premier à p). De façon générale, on appelle K_ψ le corps fixe par le noyau de ψ , on appelle f_ψ le conducteur de ψ , et on désigne par $\mathbb{Z}_p(\psi)$ l'anneau des valeurs de ψ sur \mathbb{Z}_p . Si un corps abélien K est donné, on appelle Ψ_K (resp. Ψ_K^+ , Ψ_K^-) l'ensemble des caractères (resp. des caractères pairs, impairs) de K . On désigne par μ_K le p -groupe des racines de l'unité contenues dans K (si d est un entier positif, μ_d est le groupe des racines d^e de l'unité). Enfin on écrit $\alpha \approx \beta$ pour dire que α/β est une unité p -adique.

1. Définitions et propriétés des invariants $\Lambda(K), \bar{\Lambda}(K)$.

Rappel des formules analytiques.

On a, pour un corps abélien quelconque K , des formules analytiques p -adiques pour exprimer $|\mathcal{G}(K)|$ (resp. $|\mathcal{H}(K)|$) lorsque K est réel (resp. imaginaire) qui reposent sur les formules analytiques p -adiques du nombre de classes :

$$(1.1) \quad |\mathcal{G}(K)| \approx p^{n_o(K)} \prod_{\alpha \neq 1} \frac{1}{2} L_p(1, \alpha), \quad \alpha \text{ parcourant l'ensemble des}$$

caractères de Dirichlet primitifs pairs $\neq 1$ de K , et où

$$p^{n_o(K)} = [K \cap \mathbb{Q}_\infty : \mathbb{Q}] \text{ (cf. [1], Appendix I, lemme 8 ; voir aussi [4], th. 2. 1).}$$

$$(1.2) \quad |\mathcal{H}(K)| \approx p^{m_o(K)} \prod_{\beta} -\frac{1}{2} B_1(\beta^{-1}), \quad \text{où } \beta \text{ parcourt l'ensemble des}$$

caractères de Dirichlet primitifs impairs de K , et où $p^{m_o(K)}$ est la p -participation de $Q(K)W(K)$ ($Q(K) = 1$ ou 2 est l'indice des unités, $W(K)$ est l'ordre de μ_K) (cf. [5], I, § 5).

Dans le second cas (K imaginaire), le nombre de Bernoulli $B_1(\beta^{-1})$ est considéré comme primitif, or on a les formules bien connues (où θ^o est le caractère de Dirichlet unité modulo q) :

$$-\frac{1}{2} B_1(\theta^0 \beta^{-1}) = \frac{1}{2} L_p(0, \theta \beta^{-1}) \text{ et } \frac{1}{2} B_1(\theta^0 \beta^{-1}) = (1 - \beta^{-1}(p)) \frac{1}{2} B_1(\beta^{-1}).$$

On a donc la possibilité d'exprimer $\frac{1}{2} B_1(\beta^{-1})$ à l'aide de la valeur en 0 d'une fonction L_p , uniquement lorsque $\beta(p) \neq 1$; dans ce cas on a :

$$-\frac{1}{2} B_1(\beta^{-1}) = (1 - \beta^{-1}(p))^{-1} \frac{1}{2} L_p(0, \theta \beta^{-1}); \text{ en conséquence on a :}$$

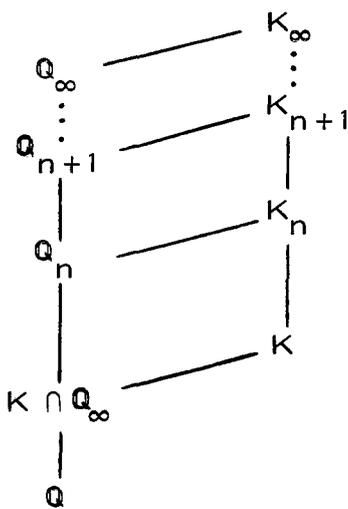
$$(1.3) \quad -\frac{1}{2} B_1(\beta^{-1}) = \frac{1}{2} L_p(0, \theta \beta^{-1}) \text{ si } p \text{ divise le conducteur du caractère primitif impair } \beta.$$

Rappels sur les invariants $\lambda(\psi)$ (cf. [3], prop. V 2).

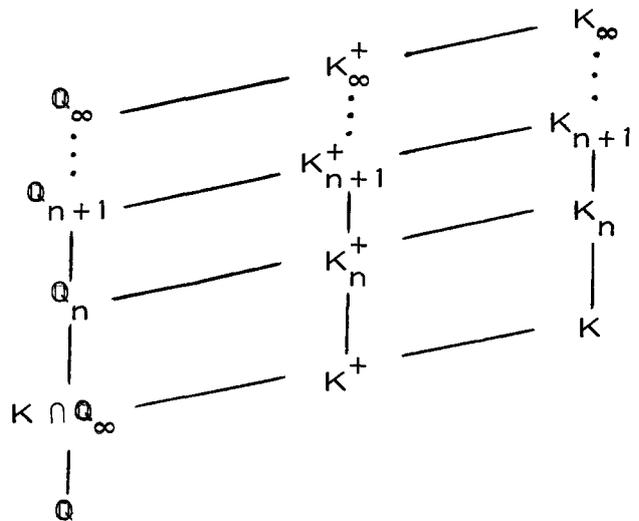
Soit ψ un caractère pair ; considérons les caractères $\gamma_n \psi$, pour tout $n \geq 0$; dans ce cas on sait que la valuation de $\frac{1}{2} L_p(s, \gamma_n \psi)$ (calculée dans $\mathbb{Z}_p(\gamma_n \psi)$) est, pour n assez grand, une constante $\lambda(\psi)$ qui ne dépend que de ψ , et non du choix des γ_n ou de $s \in \mathbb{Z}_p$ (ceci repose sur le résultat fondamental de Ferrero-Washington).

Formules d'Iwasawa.

Considérons les schémas suivants :



cas réel



cas imaginaire

On peut, dans la \mathbb{Z}_p -extension cyclotomique du corps K , écrire les formules "relatives" suivantes (pour n assez grand) en termes de fonctions L p -adiques (cf. 1.1, et 1.2 associée à 1.3) :

(i) K est réel (cf. [4], prop. 4.1).

$$\text{On a } \frac{|\zeta(K_{n+1})|}{|\zeta(K_n)|} \approx p^{n_o(K_{n+1}) - n_o(K_n)} \prod_{\alpha_{n+1}} \frac{1}{2} L_p(1, \alpha_{n+1}), \text{ où}$$

α_{n+1} parcourt l'ensemble des caractères de K_{n+1} qui ne sont pas caractères de K_n . On a $n_o(K_{n+1}) = p^{n+1}$ et $n_o(K_n) = p^n$; ensuite on voit que

α_{n+1} est de la forme $\gamma_{n+1}^a \psi$, $a \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^*$, ψ parcourant un système exact de représentants de $\Psi_K / \Psi_K \cap \mathbb{Q}_\infty$, noté $\tilde{\Psi}_K$. On obtient alors

$$\frac{|\zeta(K_{n+1})|}{|\zeta(K_n)|} \approx p \prod_{a, \psi} \frac{1}{2} L_p(1, \gamma_n^a \psi), \quad a \in (\mathbb{Z}/p^n\mathbb{Z})^*, \quad \psi \in \tilde{\Psi}_K, \text{ d'où, si l'on}$$

pose $\frac{|\zeta(K_{n+1})|}{|\zeta(K_n)|} = p^{\Lambda_n(K)}$, pour n assez grand $\Lambda_n(K) = \Lambda(K)$ est indépendant

de n (et du choix des γ_n) et on a :

$$(1.4) \quad \Lambda(K) = 1 + \sum_{\psi \in \tilde{\Psi}_K} \lambda(\psi),$$

ce qui donne une démonstration analytique de la formule d'Iwasawa, pour la famille ζ dans K_∞ :

$$(1.5) \quad |\zeta(K_n)| = p^{\Lambda(K)n + c} \text{ pour tout } n \text{ assez grand, } c \text{ constante.}$$

(ii) K est imaginaire.

On introduit les sous-corps réels maximaux K_n^+ des corps K_n .

$$\text{On a } \frac{|\mathcal{K}(K_{n+1})|}{|\mathcal{K}(K_n)|} \approx p^{m_o(K_{n+1}) - m_o(K_n)} \prod_{\beta_{n+1}} \frac{1}{2} B_1(\beta_{n+1}^{-1}),$$

où β_{n+1} parcourt l'ensemble des caractères impairs de K_{n+1} qui ne sont pas caractères de K_n .

Etudions la différence $m_o(K_{n+1}) - m_o(K_n)$:

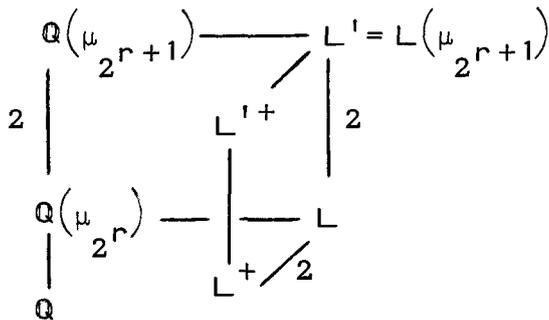
Il y a deux cas : ou bien $\mu_q \subset K_\infty$, ou bien $\mu_q \not\subset K_\infty$. Dans le premier cas, K_∞ contient $\bigcup_{n \geq 0} \mathbb{Q}(\mu_{qp^n})$, dans le second cas, K_∞ ne contient pas de racines de l'unité d'ordre une puissance de p autres que 1 (resp. ± 1) dans le cas $p \neq 2$ (resp. $p = 2$).

Dans le premier cas, on remarque que pour n assez grand on a $\mu_q \subset K_n$, donc en fait $\mu_{qp^n} \subset K_n$, $\mu_{qp^{n+1}} \not\subset K_n$, d'où : $W(K_{n+1}) = qp^{n+1}$, $W(K_n) = qp^n$.

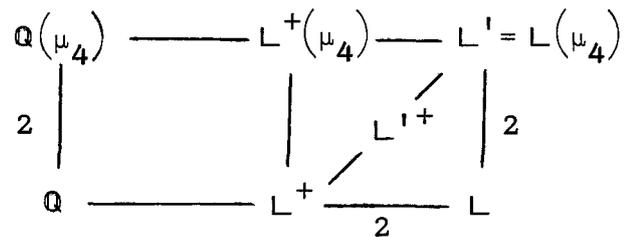
Dans le second cas, on a $W(K_{n+1}) = W(K_n)$ pour tout n assez grand.

Il nous reste à voir le comportement de l'indice des unités de K_n à K_{n+1} (uniquement lorsque $p = 2$). On utilise pour cela le critère donné par Hasse ([5], III, § 22, Satz 15) :

Soit L une extension abélienne imaginaire de \mathbb{Q} ; on suppose $\mu_{2^r} \subset L$, $\mu_{2^{r+1}} \not\subset L$; on pose $L' = L(\mu_{2^{r+1}})$ et on appelle L'^+ et L^+ les sous-corps réels maximaux de L' et L (Ceci est résumé par les schémas ci-après) :



cas $r \geq 2$



cas $r = 1$

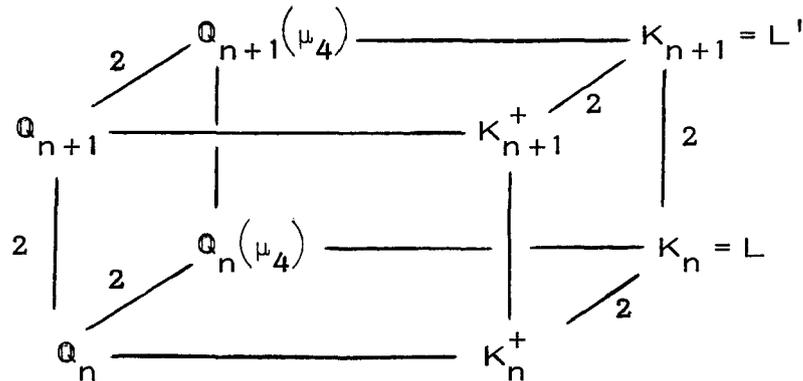
On a alors $Q(L) = 2$ si et seulement si l'extension de Kummer L'^+/L^+ est de type unité (i. e. s'il existe une unité $\epsilon \in L^+$ telle que $L'^+ = L^+(\sqrt{\epsilon})$).

Appliquons ceci au cas où $L = K_n$ ou K_{n+1} .

α) Cas où $\mu_4 \subset K_\infty$.

On a le schéma suivant (compte tenu du fait qu'ici, pour n assez grand, $L = K_n$ contient $\mu_{4 \cdot 2^n}$ et non $\mu_{4 \cdot 2^{n+1}}$, et que

$$L' = L(\mu_{4 \cdot 2^{n+1}}) = K_{n+1} :$$



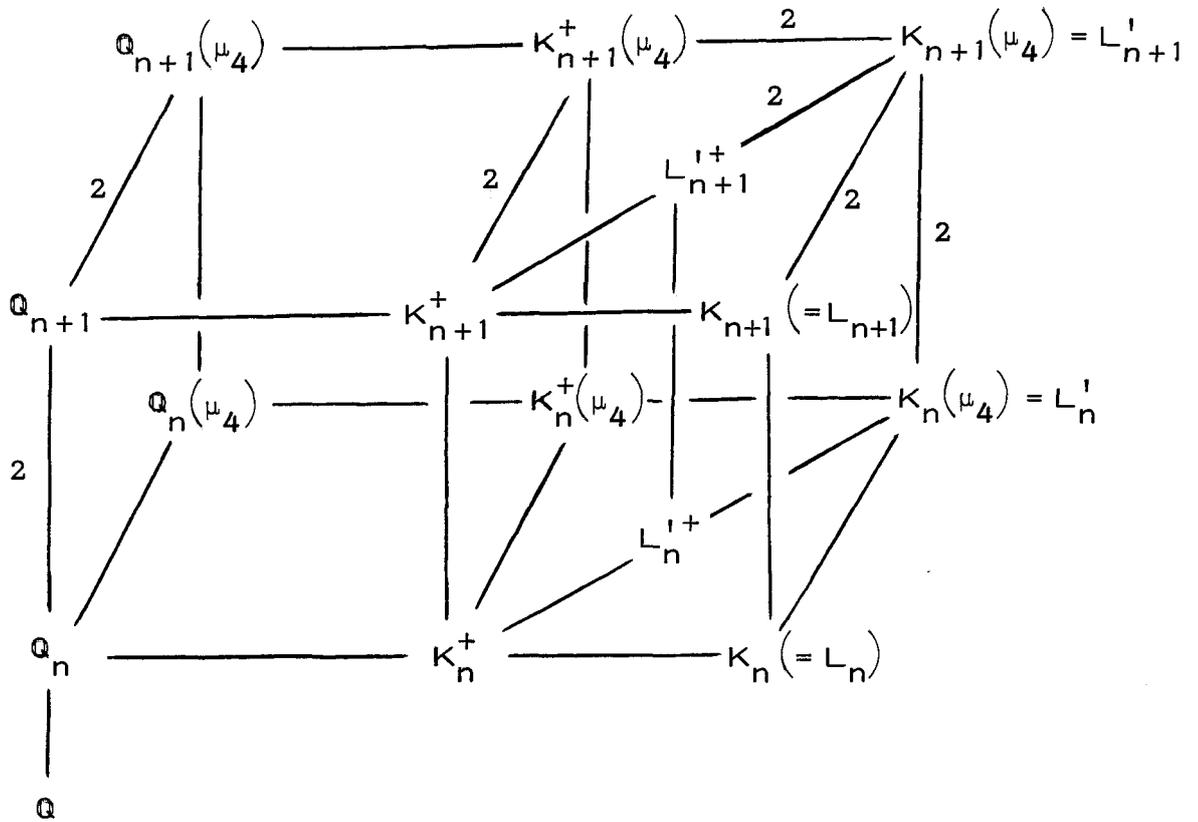
Il est bien connu que $Q_{n+1} = Q_n(\sqrt{\pi_n})$, où π_n engendre l'idéal premier \mathfrak{p}_n au-dessus de 2 dans Q_n ; on a donc $K_{n+1}^+ = K_n^+(\sqrt{\pi_n})$. Comme pour n assez grand 2 est ramifié dans K_{n+1}^+/K_n^+ , et non ramifié dans $K_n/Q_n(\mu_4)$, il en résulte que l'indice de ramification de 2 dans K_n^+/Q_n est 1 ou 2 et est constant pour n assez grand. On a $K_n^+(\sqrt{\pi_n}) = K_n^+(\sqrt{\epsilon_n})$, ϵ_n unité de K_n^+ , si et seulement si $\pi_n = \epsilon_n u_n^2$, $u_n \in K_n^+$, autrement dit on a $Q(K_n) = 2$ si et seulement si l'idéal (π_n) de K_n^+ est le carré d'un idéal principal de K_n^+ (ce qui implique 2 ramifié dans K_n^+/Q_n ; si pour un entier n_1 , 2 est non ramifié dans $K_{n_1}^+/Q_{n_1}$, cette propriété se conserve pour tout $n \geq n_1$, et pour tout n assez grand, $Q(K_n) = 1$).

Montrons que $Q(K_n) = 1$ entraîne $Q(K_{n+1}) = 1$ (pour n assez grand et en supposant K_n^+/Q_n ramifiée en 2). En effet, $Q(K_n) = 1$ équivaut à $(\pi_n) = q_n^2$ dans K_n^+ , q_n idéal non principal de K_n^+ ; si on suppose $Q(K_{n+1}) = 2$, on a dans K_{n+1}^+ : $(\pi_{n+1}) = q_{n+1}^2$ avec cette fois q_{n+1}

principal, et comme il y a ramification de 2 dans K_{n+1}^+/K_n^+ il en résulte que $N_{K_{n+1}^+/K_n^+} q_{n+1} = q_n$ est principal, ce qui est absurde ; d'où l'assertion. Donc à partir d'un certain rang $Q(K_n)$ est constant.

β) Cas où $\mu_4 \notin K_\infty$.

Dans ce cas on a $\mu_4 \notin K_n$ pour tout n ; on a le schéma suivant :



Le critère de Hasse repose donc sur l'étude des extensions L_n^{1+}/K_n^+ .

Soit $\alpha \in K^+$ tel que $K = K^+(\sqrt{\alpha})$; alors pour tout n on a $K_n = K_n^+(\sqrt{\alpha})$, d'où $L_n^{1+} = K_n^+(\sqrt{-\alpha})$. Si pour un entier n_1 on a $-\alpha = \epsilon_{n_1} u_{n_1}^2$,

ϵ_{n_1} unité de $K_{n_1}^+$, $u_{n_1} \in K_{n_1}^+$, alors L_n^+/K_n^+ est de type unité pour tout $n \geq n_1$, et dans ce cas $Q(K_n) = 2$ pour tout $n \geq n_1$. Il en résulte bien que $Q(K_n)$ est encore constant pour n assez grand.

$$\text{On a donc } \frac{|\mathcal{H}(K_{n+1})|}{|\mathcal{H}(K_n)|} \approx p^{\rho(K)} \prod_{\beta_{n+1}} \frac{1}{2} B_1(\beta_{n+1}^{-1}), \text{ où } \rho(K) = 1 \text{ ou } 0$$

selon que K_∞ contient ou non μ_q , avec β_{n+1} caractère impair de K_{n+1} non caractère de K_n . Un tel caractère est encore de la forme $\gamma_n^a \psi'$, $a \in (\mathbb{Z}/p^n \mathbb{Z})^*$, ψ' parcourant l'ensemble, noté $\tilde{\Psi}_K^-$, des caractères impairs de $\tilde{\Psi}_K$ ($\tilde{\Psi}_K$ désignant comme précédemment un système exact de représentants de $\Psi_K / \Psi_K \cap Q_\infty$); le résultat ne dépend pas du choix de $\tilde{\Psi}_K$ car $\Psi_K \cap Q_\infty$ est constitué de caractères pairs.

Comme β_{n+1} a un conducteur divisible par p , on a d'après 1.3 : $-\frac{1}{2} B_1(\beta_{n+1}^{-1}) = \frac{1}{2} L_p(0, \theta \beta_{n+1}^{-1}) = \frac{1}{2} L_p(0, \gamma_n^{-a} \theta \psi'^{-1})$. Si l'on pose d'une façon générale $\psi = \theta \psi'^{-1}$, ceci définit une involution, notée \mathfrak{m} , de l'ensemble des caractères abéliens impairs dans celui des caractères pairs. Lorsque ψ' parcourt $\tilde{\Psi}_K^-$, ψ parcourt $\mathfrak{m}(\tilde{\Psi}_K^-)$; or un tel ensemble n'est pas, en général, de la forme $\tilde{\Psi}_L$ pour un corps réel L .

$$\text{On a alors } \frac{|\mathcal{H}(K_{n+1})|}{|\mathcal{H}(K_n)|} = p^{\rho(K)} \prod_{b, \psi} \frac{1}{2} L_p(0, \gamma_n^b \psi), \quad b \in (\mathbb{Z}/p^n \mathbb{Z})^*,$$

$$\psi \in \mathfrak{m}(\tilde{\Psi}_K^-), \text{ d'où, en posant } \frac{|\mathcal{H}(K_{n+1})|}{|\mathcal{H}(K_n)|} = p^{\bar{\Lambda}_n(K)}, \text{ pour tout } n \text{ assez grand}$$

$\bar{\Lambda}_n(K) = \bar{\Lambda}(K)$ est indépendant de n , et on a :

$$(1.6) \quad \bar{\Lambda}(K) = \rho(K) + \sum_{\psi} \lambda(\psi), \quad \psi \in \mathfrak{m}(\tilde{\Psi}_K^-), \text{ et où } \rho(K) = 1 \text{ ou } 0 \text{ selon que } K_\infty \text{ contient ou non } \mu_q.$$

Ceci donne une démonstration analytique de la formule d'Iwasawa proprement dite :

$$(1.7) \quad |\mathcal{H}(K_n)| = p^{\bar{\Lambda}(K)n + \bar{c}}, \text{ pour tout } n \text{ assez grand, } \bar{c} \text{ constante.}$$

Un cas particulier.

Supposons $\mu_q \subset K$; alors les groupes $\Psi_K^+ = \Psi_{K^+}$ et Ψ_K^- se correspondent bijectivement par \mathfrak{M} , et il en résulte facilement que l'on peut choisir $\tilde{\Psi}_K^-$ et $\tilde{\Psi}_{K^+}$ de telle sorte que $\mathfrak{M}(\tilde{\Psi}_K^-) = \tilde{\Psi}_{K^+}$; il s'en suit que dans ce cas on a :

$$\Lambda(K^+) = 1 + \sum_{\psi \in \tilde{\Psi}_{K^+}} \lambda(\psi) \quad (\text{d'après 1.4}),$$

$$\bar{\Lambda}(K) = 1 + \sum_{\psi \in \tilde{\Psi}_{K^+}} \lambda(\psi) \quad (\text{d'après 1.6, compte tenu du fait$$

que $\rho(K) = 1$ par hypothèse) ; d'où :

$$(1.8) \quad \text{Si } \mu_q \subset K, \text{ alors } \Lambda(K^+) = \bar{\Lambda}(K).$$

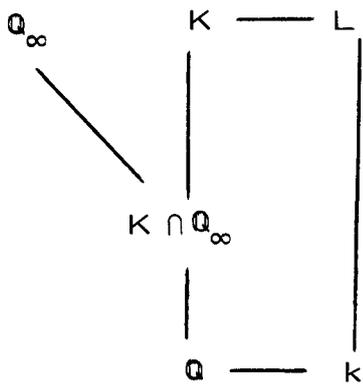
On voit aussi que le cas général est inadéquat pour comparer Λ et $\bar{\Lambda}$; ceci provient du fait que \mathfrak{M} respecte les caractères p -adiques et non les corps. Ceci justifie l'étude que nous allons faire plus loin (§ 3), et qui consiste non plus à utiliser $\Lambda(K)$ (resp. $\bar{\Lambda}(K)$) dans le cas réel (resp. imaginaire) mais des invariants $\Lambda(\emptyset)$ (resp. $\bar{\Lambda}(\emptyset)$), qui sont des termes convenables de $\Lambda(K)$ (resp. $\bar{\Lambda}(K)$), dépendant des caractères p -adiques abéliens pairs (resp. impairs), et non plus des corps.

Auparavant nous allons donner quelques formules sur ces invariants montrant qu'il suffit de les connaître pour les corps K de degré premier à p sur \mathbb{Q} .

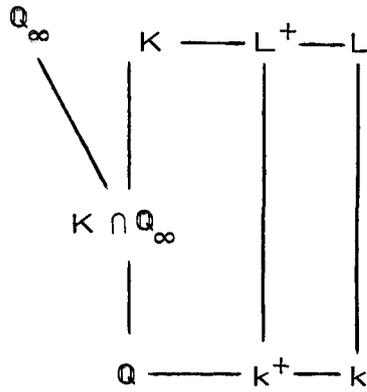
2. Translation des invariants Λ et $\bar{\Lambda}$ par extension de degré puissance de p .

Soit M/L une extension de degré puissance de p (avec M et L abéliens, réels ou imaginaires simultanément). On se propose de comparer $\Lambda(M)$ et $\Lambda(L)$ (resp. $\bar{\Lambda}(M)$ et $\bar{\Lambda}(L)$) si M et L sont réels (resp. imaginaires). On remarque qu'il y a, dans le cas imaginaire, à distinguer le cas $p \neq 2$ du cas $p = 2$.

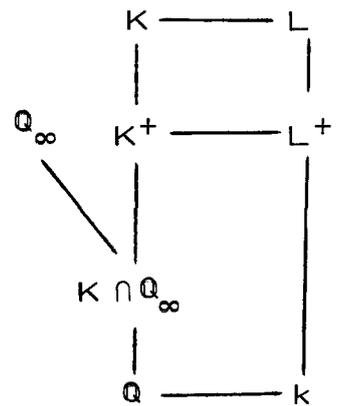
On ramène cette étude à la situation suivante (où K/\mathbb{Q} (resp. k/\mathbb{Q}) est de degré puissance de p (resp. premier à p), où $L = Kk$, et où l'on pose $p^n \circ = [K \cap \mathbb{Q}_\infty : \mathbb{Q}]$) :



cas réel



cas imaginaire
($p \neq 2$)



cas imaginaire
($p = 2$)

(i) Cas réel.

D'après 1.4 on a $\Lambda(L) = 1 + \sum_{\psi} \lambda(\psi)$, $\psi \in \tilde{\Psi}_L$. Si on écrit $\Psi_L = \Psi_K \times \Psi_k$,

alors $\tilde{\Psi}_L = \tilde{\Psi}_K \times \Psi_k$ convient. On a d'après [3], prop. V3 :

$\lambda(\psi_p \psi_o) = \lambda(\psi_o) + \sum_{\ell} p^{n(\ell)}$, où la sommation est relative aux premiers $\ell \neq p$, $\ell \mid f_{\psi_p}$, $\theta_{\psi_o}^{-1}(\ell)$ étant une racine de l'unité d'ordre puissance de p ; on

rappelle que $n(\ell)$ est défini par $\ell \theta^{-1}(\ell) = 1 + qp^{n(\ell)}u$, $(u, p) = 1$. Si

$\ell \mid f_{\psi_p}$, nécessairement on a $\ell \equiv 1 \pmod p$, d'où : la condition sur $\theta_{\psi_o}^{-1}(\ell)$

équivaut à $\psi_o(\ell) = 1$ (i. e. ℓ totalement décomposé dans $K_{\psi_o} \subset k$).

$$\begin{aligned} \text{On a } \Lambda(L) &= 1 + \sum_{\psi_p, \psi_o} \left(\lambda(\psi_o) + \sum_{\ell} p^{n(\ell)} \right) \\ &= 1 + \frac{[K:Q]}{p^{n_o}} \sum_{\psi_o} \lambda(\psi_o) + \sum_{\psi_p, \psi_o} \sum_{\ell} p^{n(\ell)}, \quad \psi_p \in \tilde{\Psi}_K, \psi_o \in \Psi_k; \end{aligned}$$

posons $a(\ell) = |\{\psi \in \tilde{\Psi}_K \times \Psi_k, \ell \mid f_{\psi_p}, \psi_o(\ell) = 1\}|$ et remarquons que

$$\Lambda(k) = 1 + \sum_{\psi_o} \lambda(\psi_o), \quad \psi_o \in \Psi_k; \text{ alors :}$$

$$\Lambda(L) = 1 + \frac{[K:Q]}{p^{n_o}} (\Lambda(k) - 1) + \sum_{\ell \neq p} p^{n(\ell)} a(\ell). \text{ Pour calculer } a(\ell), \text{ soit } d(\ell)$$

le degré sur \mathbb{Q} du corps de décomposition $k(\ell)$ de ℓ dans k ; soit $e_{L/k}(\ell)$

l'indice de ramification de ℓ dans L/k . Alors on a $\psi_o(\ell) = 1$ si et seulement si $\psi_o \in \Psi_{k(\ell)}$, et $\ell \nmid f_{\psi_p}$ si et seulement si ψ_p est caractère du corps d'inertie pour ℓ dans K/\mathbb{Q} . Il en résulte immédiatement que

$$a(\ell) = \frac{[K:\mathbb{Q}]_p}{n_o} \frac{e_{L/k}(\ell) - 1}{e_{L/k}(\ell)} d(\ell), \text{ d'où :}$$

$$(2.1) \quad \Lambda(L) - 1 = \frac{[L:k]}{[L \cap \mathbb{Q}_\infty:\mathbb{Q}]} \left(\Lambda(k) - 1 + \sum_{\ell \neq p} \frac{e_{L/k}(\ell) - 1}{e_{L/k}(\ell)} d(\ell) p^{n(\ell)} \right).$$

Si M est une extension abélienne réelle de \mathbb{Q} , de degré puissance de p sur L , on obtient, par combinaison des formules 2.1 obtenues pour L et M , la formule suivante (en remarquant que le corps k est commun à L et M) :

$$(2.2) \quad \Lambda(M) - 1 = \frac{[M:L]}{[M \cap \mathbb{Q}_\infty:L \cap \mathbb{Q}_\infty]} (\Lambda(L) - 1 + \frac{[L:k]}{[L \cap \mathbb{Q}_\infty:\mathbb{Q}]} \sum_{\ell \neq p} \frac{e_{M/L}(\ell) - 1}{e_{M/k}(\ell)} d(\ell) p^{n(\ell)}),$$

où $e_{M/L}(\ell)$, $e_{M/k}(\ell)$ sont les indices de ramification de ℓ dans M/L et M/k , où $d(\ell)$ est le degré sur \mathbb{Q} du corps de décomposition de ℓ dans k .

Remarque. Si M/L est non ramifiée en dehors de p , alors on obtient

$\Lambda(M) - 1 = \frac{[M:L]}{[M \cap \mathbb{Q}_\infty:L \cap \mathbb{Q}_\infty]} (\Lambda(L) - 1)$; donc en général (i. e. lorsque $[M \cap \mathbb{Q}_\infty:L \cap \mathbb{Q}_\infty] = [M:L]$), on obtient $\Lambda(M) = \Lambda(L)$. Il n'est d'ailleurs pas difficile d'établir, à partir de la formule 2.2, que la condition nécessaire et suffisante pour que $\Lambda(M) = \Lambda(L)$ est que $[M \cap \mathbb{Q}_\infty:L \cap \mathbb{Q}_\infty] = [M:L]$ et que M/L soit non ramifiée en dehors de p .

(ii) Cas imaginaire ($p \neq 2$).

D'après 1.6 on a $\bar{\Lambda}(L) = \rho(L) + \sum_{\psi} \lambda(\psi)$, ψ parcourant $\mathfrak{M}(\tilde{\Psi}_L^-)$, soit

$\bar{\Lambda}(L) = \rho(L) + \sum_{\psi'} \lambda(\theta \psi'^{-1})$, ψ' parcourant $\tilde{\Psi}_L^-$. On a

$\tilde{\Psi}_L^- = (\tilde{\Psi}_K \times \Psi_K)^- = \tilde{\Psi}_K \times \Psi_K^-$, donc

$$\bar{\Lambda}(L) = \rho(L) + \sum_{\psi'_p, \psi'_o} \lambda(\theta \psi'_p^{-1} \psi'_o^{-1}) = \rho(L) + \sum_{\psi'_p, \psi'_o} \left(\lambda(\theta \psi'_o^{-1}) + \sum_{\ell} p^{n(\ell)} \right),$$

$\psi'_p \in \tilde{\Psi}_K$, $\psi'_o \in \Psi_K^-$, et où la dernière sommation est étendue aux premiers $\ell \neq p$ tels que $\ell \mid f_{\psi'_p}$, $\theta(\theta^{-1} \psi'_o)(\ell) = \psi'_o(\ell)$ soit une racine de l'unité d'ordre

puissance de p , soit $\psi'_o(\ell) = 1$. On obtient alors

$$\bar{\Lambda}(L) = \rho(L) + \frac{[K:\mathbb{Q}]}{p^{n_o}} \sum_{\psi'_o} \lambda(\theta \psi'_o^{-1}) + \sum_{\ell \neq p} p^{n(\ell)} a(\ell), \text{ avec}$$

$$a(\ell) = |\{\psi'_i \in \tilde{\Psi}_K \times \Psi_K^-, \ell \mid f_{\psi'_i}, \psi'_o(\ell) = 1\}|. \text{ Comme, d'après 1.6,}$$

$$\bar{\Lambda}(k) = \rho(k) + \sum_{\psi'_o} \lambda(\theta \psi'_o^{-1}), \psi'_o \in \Psi_K^-, \text{ il vient}$$

$$\bar{\Lambda}(L) = \rho(L) + \frac{[K:\mathbb{Q}]}{p^{n_o}} (\bar{\Lambda}(k) - \rho(k)) + \sum_{\ell \neq p} p^{n(\ell)} a(\ell). \text{ Le calcul de } a(\ell) \text{ est}$$

similaire à celui fait dans (i), à ceci près que si $k(\ell)$ est réel, alors aucun caractère de $k(\ell)$ n'est impair et que si $k(\ell)$ est imaginaire, il y a $\frac{d(\ell)}{2}$ caractères impairs de la forme ψ'_o . D'où :

$$(2.3) \quad \bar{\Lambda}(L) - \rho(L) = \frac{[L:k]}{[L \cap \mathbb{Q}_\infty:\mathbb{Q}]} (\bar{\Lambda}(k) - \rho(k) + \sum_{\ell^+ \neq p} \frac{e_{L/k}(\ell^+) - 1}{e_{L/k}(\ell^+)} \frac{d(\ell^+)}{2} p^{n(\ell^+)})$$

où la sommation est étendue aux premiers ℓ^+ décomposés dans k/k^+ ($p \neq 2$).

Comme pour le cas des invariants Λ , on obtient une formule de translation d'un corps L à un corps abélien M de degré puissance de p sur L ($p \neq 2$) :

$$(2.4) \quad \bar{\Lambda}(M) - \rho(M) = \frac{[M:L]}{[M \cap \mathbb{Q}_\infty:L \cap \mathbb{Q}_\infty]} (\bar{\Lambda}(L) - \rho(L) + \frac{[L:k]}{[L \cap \mathbb{Q}_\infty:\mathbb{Q}]} \sum_{\ell^+ \neq p} \frac{e_{M/L}(\ell^+) - 1}{e_{M/k}(\ell^+)} \frac{d(\ell^+)}{2} p^{n(\ell^+)})$$

où la sommation est étendue aux premiers $\ell^+ \neq p$ décomposés dans k/k^+ ($p \neq 2$).

Ces formules ont été données par Kida ([6], [7]), dans le cadre des "C. M-fields", en appliquant la théorie des genres convenablement.

(iii) Cas imaginaire (p = 2).

On a toujours $\bar{\Lambda}(L) = \rho(L) + \sum_{\psi'} \lambda(\theta \psi'^{-1})$, où ψ' parcourt $\tilde{\Psi}_L^-$;
 comme ici les caractères ψ'_0 sont pairs, on a $\tilde{\Psi}_L^- = (\tilde{\Psi}_K \times \Psi_K)^- = \tilde{\Psi}_K^- \times \Psi_K$,
 d'où $\bar{\Lambda}(L) - \rho(L) = \sum_{\psi'_2, \psi'_0} \lambda(\theta \psi'_2{}^{-1} \psi'_0{}^{-1})$, $\psi'_2 \in \tilde{\Psi}_K^-$, $\psi'_0 \in \Psi_K$. Ici le caractè-
 re $\theta \psi'_2{}^{-1} \psi'_0{}^{-1}$ ne peut plus être décomposé comme dans le cas (ii) ; on
 écrit que $\theta \psi'_2{}^{-1} \psi'_0{}^{-1}$ est le produit des caractères pairs $\theta \psi'_2{}^{-1}$ et $\psi'_0{}^{-1}$:
 $\lambda(\theta \psi'_2{}^{-1} \psi'_0{}^{-1}) = \lambda(\psi'_0{}^{-1}) + \sum_{\ell} 2^{n(\ell)}$, sommation sur les $\ell \neq 2$ tels que
 $\ell \mid f_{\psi'_2}$, $\theta \psi'_0(\ell)$ est une racine de l'unité d'ordre puissance de 2, soit
 $\psi'_0(\ell) = 1$. On a $\bar{\Lambda}(L) = \rho(L) + \sum_{\psi'_p, \psi'_0} \lambda(\psi'_0{}^{-1}) + \sum_{\ell \neq p} 2^{n(\ell)} a(\ell)$, où
 $a(\ell) = |\{\psi' \in \tilde{\Psi}_K^- \times \Psi_K, \ell \mid f_{\psi'_2}, \psi'_0(\ell) = 1\}|$. Les caractères ψ'_0 sont au
 nombre de $d(\ell)$; les caractères ψ'_2 sont impairs et doivent être non caractè-
 res du corps d'inertie pour ℓ dans K/\mathbb{Q} donc il n'intervient que les pre-
 miers ℓ pour lesquels le corps d'inertie en question est imaginaire. Si
 $e_{L/k}^+(\ell)$ est l'indice de ramification de ℓ dans L^+/k , alors la quantité
 $2 \frac{e_{L/k}(\ell) - 1}{e_{L/k}(\ell)} - \frac{e_{L/k}^+(\ell) - 1}{e_{L/k}^+(\ell)}$ vaut $\frac{e_{L/k}(\ell) - 1}{e_{L/k}(\ell)}$ (resp. 1) si le corps d'inertie
 de ℓ dans L/k est réel (resp. imaginaire) ce qui donne bien le nombre de
 caractères ψ'_2 cherchés, relativement au calcul de $a(\ell)$.

On remarque que $\sum_{\psi'_0} \lambda(\psi'_0{}^{-1})$ n'est pas relié à $\bar{\Lambda}(k)$ (en effet k est
 réel) ; considérons pour cela $\bar{\Lambda}(k(\mu_4)) = 1 + \sum_{\psi''} \lambda(\theta \psi''^{-1})$, $\psi'' \in \Psi_K^-(\mu_4)$,
 sachant que $\Psi_K^-(\mu_4) = \{\theta \psi'_0, \psi'_0 \in \Psi_K\}$; on obtient $\bar{\Lambda}(k(\mu_4)) = 1 + \sum_{\psi'_0} \lambda(\psi'_0)$,
 et finalement :

$$(2.5) \quad \bar{\Lambda}(L) - \rho(L) = \frac{[L : k]}{2[L \cap \mathbb{Q}_\infty : \mathbb{Q}]} \left(\bar{\Lambda}(k(\mu_4)) - 1 + \sum_{\ell \neq 2} \left(2 \frac{e_{L/k}(\ell) - 1}{e_{L/k}(\ell)} - \frac{e_{L/k}^+(\ell) - 1}{e_{L/k}^+(\ell)} \right) d(\ell) 2^{n(\ell)} \right),$$

et la formule de translation :

$$(2.6) \quad \bar{\Lambda}(M) - \rho(M) = \frac{[M:L]}{2[M \cap \mathbb{Q}_\infty : L \cap \mathbb{Q}_\infty]} \left(\bar{\Lambda}(L) - \rho(L) + \frac{[L:k]}{[L \cap \mathbb{Q}_\infty : \mathbb{Q}]} \sum_{\ell \neq 2} \left(2 \frac{e_{M/L}(\ell) - 1}{e_{M/L}(\ell)} - \frac{e_{M^+/L^+}(\ell) - 1}{e_{M^+/L^+}(\ell)} \right) d(\ell) 2^{n(\ell)} \right).$$

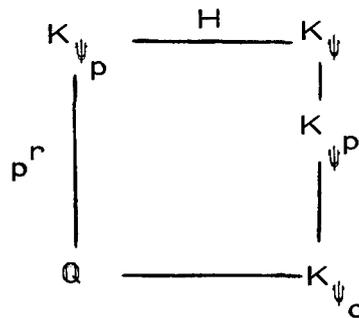
3. Les invariants $\mathcal{L}(\phi), \bar{\mathcal{L}}(\phi)$.

C'est la notion de ϕ -objets développée dans [2] qui va nous conduire à la définition de ces invariants.

Rappels sur les modules $\mathcal{C}(\phi)$ et $\mathcal{X}(\phi)$.

Si ψ est un caractère abélien, on appelle ϕ (resp. φ) le caractère p -adique au-dessus de ψ (resp. ψ_o).

Considérons le schéma suivant :



On peut considérer φ comme caractère du groupe $H = \text{Gal}(K_{\psi}/K_{\psi_p})$;

il existe alors un idempotent $e_{\varphi} = \frac{1}{|H|} \sum_{\tau \in H} \varphi(\tau^{-1}) \tau$ qui est dans $\mathbb{Z}_p[H]$.

Soit $v_{\psi} = \sum_{s_{\psi}} s_{\psi}$, s_{ψ} parcourant $\text{Gal}(K_{\psi}/K_{\psi_p})$.

Soit t un générateur de $\text{Gal}(K_{\psi}/\mathbb{Q})$; on pose :

$$(3.1) \quad A = \prod_{\alpha | \phi} (t - \alpha(t)) \in \mathbb{Z}_p[\text{Gal}(K_{\psi}/\mathbb{Q})].$$

On définit alors :

$$(3.2) \quad \mathcal{C}(\phi) = \{ \tau \in \mathcal{C}(K_{\psi}), \tau^A = 1 \}, \text{ si } \phi \text{ est pair.}$$

D'après [2], § 1, on a aussi $\mathcal{C}(\varphi) = \{\tau \in \mathcal{C}(K_\psi), \tau^\psi = 1\}^{e_\varphi}$.

De même dans le cas impair on pose :

$$(3.3) \quad \mathcal{H}(\varphi) = \{h \in \mathcal{H}(K_\psi), h^A = 1\}, \text{ si } \varphi \text{ est impair.}$$

Comme précédemment on a aussi $\mathcal{H}(\varphi) = \{h \in \mathcal{H}(K_\psi), h^\psi = 1\}^{e_\varphi}$.

Il résulte de ces définitions et propriétés que $\mathcal{C}(\varphi)$ et $\mathcal{H}(\varphi)$ sont des modules sur l'anneau $\mathbb{Z}_p(\psi)$ (par utilisation de l'application $\mathbb{Z}_p[\text{Gal}(K_\psi/\mathbb{Q})] \rightarrow \mathbb{Z}_p(\psi)$ qui à t associe $\psi(t)$, dont le noyau est précisément l'idéal engendré par A).

A l'heure actuelle on ne connaît pas de formules analytiques pour exprimer $|\mathcal{C}(\varphi)|$, $|\mathcal{H}(\varphi)|$, en termes de fonctions L_p (on a des expressions conjecturales : cf. [2], § III et [4], § 3.5.3). Cependant les nombres $\prod_{\varphi} |\mathcal{C}(\varphi)|$, $\prod_{\varphi} |\mathcal{H}(\varphi)|$, où φ parcourt l'ensemble des caractères p -adiques divisant un caractère rationnel χ , peuvent s'interpréter comme ordres de modules $\mathcal{C}(\chi)$, $\mathcal{H}(\chi)$ convenables, qui admettent une telle formule (dans le cas de \mathcal{C} voir [4], Th. 3.1, et dans celui de \mathcal{H} voir [2], Th. II2) ; rappelons ces formules :

$$(3.4) \quad |\mathcal{C}(\chi)| \approx p^{n_o(\chi)} \prod_{\alpha | \chi} \frac{1}{2} L_p(1, \alpha), \text{ dans le cas où } \chi \text{ est un caractère rationnel pair, où } n_o(\chi) = 1 \text{ ou } 0 \text{ selon que } \chi \text{ est caractère de } \mathbb{Q}_\infty \text{ ou non.}$$

$$(3.5) \quad |\mathcal{H}(\chi)| \approx p^{m_o(\chi)} \prod_{\beta | \chi} \frac{1}{2} B_1(\beta^{-1}), \text{ dans le cas où } \chi \text{ est un caractère rationnel impair, où } m_o(\chi) \text{ est ainsi défini :}$$

si $p \neq 2$, $m_o(\chi) = 1$ ou 0 selon que K_χ est ou non égal à un corps cyclotomique de la forme $\mathbb{Q}(\mu_{p^n})$, $n \geq 1$;

si $p = 2$, $m_o(\chi) = 2$, et dans les autres cas, $m_o(\chi) = 1$ ou 0 selon que l'ordre des caractères $\beta | \chi$ est une puissance de 2 ou non.

Par un raisonnement analogue à celui du § 1 on voit que si χ_n est le caractère rationnel au-dessus de $\gamma_n \psi$, alors pour n assez grand $|\mathcal{C}(\chi_n)|$ (resp. $|\mathcal{H}(\chi_n)|$) est constant et ne dépend que du caractère ration-

nel χ au-dessus de ψ (nous laissons au lecteur le soin d'écrire les formules explicites reliant ces ordres aux invariants λ ; on pourrait définir ainsi des invariants $\Lambda(\chi)$ (resp. $\bar{\Lambda}(\chi)$) qui permettraient de décomposer les invariants $\Lambda(K)$ (resp. $\bar{\Lambda}(K)$) par rapport aux caractères abéliens rationnels).

Outre cela, on voit que les nombres $|\mathcal{Z}(\phi_n)|$ (resp. $|\mathcal{H}(\phi_n)|$) sont bornés pour n assez grand (ϕ_n désignant n'importe quel caractère p -adique divisant χ_n). Nous utiliserons ce fait plus loin (cf. 4.1).

A partir de ceci nous avons démontré dans [4] que $|\mathcal{Z}(\phi_n)|$ était constant pour n assez grand, ce qui définit l'invariant $\Lambda(\phi)$ par l'égalité :

$$(3.6) \quad |\mathcal{Z}(\phi_n)| = p^{\Lambda(\phi)} \text{ pour tout } n \text{ assez grand.}$$

On peut, par une méthode analogue, prouver que, dans le cas impair on a aussi :

$$(3.7) \quad |\mathcal{H}(\phi_n)| = p^{\bar{\Lambda}(\phi)}, \text{ pour tout } n \text{ assez grand.}$$

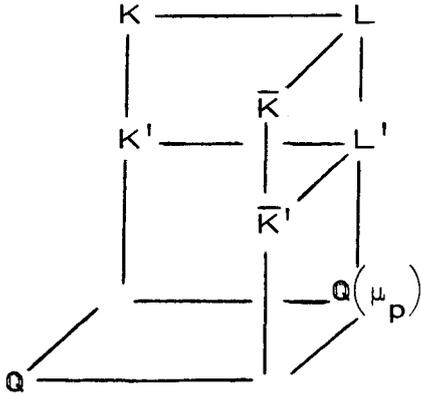
Nous ne le ferons pas ici car le théorème que nous avons en vue ci-après l'entraînera trivialement.

4. Comparaison des modules $\mathcal{Z}(\phi_n)$ et $\mathcal{H}(\bar{\phi}_n)$.

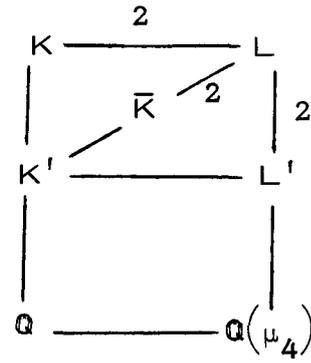
Définitions et résultats préliminaires.

Considérons un caractère pair quelconque ψ fixé, et un entier n assez grand. On appelle g l'ordre de ψ_0 . On considère les caractères $\gamma_n \psi$ et $\theta \gamma_n^{-1} \psi^{-1}$, et on appelle $\varphi, \bar{\varphi}, \phi, \bar{\phi}, \phi_n, \bar{\phi}_n$ les caractères p -adiques au-dessus de $\psi_0, \theta \psi_0^{-1}, \psi, \theta \psi^{-1}, \gamma_n \psi, \theta \gamma_n^{-1} \psi^{-1}$ respectivement. Pour simplifier, on pose $K = K_{\gamma_n \psi}$ (qui est réel), $\bar{K} = K_{\theta \gamma_n^{-1} \psi^{-1}}$ (qui est imaginaire), et $L = K\bar{K}$. Il est clair que L contient μ_q puisque θ est un caractère de L ; on a aussi $L = K(\mu_q) = \bar{K}(\mu_q)$. Enfin on appelle K', \bar{K}' et L' les uniques sous-corps d'indice p de K, \bar{K} et L respectivement. Pour simplifier certains calculs, nous poserons parfois $\mathcal{Z} = \mathcal{Z}(\phi_n)$, et $\mathcal{H} = \mathcal{H}(\bar{\phi}_n)$.

On a les schémas suivants :



cas p ≠ 2



cas p = 2

Soient $G, G_K, G_{\bar{K}}$ les groupes de Galois de $L/\mathbb{Q}, K/\mathbb{Q}$ et \bar{K}/\mathbb{Q} ; soit H le plus grand sous-groupe de G d'ordre premier à p . On appelle s un générateur de $\text{Gal}(L/L')$, σ_∞ la conjugaison complexe, t un générateur de G_K et \bar{t} un générateur de $G_{\bar{K}}$.

On définit l'involution suivante ([8], [9]) :

$$\begin{aligned} \mathfrak{M} : \mathbb{Z}_p[G] &\longrightarrow \mathbb{Z}_p[G] \\ \sum_{\sigma} a_{\sigma} \sigma &\longrightarrow \sum_{\sigma} a_{\sigma} \theta(\sigma) \sigma^{-1}. \end{aligned}$$

On pose $v = \sum_{i=1}^p s^i$; alors $\mathfrak{M}(v) = \sum_{i=1}^p s^{-i}$ car comme L' contient μ_q , on a $\theta(s) = 1$; d'où $\mathfrak{M}(v) = v$.

Considérons φ comme caractère de H et posons $e_{\varphi} = \frac{1}{|H|} \sum_{\sigma \in H} \varphi(\sigma^{-1})\sigma$.

Pour $p \neq 2$, on a $\mathfrak{M}(e_{\varphi}) = \frac{1}{|H|} \sum_{\sigma \in H} \theta(\sigma)\varphi(\sigma^{-1})\sigma^{-1} = \frac{1}{|H|} \sum_{\sigma \in H} \bar{\varphi}(\sigma^{-1})\sigma = e_{\bar{\varphi}}$

($\bar{\varphi}$ est encore un caractère de H). Pour $p = 2$, on a

$\mathfrak{M}(e_{\varphi}) = \frac{1}{|H|} \sum_{\sigma \in H} \varphi(\sigma^{-1})\sigma^{-1}$, car $\theta(\sigma) = 1$ (ici $[\mathbb{Q}(\mu_4) : \mathbb{Q}] = 2$, donc

$\mathbb{Q}(\mu_4)$ est fixé par H) ; d'où $\mathfrak{M}(e_{\varphi}) = e_{\varphi^*}$ où φ^* est le caractère 2-adique au-dessus de ψ_0^{-1} .

On rappelle que d'après 3.2 et 3.3 on peut écrire :

$$\mathcal{C}(\phi_n) = \{\tau \in \mathcal{C}(K), \tau^v = \tau^{1 - e_\phi} = 1\} = \{\tau \in \mathcal{C}(K), \tau^A = 1\},$$

$$\text{où } A = \prod_{\alpha | \phi_n} (t - \alpha(t)),$$

$$\mathcal{H}(\bar{\phi}_n) = \{h \in \mathcal{H}(\bar{K}), h^v = h^{1 - e_{\bar{\phi}}} = 1\} = \{h \in \mathcal{H}(\bar{K}), h^{\bar{A}} = 1\},$$

$$\text{où } \bar{A} = \prod_{\beta | \bar{\phi}_n} (\bar{t} - \beta(\bar{t})) \text{ (cas } p \neq 2),$$

$$\mathcal{H}(\bar{\phi}_n) = \{h \in \mathcal{H}(\bar{K}), h^v = h^{1 - e_{\phi^*}} = 1\} = \{h \in \mathcal{H}(\bar{K}), h^{\bar{A}} = 1\},$$

où \bar{A} est inchangé (cas $p = 2$: en effet, ici le caractère de \bar{K} est

$\psi^1 = \theta \gamma_n^{-1} \psi_2^{-1} \psi_0^{-1}$ pour lequel le caractère ψ_0^1 associé est ψ_0^{-1} contrairement au cas $p \neq 2$ où ce caractère est $\theta \psi_0^{-1}$).

On utilisera ce qui précède sous la forme suivante :

$$\mathcal{C}(\phi_n) = \{\tau \in \mathcal{C}(K), \tau^\omega = 1, \text{ pour tout } \omega \in (v, 1 - e_\phi)\},$$

$$\mathcal{H}(\bar{\phi}_n) = \{h \in \mathcal{H}(\bar{K}), h^{\bar{\omega}} = 1, \text{ pour tout } \bar{\omega} \in \mathfrak{M}(v, 1 - e_\phi)\},$$

sachant que $\mathfrak{M}(v, 1 - e_\phi)$ a été calculé plus haut : $\mathfrak{M}(v, 1 - e_\phi) = (v, 1 - e_{\bar{\phi}})$ (resp. $(v, 1 - e_{\phi^*})$) si $p \neq 2$ (resp. $p = 2$).

Comme dans [4], § 1, appelons \hat{K} la p -extension abélienne p -ramifiée maximale de K ; $\mathcal{C}(K)$ est par définition le G -module $\text{Gal}(\hat{K}/K_\infty)$. Soit N le sous-corps de \hat{K} fixé par $\mathcal{C}(K)^A$, et soit $M = NL$; on a $\text{Gal}(N/K_\infty) \simeq \mathcal{C}(K)/\mathcal{C}(K)^A$; en vertu de 3.2 il en résulte que $|\mathcal{C}(\phi_n)| = (\mathcal{C}(K) : \mathcal{C}(K)^A)$.

Démontrons maintenant :

(4.1) Les groupes $\text{Gal}(N/K_\infty) \simeq \mathcal{C}(K)/\mathcal{C}(K)^A$ et $\mathcal{H}(\bar{\phi}_n)$ sont d'exposants diviseurs de p .

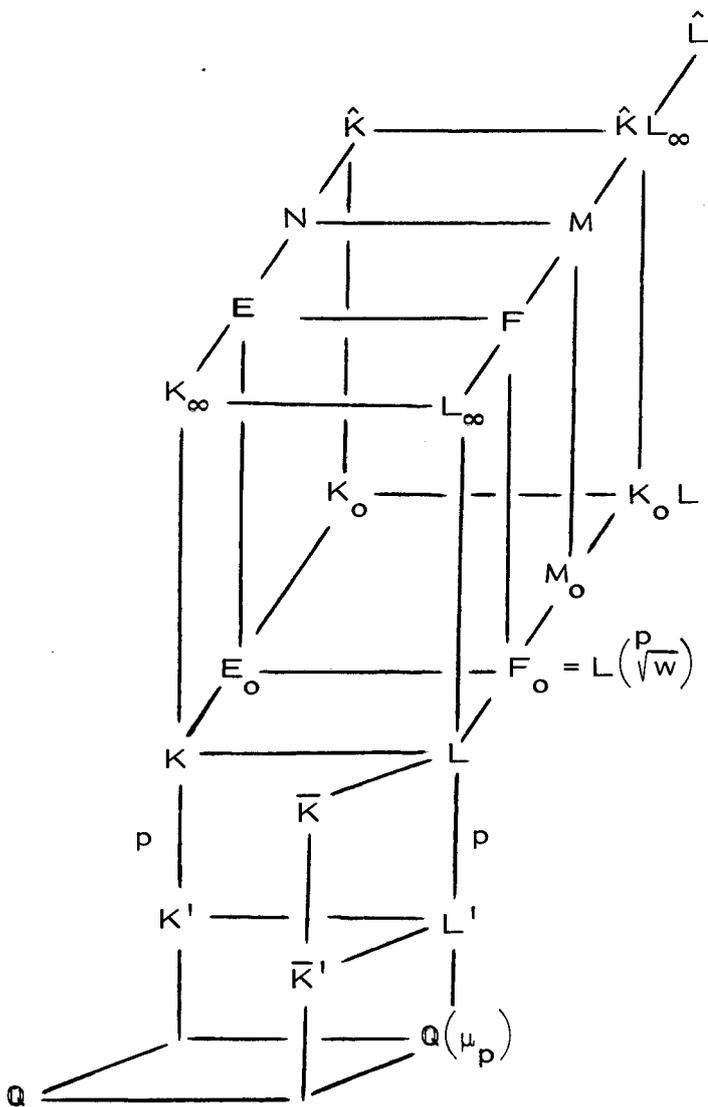
Soit \mathfrak{P}_n l'idéal maximal de $\mathbb{Z}_p(\gamma_n \psi)$; alors $\mathcal{C}(K)/\mathcal{C}(K)^A$, qui est annihilé par A , est isomorphe à un $\mathbb{Z}_p(\gamma_n \psi)$ -module de la forme

$\prod_{i \geq 0} \mathbb{Z}_p(\gamma_n \psi) / \mathfrak{P}_n^{a_n^i}$, $a_n^i \geq 0$. La formule 3.4 montre que l'ordre de $\mathcal{C}(K)/\mathcal{C}(K)^A$ est borné sur n ; par conséquent comme $\mathbb{Z}_p(\gamma_n \psi) / \mathfrak{P}_n$ est d'ordre $p^{\varphi(1)}$

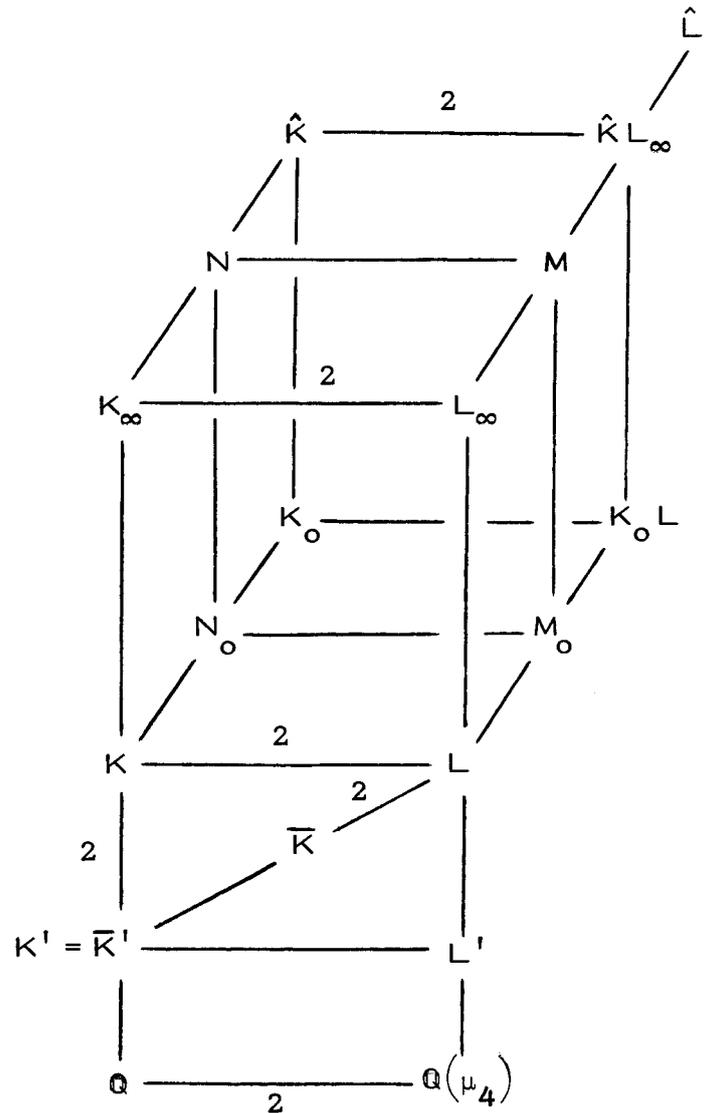
(indépendant de n), les a_n^i sont uniformément bornés sur n et i par une constante a ; d'où l'annulation par p d'un tel module pour tout n assez grand.

La démonstration est identique pour $\mathcal{H}(\bar{\varphi}_n)$, à partir de 3.5.

On a les schémas généraux suivants :



cas $p \neq 2$



cas $p = 2$

Nous allons utiliser une méthode de type "Spiegelungssatz" de Leopoldt ([8]), avec des techniques voisines de celles développées dans [9].

Soit \mathcal{W}_∞ le radical, dans L_∞ , de l'extension de Kummer (d'exposant diviseur de p) M/L_∞ (i. e. $\{w \in L_\infty, L_\infty(\sqrt[p]{w}) \subset M\}$). On pose $\tilde{\mathcal{W}}_\infty = \mathcal{W}_\infty/L_\infty^p$, et on appelle \tilde{w} les éléments de $\tilde{\mathcal{W}}_\infty$. Plus généralement on pose $\tilde{L}_\infty = L_\infty/L_\infty^p$: $\tilde{\mathcal{W}}_\infty$ est une partie de \tilde{L}_∞ .

On a le résultat suivant :

(4.2) On a $L \cap L_\infty^p = \mu_L L^p$.

Il suffit de montrer l'inclusion $L \cap L_\infty^p \subset \mu_L L^p$, l'autre résultant du fait que $\mu_L \subset L_\infty^p$ car L contient μ_q , donc L_∞ contient $\bigcup_{n \geq 0} \mu_{q^n}$. Si $x \in L \cap L_\infty^p$, et si $x \notin L^p$, alors $L(\sqrt[p]{x})/L$ est kummerienne et est contenue dans L_∞ , donc $L(\sqrt[p]{w})$ est de la forme $L(\sqrt[p]{\zeta})$, $\zeta \in \mu_L$, soit $x = \zeta a^p$, $a \in L$.

(4.3) Tout élément $\tilde{w} \in \tilde{\mathcal{W}}_\infty$ a un représentant dans L (resp. un représentant totalement positif dans K) dans le cas $p \neq 2$ (resp. $p = 2$). Enfin $\tilde{\mathcal{W}}_\infty$ est un G -module annihilé par $\mathfrak{m}(\nu, 1 - e_\varphi)$.

On a $\text{Gal}(\hat{K}/K) \simeq \mathbb{Z}_p \oplus \mathcal{C}(K)$; il suffit donc de considérer un corps K_o fixe par la composante isomorphe à \mathbb{Z}_p : K_o/K et K_∞/K sont linéairement disjointes et $\hat{K} = K_o K_\infty$; de même, comme L/K et \hat{K}/K sont linéairement disjointes (car $[L : K]$ est premier à p pour $p \neq 2$, et pour $p = 2$, $[L : K] = 2$ mais \hat{K} est réelle tandis que L est imaginaire), $K_o L/L$ et L_∞/L sont linéairement disjointes. Il existe donc une extension M_o de L contenue dans $K_o L$ telle que $M_o L_\infty = M$; comme M_o/L est aussi une extension de Kummer (exposant diviseur de p), le résultat est immédiat. Dans le cas $p = 2$ on peut trouver $N_o \subset K_o$ telle que $N_o K_\infty = N$; dans ce cas, N_o/K est encore kummerienne (exposant diviseur de 2) et le résultat en découle (remarquons qu'un tel représentant dans K est nécessairement totalement positif puisque \hat{K} est totalement réel).

Par hypothèse $\text{Gal}(N/K_\infty)$ est annihilé par l'idéal $(\nu, 1 - e_\varphi)$, donc $\text{Gal}(M/L_\infty)$ est annihilé par ce même idéal et, par utilisation de la "Spiegelungsrelation" de Leopoldt ([8], § 3 ; cf. [9], Prop. 3.3), on en déduit que $\mathfrak{m}(\nu, 1 - e_\varphi)$ annule $\tilde{\mathcal{W}}_\infty$.

Démonstration du résultat principal (th. 5.1 de [4]).

Pour poursuivre, nous devons distinguer les cas $p \neq 2$ et $p = 2$.

Si Ω est un corps, \mathcal{O}_Ω désigne son anneau d'entiers ; on appelle p -idéal de Ω tout produit d'idéaux premiers de Ω au-dessus de p .

(i) Cas $p \neq 2$. On va construire une application de \mathcal{H} dans $\tilde{\mathcal{W}}_\infty$:

Soit $h \in \mathcal{H}$; on a $h^p = 1$, donc si $a \in h$, $a^p = a \mathcal{O}_{\bar{K}}$, $a \in \bar{K}$. On pose $\tilde{w} = \tilde{a}^{e_{\bar{\varphi}}}$ dans \tilde{L}_∞ . Si $b \in h$, $b = a c \mathcal{O}_{\bar{K}}$, $c \in \bar{K}$, soit, en posant $b^p = b \mathcal{O}_{\bar{K}}$, $b = a c^p \varepsilon$, ε unité de \bar{K} , et \tilde{w} est aussi défini par $(\tilde{a} \varepsilon)^{e_{\bar{\varphi}}}$. Or \bar{K} est imaginaire et cyclique ; d'après [5], § 25, Satz 24, on peut écrire $\varepsilon = \varepsilon_0 \zeta$, ε_0 unité réelle de \bar{K} , $\zeta \in \mu_{\bar{K}}$. On a $\tilde{\varepsilon}_0^{e_{\bar{\varphi}}} = \tilde{\gamma}$ car $\bar{\varphi}$ est impair, et $\tilde{\zeta} = \tilde{\gamma}$. L'application est donc bien définie.

Calcul du noyau. Supposons que $\tilde{w} = \tilde{a}^{e_{\bar{\varphi}}} = \tilde{\gamma}$; soit e un représentant mod p de $e_{\bar{\varphi}}$ dans $\mathbb{Z}[G]$, alors $a^e = u^p$, $u \in L_\infty$, et d'après 4.2, $a^e = \zeta b^p$, $\zeta \in \mu_L$, $b \in L$. On a donc dans L : $a^{e^p} \mathcal{O}_L = b^p \mathcal{O}_L$, soit $a^e \mathcal{O}_L = b \mathcal{O}_L$; comme $[L : \bar{K}]$ est premier à p , ceci entraîne $h = 1$.

Image. Montrons que $\tilde{w} = \tilde{a}^{e_{\bar{\varphi}}} \in \tilde{\mathcal{W}}_\infty$; comme $a \in \bar{K}$, on peut supposer $w \in \bar{K}$ (par exemple $w = a^e$). Soit $\tau \in \text{Gal}(L/K)$; par définition de K , on a $\gamma_n \psi_p \psi_0(\tau) = 1$, soit $\psi_0(\tau) = 1$. Calculons $\tau e_{\bar{\varphi}}$: on a $e_{\bar{\varphi}} = \frac{1}{|H|} \sum_{\sigma \in G} \bar{\varphi}(\sigma^{-1}) \sigma$, donc $\tau e_{\bar{\varphi}} = \frac{1}{|H|} \sum_{\sigma \in G} \bar{\varphi}(\sigma^{-1}) \tau \sigma = \frac{1}{|H|} \sum_{\sigma \in G} \bar{\varphi}(\tau \sigma^{-1}) \sigma$; or $\bar{\varphi} = \sum_{\psi_0 | \varphi} \theta \psi_0^{-1}$, d'où $\bar{\varphi}(\tau \sigma^{-1}) = \left(\theta \sum_{\psi_0 | \varphi} \psi_0^{-1} \right) (\tau \sigma^{-1}) = \theta(\tau) \theta(\sigma^{-1}) \sum_{\psi_0 | \varphi} \psi_0^{-1}(\sigma^{-1}) = \theta(\tau) \bar{\varphi}(\sigma^{-1})$,

et $\tau e_{\bar{\varphi}} = \theta(\tau) e_{\bar{\varphi}}$. Il résulte de ceci que dans \bar{K}^*/\bar{K}^{*p} l'image de w vérifie $(w \bar{K}^{*p})^{\tau - \theta(\tau)} = \bar{K}^{*p}$, pour tout $\tau \in \text{Gal}(L/K)$: ceci est le critère classique de décomposition qui montre que $F_0 = L(\sqrt[p]{w})$ est décomposée sur K par une extension cyclique E_0 de K telle que $E_0 L = F_0$. Comme $w \mathcal{O}_{\bar{K}} = a^{e^p}$ dans \bar{K} , la théorie élémentaire de Kummer montre que F_0/L , donc E_0/K , est

p -ramifiée, donc $E = E_0 K_\infty$ est contenue dans \hat{K} . Vérifions qu'elle est contenue dans N ; pour cela il suffit de prouver que $F = F_0 L_\infty$ est contenue dans M . Ceci revient à montrer que $\text{Gal}(F/L_\infty)$ est annulé par $(v, 1 - e_{\bar{\phi}})$, soit que $\langle \tilde{w} \rangle$ est annulé par $(v, 1 - e_{\bar{\phi}})$. L'annulation par $1 - e_{\bar{\phi}}$ est évidente par construction de \tilde{w} ($\tilde{w} = \tilde{a}^{e_{\bar{\phi}}}$). On étudie ensuite $\tilde{w}^v = a^{v e_{\bar{\phi}}}$: comme $h^v = 1$, on a $a^v = c \mathcal{O}_{\bar{K}}$, $c \in \bar{K}$, et $a^v = c^p \varepsilon$, ε unité de \bar{K} ; donc $\tilde{w}^v = \varepsilon^{e_{\bar{\phi}}} = \tilde{\gamma}$ comme on l'a déjà prouvé plus haut.

Surjectivité. Soit $\tilde{w}_1 \in \tilde{W}_\infty$ représenté par un élément $w_1 \in L$ tel que $F_0 = L(\sqrt[p]{w_1}) \subset M_0$; soit $v' = \sum_{\tau} \tau$, τ parcourant $\text{Gal}(L/\bar{K})$, alors $e_{\bar{\phi}}^{v'} = \bar{d} e_{\bar{\phi}}$, où $\bar{d} = [L : \bar{K}]$, et comme \bar{d} est premier à p , on peut remplacer w_1 par $w = N_{L/\bar{K}} w_1^{\bar{d}^*}$, \bar{d}^* inverse de $\bar{d} \pmod{p}$, et w est un représentant de $w_1 L^{*p}$ dans \bar{K} . Par la théorie de Kummer, on a $w \mathcal{O}_L = \mathfrak{a}^p \mathfrak{p}$ dans L , où \mathfrak{p} est un p -idéal de L ; comme $w \in \bar{K}$ et que $(\bar{d}, p) = 1$, il en résulte immédiatement $w \mathcal{O}_{\bar{K}} = \mathfrak{a}^p \mathfrak{p}$ dans \bar{K} , avec un p -idéal \mathfrak{p} de \bar{K} . On traduit le fait que \tilde{w} est annulé par l'idéal $(v, 1 - e_{\bar{\phi}})$: on a $\tilde{w}^v = \tilde{\gamma}$ soit $w^v \in L_\infty^p \cap L$, donc, d'après 4.2, $w^v = \zeta a^p$, $\zeta \in \mu_L$, ζ d'ordre puissance de p , $a \in L$; comme $w \in \bar{K}$, on peut supposer, quitte à utiliser $N_{L/\bar{K}}$, $\zeta \in \mu_{\bar{K}}$ et $a \in \bar{K}$. Montrons que $a^p \in \bar{K}'$.

Si $\zeta \in \bar{K}'$ c'est terminé. Supposons le contraire; on a nécessairement $\mu_p \subset \bar{K}'$ d'où $\bar{K} = L$ et $\bar{K}' = L'$. Comme une puissance non triviale de ζ est dans L' , L/L' est une extension de Kummer par une racine de l'unité (en particulier L/L' est p -ramifiée): ceci entraîne que L' et L sont de la forme $k(\mu_{p^n})$ et $k(\mu_{p^{n+1}})$ respectivement, où $k = K_{\psi_0}$. On a donc $\zeta^p \in L'$, donc $a^{p^2} \in L'$; on a $a^s = \xi a$, avec $\xi^{p^2} = 1$, mais comme n est assez grand, ξ est fixe par s , ce qui donne $a^{s^\lambda} = \xi^\lambda a$, $\lambda \geq 0$, soit (en faisant $\lambda = p$) $\xi^p = 1$, d'où $a^p \in L'$.

Donc dans tous les cas, $a^p \in \bar{K}'$, et $\zeta \in \bar{K}'$.

La relation $w \mathcal{O}_{\bar{K}} = a^p \mathfrak{p}$ dans \bar{K} donne, par $\bar{N} = N_{\bar{K}/\bar{K}'}$:
 $w^v \mathcal{O}_{\bar{K}'} = (\bar{N} a)^p \bar{N} \mathfrak{p}$; on a donc $a^p \mathcal{O}_{\bar{K}'} = (\bar{N} a)^p \bar{N} \mathfrak{p}$.

Si on a $a \notin \bar{K}'$, comme $a^p \in \bar{K}'$, on a un élément de Kummer pour l'extension \bar{K}/\bar{K}' (qui est nécessairement de Kummer), et la décomposition en idéaux (ci-dessus) de a^p dans \bar{K}' montre que \bar{K}/\bar{K}' est p -ramifiée ; on est donc à nouveau dans le cas où $\bar{K}' = k(\mu_{p^n})$, $\bar{K} = k(\mu_{p^{n+1}})$; on a donc une relation de la forme $a = \zeta b$, $\zeta \in \mu_{\bar{K}}$, $\zeta^p \in \mu_{\bar{K}'}$, et $b \in \bar{K}'$, d'où $a^p \mathcal{O}_{\bar{K}'} = b^p \mathcal{O}_{\bar{K}'}$, soit $(\bar{N} a)^p \bar{N} \mathfrak{p} = (b \mathcal{O}_{\bar{K}'})^p$ dans \bar{K}' , ce qui fait que $\bar{N} \mathfrak{p} = \mathfrak{q}'^p$ dans \bar{K}' , où \mathfrak{q}' est un p -idéal de \bar{K}' .

Si $a \in \bar{K}'$, on a directement $\bar{N} \mathfrak{p} = \mathfrak{q}'^p$ dans \bar{K}' .

Comme l'extension \bar{K}/\bar{K}' est totalement ramifiée en p , il en résulte que \mathfrak{p} est de la forme \mathfrak{q}^p pour un p -idéal \mathfrak{q} de \bar{K} , et $w \mathcal{O}_{\bar{K}} = b^p$ dans \bar{K} . On vérifie facilement que la classe h de b est telle que $h^{\bar{\varphi}} \in \mathcal{H}$ et redonne \tilde{w} par l'application étudiée.

On a donc obtenu l'isomorphisme de G -modules $\tilde{w}_\infty \simeq \mathcal{H}$; il en résulte que les G -structures de \mathcal{H} et $\mathcal{Z}(K)/\mathcal{Z}(K)^A$ sont reliées par la "Spiegelungsrelation".

(ii) Cas $p = 2$. On peut écarter provisoirement le cas où $\psi_0 = 1$: en effet, dans ce cas, $\gamma_n \psi$ et $\theta \gamma_n^{-1} \psi^{-1}$ sont des caractères d'ordre puissance de 2, donc ϕ_n et $\bar{\phi}_n$ sont rationnels, et dans ce cas les ordres de \mathcal{Z} et \mathcal{H} sont donnés par les formules analytiques 3.4 et 3.5 :

$$|\mathcal{Z}| \approx 2^\delta \prod_a \frac{1}{2} L_2(1, \gamma_n^a \psi^a), \quad a \in (\mathbb{Z}/2^n \mathbb{Z})^*, \quad \delta = 1 \text{ ou } 0 \text{ selon}$$

que ψ est caractère de \mathbb{Q}_∞ ou non,

$$|\mathcal{H}| \approx 2 \prod_a \frac{1}{2} L_2(0, \gamma_n^a \psi^a), \quad a \in (\mathbb{Z}/2^n \mathbb{Z})^*.$$

D'où $|\mathcal{H}| = 2^{1-\delta} |\mathcal{Z}|$, ce qui établit le théorème dans ce cas.

Supposons maintenant $\psi_o \neq 1$: on a $e_\varphi \neq 1$ et $e_{\varphi^*} \neq 1$.

Cette hypothèse permet de prouver que :

(4.4) Pour tout sous-corps Ω de L , l'application canonique

$$(\Omega^*/\Omega^{*2})^{e_{\varphi^*}} \longrightarrow (\tilde{L}_\infty^*)^{e_{\varphi^*}} \text{ est injective.}$$

Soit $a \in \Omega^*$ tel que $(a\Omega^{*2})^{1-e_{\varphi^*}} = \Omega^{*2}$, et tel que $\tilde{a} = \tilde{1}$ dans \tilde{L}_∞^* ; d'après 4.2 on a $a = \zeta v^2$, $\zeta \in \mu_L$, $v \in L$. On a $a^e = \zeta^e v^{2e}$, en appelant ici e un représentant mod une puissance de 2 convenable de e_{φ^*} dans $\mathbb{Z}[G]$.

Comme $\varphi^* \neq 1$, on vérifie que $\zeta^e = 1$. On a donc $a^e = v^{2e} \in \Omega$. Soit $\tau \in \text{Gal}(L/\Omega)$; alors on a, puisque $a \in \Omega$, $1 = v^{2e(\tau-1)}$, soit $v^{e(\tau-1)} = \pm 1$. Comme $(-1)^e = 1$, on a $v^{e^2(\tau-1)} = 1$; donc $v^{e^2} \in \Omega$, et on a $a^{e^2} \Omega^{*2} = \Omega^{*2}$, soit $a \in \Omega^{*2}$.

Ici, $\text{Gal}(M/L_\infty)$ est annulé par l'idéal $(1+s, 1-e_\varphi)$, donc, par la "Spiegelungsrelation", \tilde{W}_∞ est annulé par l'idéal $(1+s, 1-e_{\varphi^*})$.

Soit \mathcal{K}' le sous-module de \mathcal{K} formé des classes des idéaux \mathfrak{a} de \bar{K} tels que $\bar{N}\mathfrak{a}$ soit, dans K' , principal au sens restreint (\bar{N} désigne toujours $N_{\bar{K}/\bar{K}'}$); on vérifie que la définition est bien indépendante du choix de l'idéal \mathfrak{a} .

Soit $\mathcal{W}^* = \{w \in (\mathcal{W}_\infty^* \cap \bar{K})^e, w\bar{K} = \mathfrak{a}^2 \text{ dans } \bar{K}\}$. On a donc la relation

$$(w\bar{K}^{*2})^{1-e_{\varphi^*}} = \bar{K}^{*2}.$$

On a le résultat suivant :

(4.5) Pour tout $w \in \mathcal{W}_\infty^* \cap \bar{K}$, $w^{1+\sigma_\infty} = a_+^2$, $a_+ \in K'$, $a_+ \gg 0$.

En effet, on peut trouver (d'après 4.3) $w_o \in K$ représentant \tilde{w} ($w_o \gg 0$); donc d'après 4.2, il existe $u \in L$, $\zeta \in \mu_L$, tels que $w = w_o \zeta u^2$, et par $1+\sigma_\infty$ on obtient $w^{1+\sigma_\infty} = w_o^2 (u^{1+\sigma_\infty})^2 = a^2$, en posant $a = w_o u^{1+\sigma_\infty} \in K$.

On a $a \gg 0$ de façon évidente; de plus $w^{1+\sigma_\infty} \in K'$, donc $a^2 \in K'$. Si $a \notin K'$, on a une extension de Kummer de degré 2, $K = K'(a)$, et nécessaire-

ment, $a^S = -a$, ce qui est absurde car on a $a \gg 0$. Donc $a = a_+ \in K'$, d'où l'assertion.

A un tel $w \in \mathcal{W}$ associons la classe de a : cette application est définie de \mathcal{W} dans le groupe des classes de \bar{K} annihilées par 2 et $1 - e_{\varphi^*}$.

Elle induit grâce à 4.4 une application f de $\tilde{\mathcal{W}} \simeq \mathcal{W}/\mathcal{W} \cap \bar{K}^{*2}$ dans le groupe des classes de \bar{K} annihilées par 2 et $1 - e_{\varphi^*}$.

Noyau de f . Si $a = a \mathcal{O}_{\bar{K}}$, $a \in \bar{K}$, $w = \epsilon a^2$, ϵ unité de \bar{K} , donc $\tilde{w} = \tilde{\epsilon}$; comme \bar{K}/\mathbb{Q} est cyclique imaginaire, $\epsilon = \zeta \epsilon'$, $\zeta \in \mu_{\bar{K}}$, ϵ' unité de K' , et $\tilde{w} = \tilde{\epsilon}'$; comme $L_{\infty}(\sqrt{\epsilon'}) \subset M$ par hypothèse, il existe $w_0 \in K$, $w_0 \gg 0$, tel que $K(\sqrt{w_0}) \subset N_0$ et $K(\sqrt{w_0})L_{\infty} = L_{\infty}(\sqrt{\epsilon'})$ (cf. 4.3), donc $\epsilon' w_0^{-1} = u^2$, $u \in L_{\infty}$, et, d'après 4.4, appliqué à $\Omega = K$, on a $\epsilon' w_0^{-1} = b^2$, $b \in K$, d'où $\epsilon' \gg 0$.

Soit alors U (resp. U^+) le groupe des unités (resp. des unités totalement positives) de K' ; alors $\tilde{w} = \tilde{\epsilon}' \in (U^+/U^2)^{e_{\varphi^*}}$. Inversement, si $\tilde{\epsilon}' \in (U^+/U^2)^{e_{\varphi^*}}$, il est clair que $K_{\infty}(\sqrt{\epsilon'})$ est contenue dans \hat{K} ; elle est contenue dans N car on a $\tilde{\epsilon}'^{1+s} = \tilde{\epsilon}'^2 = \tilde{\gamma}$ et $\tilde{\epsilon}'^{1-e_{\varphi^*}} = \tilde{\gamma}$ par hypothèse. Donc $\tilde{\epsilon}' \in \tilde{\mathcal{W}}$.

Image de f . Si $w \in \mathcal{W}$, on a $w \mathcal{O}_{\bar{K}} = a^2$, et, d'après 4.5, $w^{1+\sigma_{\infty}} = a_+^2$, $a_+ \gg 0$ dans K' ; d'où par \bar{N} : $\bar{N} w \mathcal{O}_{K'} = (a_+ \mathcal{O}_{K'})^2 = (\bar{N} a)^2$, soit $\bar{N} a = a_+ \mathcal{O}_{K'}$, et la classe h de a est un élément dont la norme est, dans K' , principale au sens restreint. On a bien $h \in \mathcal{H}'$, car $h^{1+s} = 1$ et $h^{1-e_{\varphi^*}} = 1$ de façon évidente.

Vérifions maintenant que le choix du sous-ensemble $\tilde{\mathcal{W}}$ n'est pas restrictif pour notre problème :

$$(4.6) \quad \text{On a } \tilde{\mathcal{W}} = \tilde{\mathcal{W}}_{\infty}.$$

Il faut montrer que tout élément \tilde{w} de $\tilde{\mathcal{W}}_{\infty}$ a un représentant w' tel que

$w' \in \bar{K}$, $w' \mathcal{O}_{\bar{K}} = a^2$ dans \bar{K} .

Prenons w_0 dans K , $w_0 \gg 0$ (cf. 4.3) et posons $w = w_0^e$; on a par hypothèse $w^{1+s} = b^2$, $b \in L_\infty$, et d'après 4.4, on peut supposer $b \in K'$.

Il faut trouver un représentant dans \bar{K} : on a $(w/b)^{1+\sigma_\infty s} = w^{1+s}/b^2 = 1$,

donc $w/b = c^{1-\sigma_\infty s}$, $c \in L$. Posons $w' = w/c^2$; alors

$w'^{\sigma_\infty s} = w^{\sigma_\infty s} / c^{2\sigma_\infty s} = w^s w^2 / c^2 b^2 = w^{-1} b^2 w^2 / c^2 b^2 = w/c^2 = w'$; donc $w' \in \mathcal{W}_\infty \cap \bar{K}$. Etudions maintenant la décomposition en idéaux de $w' \mathcal{O}_{\bar{K}}$.

On a $L_\infty(\sqrt{w'})/L_\infty$ qui est 2-ramifiée; par conséquent, comme L_∞/L est 2-ramifiée, $L(\sqrt{w'})/L$ est aussi 2-ramifiée. Enfin $L = \bar{K}(\mu_4)$, donc L/\bar{K} est 2-ramifiée et $\bar{K}(\sqrt{w'})/\bar{K}$ est 2-ramifiée. D'où $w' \mathcal{O}_{\bar{K}} = a^2 \mathfrak{p}$, où \mathfrak{p} est un 2-idéal de \bar{K} ; $(\bar{N} w') \mathcal{O}_{K'} = (\bar{N} a)^2 \bar{N} \mathfrak{p}$, or, comme $w' \in \mathcal{W}_\infty \cap \bar{K}$, on a, d'après 4.5, $\bar{N} w' = w'^{1+\sigma_\infty} = b_+^2$, $b_+ \gg 0$, $b_+ \in K'$. On a donc $b_+^2 \mathcal{O}_{K'} = (\bar{N} a)^2 \bar{N} \mathfrak{p}$, et $\bar{N} \mathfrak{p}$ est de la forme q'^2 , où q' est un 2-idéal de K' ; comme \bar{K}/K' est totalement ramifiée en 2, il est nécessaire que \mathfrak{p} soit le carré d'un 2-idéal de \bar{K} , et on a prouvé 4.6.

On a donc, à ce stade, la suite exacte :

$$(4.7) \quad 1 \longrightarrow (U^+/U^2)^{e \varphi^*} \longrightarrow \tilde{\mathcal{W}}_\infty \xrightarrow{f} \mathcal{H}'.$$

Il est maintenant nécessaire de relier \mathcal{H} et \mathcal{H}' : On a la suite exacte suivante (où S est l'homomorphisme signature dans K' ; S est un homomorphisme de G -modules si l'on définit sur $S(K')$ l'opération de G par $\sigma S(\alpha) = S(\alpha^\sigma)$ pour tout $\sigma \in G$):

$$(4.8) \quad 1 \longrightarrow \mathcal{H}' \longrightarrow \mathcal{H} \xrightarrow{g} (S(K')/S(U))^{e \varphi^*} \longrightarrow 1.$$

Soit $h \in \mathcal{H}$; si $a \in h$, comme h est une classe relative, on a $\bar{N} a = a \mathcal{O}_{K'}$, $a \in K'$; à h on associe $S(a) \text{ mod } S(U)$: si b représente aussi h , on a $\bar{N} b = b \mathcal{O}_{K'}$, $b \in K'$; en écrivant $b = a c \mathcal{O}_{\bar{K}}$, $c \in \bar{K}$, on a $b \mathcal{O}_{K'} = a \mathcal{O}_{K'} \bar{N} c \mathcal{O}_{K'}$, soit $b = a \bar{N} c \eta$, $\eta \in U$, d'où $S(b) = S(a) S(\eta)$ car

$\bar{N}c \gg 0$: ceci définit bien l'application notée g .

On a $h \in \text{Ker } g$ si et seulement si $S(a) \in S(U)$, soit $S(a) = S(\epsilon)$, $\epsilon \in U$, et $a = \epsilon a_+$, $a_+ \in K^1$, $a_+ \gg 0$; on a donc $\bar{N}a = a \mathcal{O}_{K^1} = a_+ \mathcal{O}_{K^1}$, et $h \in \mathcal{H}^1$.

L'image de g est bien contenue dans $(S(K^1)/S(U))^e_{\varphi^*}$ comme on le vérifie immédiatement.

Pour démontrer la surjectivité de g , on utilise le corps de classes : Soit \tilde{K}^1 (resp. \tilde{K}) la 2-extension abélienne, non ramifiée pour les idéaux premiers, maximale, de K^1 (resp. \bar{K}) ; on a $\tilde{K}^1 \bar{K} \subset \tilde{K}$, et comme \bar{K}/K^1 est ramifiée en 2, on a $\tilde{K}^1 \cap \bar{K} = K^1$. On a $\text{Gal}(\tilde{K}/\bar{K})$ isomorphe au 2-groupe des classes de \bar{K} , et $\text{Gal}(\tilde{K}^1/K^1)$ isomorphe au 2-groupe des classes au sens restreint de K^1 . La restriction $\text{Gal}(\tilde{K}/\bar{K}) \longrightarrow \text{Gal}(\tilde{K}^1/K^1)$ correspond, dans ces isomorphismes, à la norme \bar{N} pour les groupes de classes ; donc cette norme est surjective : pour un idéal principal au sens ordinaire $a \mathcal{O}_{K^1}$ de K^1 , il existe \mathfrak{a} idéal de \bar{K} tel que $\bar{N}\mathfrak{a}$ engendre, dans K^1 , la classe au sens restreint de $a \mathcal{O}_{K^1}$: $\bar{N}\mathfrak{a} = a_+ a \mathcal{O}_{K^1}$, $a_+ \gg 0$, $a_+ \in K^1$.

Supposons que $S(a) \stackrel{1-e}{\varphi^*} = 1$, et considérons $h \stackrel{e}{\varphi^*}$, où h est la classe de \mathfrak{a} dans \bar{K} : on a $\bar{N}h \stackrel{e}{\varphi^*}$ qui est représentée par $\bar{N}\mathfrak{a}^e = (a_+ a)^e \mathcal{O}_{K^1}$, donc $S(a_+ a)^e = S(a)$, et il reste à vérifier que $h \stackrel{e}{\varphi^*} \in \mathcal{H}$, donc en fait que $h^{1+s} = 1$; or on a $\bar{N}h = 1$, d'où l'assertion.

Il reste ensuite à vérifier que $(U^+/U^2)^e_{\varphi^*}$ et $(S(K^1)/S(U))^e_{\varphi^*}$ ont même ordre. Soit $G^1 = \text{Gal}(K^1/\mathbb{Q})$; on peut identifier $S(K^1)$ et $\mathbb{F}_2[G^1]$ par l'application : $K^{1*}/K^{1*2} \rightarrow \mathbb{F}_2[G^1]$ définie par $\alpha K^{1*2} \rightarrow \sum_{\sigma} \text{sgn}(\alpha^{\sigma}) \sigma^{-1}$ (σ parcourant G^1 , et sgn étant la fonction signe notée additivement), on a alors l'isomorphisme de G -modules : $S(K^1) \simeq \mathbb{F}_2[G^1]$; il en résulte

$S(K^1) \stackrel{e}{\varphi^*} \simeq \mathbb{F}_2[G^1] \stackrel{e}{\varphi^*}$. On a la suite exacte :

$$1 \longrightarrow (U^+/U^2)^e_{\varphi^*} \longrightarrow (U/U^2)^e_{\varphi^*} \xrightarrow{S} S(U)^e_{\varphi^*} \longrightarrow 1$$

qui montre que l'on est ramené à prouver que $(U/U^2)^{e_{\varphi^*}}$ et $\mathbb{F}_2[G'] e_{\varphi^*}$ ont même ordre. En général U/U^2 et $\mathbb{F}_2[G']$ ne sont pas des G -modules isomorphes (bien que de même ordre) et il faut procéder autrement pour comparer leur φ^* -composante. Soit $\mathcal{U} = \mathbb{Z}_2 \otimes_{\mathbb{Z}} (U/\{\pm 1\})$, et soit $\mathcal{U}_0 \simeq \mathbb{Z}_2$ sur lequel G opère trivialement ; alors le théorème de Dirichlet sur les unités entraîne que l'on a l'isomorphisme de G -modules :

$$\mathbb{Q}_2 \otimes_{\mathbb{Z}_2} (\mathcal{U} \oplus \mathcal{U}_0) \simeq \mathbb{Q}_2[G'].$$

Comme $\mathcal{U} = \bigoplus_{\varphi^1 \neq 1} \mathcal{U}^{e_{\varphi^1}}$, φ^1 parcourant l'ensemble des caractères 2-adiques irréductibles de $k = K_{\psi_0}$, on en déduit $\mathbb{Q}_2 \otimes \mathcal{U}^{e_{\varphi^1}} \simeq \mathbb{Q}_2[G'] e_{\varphi^1}$, pour $\varphi^1 \neq 1$. Appelons encore H le plus grand sous-groupe de G' d'ordre impair, et soit $\Gamma = \text{Gal}(K'/k)$; on a $\mathbb{Q}_2[G'] \simeq \mathbb{Q}_2[H][\Gamma]$ et dans cet isomorphisme on a $\mathbb{Q}_2[G'] e_{\varphi^1} \simeq (\mathbb{Q}_2[H] e_{\varphi^1})[\Gamma]$, en considérant e_{φ^1} comme élément de $\mathbb{Q}_2[H]$; or $\mathbb{Q}_2[H] e_{\varphi^1}$ est un corps de degré $\varphi^1(1)$ sur \mathbb{Q}_2 , par conséquent $\mathbb{Q}_2[G'] e_{\varphi^1}$ est un \mathbb{Q}_2 -espace vectoriel de dimension $|\Gamma| \varphi^1(1)$. Il en résulte que $\mathcal{U}^{e_{\varphi^1}}$ est de \mathbb{Z}_2 -dimension $|\Gamma| \varphi^1(1)$, donc que $(U/U^2)^{e_{\varphi^1}}$ est de \mathbb{F}_2 -dimension $|\Gamma| \varphi^1(1)$; appliqué à $\varphi^1 = \varphi^* \neq 1$ ceci donne le résultat car $\mathbb{F}_2[G'] e_{\varphi^*} \simeq (\mathbb{F}_2[H] e_{\varphi^*})[\Gamma]$ a aussi pour \mathbb{F}_2 -dimension le nombre $|\Gamma| \varphi^*(1)$.

On a donc $|\mathcal{H}| = |(S(K')/S(U))^{e_{\varphi^*}}| |\mathcal{H}'| = |(U^+/U^2)^{e_{\varphi^*}}| |\mathcal{H}'| = |\tilde{\mathcal{W}}_{\infty}| |\mathcal{H}'| / |\text{Im} f| \geq |\tilde{\mathcal{W}}_{\infty}|$; on a donc obtenu universellement les inégalités (même lorsque $\psi_0 = 1$) :

$$|\mathcal{Z}(\varphi_n)| \leq |\mathcal{H}(\bar{\varphi}_n)|, \text{ pour tout } \psi \text{ pair, et tout } n \text{ assez grand.}$$

Soit χ_0 le caractère rationnel au-dessus de ψ_0 ; comme ici θ est d'ordre 2, les sommes $\sum_a \sum_{\psi_0 | \chi_0} \gamma_n^a \psi_p^a \psi_0$ et $\sum_a \sum_{\psi_0 | \chi_0} (\theta \gamma_n^{-1} \psi_p^{-1})^a \psi_0^{-1}$, a parcourant $(\mathbb{Z}/p^n \mathbb{Z})^*$, sont les deux caractères rationnels χ_n et $\bar{\chi}_n$ associés à K et \bar{K} respectivement. Donc les ensembles $\{\varphi'_n | \chi_n\}$ et $\{\bar{\varphi}'_n | \bar{\chi}_n\}$ se correspondent bijectivement, ce qui donne, en faisant le produit

des inégalités précédentes : $\prod_{\phi'_n | \chi_n} |\mathcal{Z}(\phi'_n)| \leq \prod_{\bar{\phi}'_n | \bar{\chi}_n} |\mathcal{H}(\bar{\phi}'_n)|$ soit $|\mathcal{Z}(\chi_n)| \leq |\mathcal{H}(\bar{\chi}_n)|$. On remarque que \bar{K} étant cyclique sur \mathbb{Q} , \bar{K} ne peut contenir μ_4 , d'où en utilisant 3.4 et 3.5 pour les caractères χ_n et $\bar{\chi}_n$, on obtient $v_p(|\mathcal{Z}(\chi_n)|) = v_p\left(\prod_{a, \psi_0} \frac{1}{2} L_2\left(1, \gamma_n^a \psi_p^a \psi_0\right)\right)$, et $v_p(|\mathcal{H}(\bar{\chi}_n)|) = v_p\left(\prod_{a, \psi_0} \frac{1}{2} L_2\left(0, \gamma_n^a \psi_p^a \psi_0\right)\right)$. Les valuations de chacun des seconds membres ci-dessus sont égales (pour n assez grand), et il en résulte les égalités $|\mathcal{Z}(\phi_n)| = |\mathcal{H}(\bar{\phi}_n)|$.

En corollaire, ceci conduit à la surjection de l'application f dans la suite exacte 4.7, d'où la suite exacte :

$$(4.9) \quad 1 \longrightarrow (U^+/U^2)^{\varphi^*} \longrightarrow \tilde{W}_\infty \longrightarrow \mathcal{H}' \longrightarrow 1 \quad (\text{pour } \varphi^* \neq 1).$$

On a donc obtenu le résultat suivant (cité dans [4], th. 5.1) :

(4.10) Soient ψ un caractère abélien pair, θ le caractère de Teichmüller, γ_n un caractère d'ordre p^n de \mathbb{Q}_∞ pour chaque $n \geq 0$, ϕ_n (resp. $\bar{\phi}_n$) le caractère p -adique au-dessus de $\gamma_n \psi$ (resp. $\theta \gamma_n^{-1} \psi^{-1}$). Alors pour tout n assez grand, on a $|\mathcal{H}(\bar{\phi}_n)| = |\mathcal{Z}(\phi_n)|$ sauf dans le cas particulier où $p = 2$, ψ est un caractère d'ordre puissance de 2 non caractère de \mathbb{Q}_∞ , auquel cas $|\mathcal{H}(\bar{\phi}_n)| = 2 |\mathcal{Z}(\phi_n)|$.

Il résulte en particulier du th. 4.2 de [4] que $|\mathcal{H}(\bar{\phi}_n)|$ est constant pour n assez grand et ne dépend que du caractère p -adique $\bar{\phi}$ au-dessus de $\theta \psi^{-1}$; ceci définit un invariant $\bar{\Lambda}(\bar{\phi})$, par $|\mathcal{H}(\bar{\phi}_n)| = p^{\bar{\Lambda}(\bar{\phi})}$, invariant qui est égal à $\Lambda(\phi)$ (sauf dans le cas particulier mentionné, où $\bar{\Lambda}(\bar{\phi}) = \Lambda(\phi) + 1$).

Ceci entraîne une précision sur une conjecture d'Iwasawa que nous avons étudiée dans [4] ($\Lambda(\phi) = \lambda(\phi)$ pour ϕ non caractère de \mathbb{Q}_∞), et dont nous avons montré qu'elle se ramenait au cas des caractères ϕ issus de caractères ψ d'ordre premier à p : en effet, un cas trivial d'exactitude de la conjecture est celui où le caractère p -adique ϕ est rationnel (dans ce cas ϕ_n est aussi rationnel, et on applique la formule 3.4) ; le théorème ci-dessus

entraîne que la conjecture $\Lambda(\phi) = \lambda(\phi)$ (ϕ non caractère de \mathbb{Q}_∞) est vraie dès que l'un au moins des caractères ϕ ou $\bar{\phi}$ est rationnel (dans le second cas, $\bar{\phi}_n$ est aussi rationnel et on utilise cette fois la formule 3.5). Par exemple, le cas le plus simple d'application effective de ce résultat est le suivant : $p = 5$, et ϕ ou $\bar{\phi}$ est un caractère 5-adique issu d'un caractère d'ordre 4.

Compléments sur le cas $p = 2$: le cas $\psi_0 = 1$.

Nous avons comparé analytiquement les ordres de ζ et \mathcal{H} lorsque $\psi_0 = 1$ (i. e. $\varphi = \varphi^* = 1$). Nous allons ici adapter à ce cas les méthodes précédentes pour établir des relations algébriques analogues, et notamment pour interpréter le facteur 2.

Nous supposons ψ (d'ordre puissance de 2) non caractère de \mathbb{Q}_∞ (sinon on a $\zeta = \mathcal{H} = (1)$).

Ici $\tilde{w}_\infty = w_\infty / L_\infty^2$ est annulé par $1+s$. On a toujours le fait que tout élément \tilde{w} de \tilde{w}_∞ a un représentant w_0 dans K totalement positif, et le fait que pour tout $w \in w_\infty \cap \bar{K}$, $w^{1+s} = a_+^2$, $a_+ \in K'$, $a_+ \gg 0$. On peut préciser ici 4.2 de la façon suivante : comme $\psi \neq 1$, on a $\mathbb{Q}_\infty \cap K \subset K'$; soit r minimum tel que ψ^{2^r} soit caractère de \mathbb{Q}_∞ ($r \geq 1$), on a $\mathbb{Q}_\infty \cap K = \mathbb{Q}_{n-r}$ et on a $\mu_L = \mu_{4.2^{n-r}} \subset L'$. Soit alors ζ_1 une racine de l'unité d'ordre 4.2^{n-r} (ζ_1 engendre μ_L), et soit $w_1 = -\zeta_1^{-1}(1-\zeta_1)^2$. On a $w_1 = 2 - (\zeta_1^{-1} + \zeta_1)$ qui est donc, dans \mathbb{Q}_{n-r} , une uniformisante en 2 totalement positive. Soit $\alpha \in L \cap L_\infty^2$; alors $\alpha = \zeta u^2$, $\zeta \in \mu_L$, $u \in L$, et $\zeta = \zeta_1^\lambda$ ($\lambda \in \mathbb{Z}$) soit $\alpha = \zeta_1^\lambda u^2 = (-w_1^{-1})^\lambda (1-\zeta_1)^{2\lambda} u^2$, ce qui s'écrit encore $\alpha = w_1^\delta v^2$, $v \in L$, $\delta = 0$ ou 1 .

Supposons maintenant que $\alpha \in K$, alors $\alpha w_1^{-\delta} = v^2 \in K$; si $v \notin K$, $L = K(v)$ est kummerienne, et comme $L = K(\sqrt{-1})$, il vient $v^2 = -a^2$, $a \in K$, et, dans tous les cas, $\alpha = \pm w_1^\delta a^2$, $a \in K$.

On a le même raisonnement en remplaçant K par \bar{K} :

$$(4.11) \quad K \cap L_\infty^2 = \langle -1, w_1 \rangle K^2 \quad \text{et} \quad \bar{K} \cap L_\infty^2 = \langle -1, w_1 \rangle \bar{K}^2.$$

On désigne encore par \mathcal{H}' le sous-groupe de \mathcal{H} formé des classes des idéaux \mathfrak{a} de \bar{K} tels que $\bar{N}\mathfrak{a}$ soit principal au sens restreint dans K' , et par $\mathcal{W}' = \{w \in \mathcal{W}'_\infty \cap \bar{K}, w\mathcal{O}_{\bar{K}} = \mathfrak{a}^2 \text{ dans } \bar{K}\}$. On conserve les notations du § 4, (ii); en particulier f est l'application de \mathcal{W}' dans \mathcal{H}' qui à w associe la classe de \mathfrak{a} dans \bar{K} , g est l'application qui à $w \in \mathcal{W}'$ associe \tilde{w} dans $\tilde{\mathcal{W}}'_\infty$.

On peut maintenant étudier f et g .

Noyau de f . Si $w\mathcal{O}_{\bar{K}} = \mathfrak{a}^2$, avec $\mathfrak{a} = a\mathcal{O}_{\bar{K}}$, $a \in \bar{K}$, alors $w = a^2 \epsilon$, ϵ unité de \bar{K} (donc $\epsilon \in U$). Soit $w_0 \in K$ un représentant totalement positif de $\tilde{w} = \tilde{\epsilon}$; on a $\tilde{\epsilon} = \tilde{w}_0$ soit $\epsilon w_0^{-1} \in K \cap L_\infty^2$ soit, d'après 4.11, $\epsilon w_0^{-1} = \pm w_1^\delta b^2$, $b \in K$, $\delta = 0$ ou 1 ; ceci implique $\pm \epsilon \in U^+$ et $w = \epsilon a^2 \in \{\pm 1\} U^+ \bar{K}^2$. Il est clair que ceci est bien le noyau.

Noyau de g . D'après 4.11, c'est $\langle -1, w_1 \rangle \bar{K}^2$.

Image de g . Soit $\tilde{w} \in \tilde{\mathcal{W}}'_\infty$ représenté par $w \gg 0$ de K . On a $w^{1+s} \in K' \cap L_\infty^2$, donc, d'après 4.11, $w^{1+s} = w_1^\delta a^2$, $a \in K$ (on a le signe $+$ car on a $w^{1+s} \gg 0$), $\delta = 0$ ou 1 . Si $a \notin K'$, comme $a^2 \in K'$, $K = K'(a)$ serait kummerienne. Montrons qu'elle serait 2-ramifiée: dans K' on a $(a^2)\mathcal{O}_{K'} = (Nw w_1^{-\delta})\mathcal{O}_{K'}$; or l'extension $K(\sqrt{w})$ est 2-ramifiée par hypothèse ($L_\infty(\sqrt{w})/L_\infty$ l'est par définition, et L_∞/K est aussi 2-ramifiée), donc $w\mathcal{O}_K = a^2 \mathfrak{p}$, dans K , où \mathfrak{p} est un 2-idéal de K , soit $Nw\mathcal{O}_{K'} = (Na)^2 N\mathfrak{p}$; ceci conduit bien à K/K' 2-ramifiée, ce qui est exclu. Donc $a \in K'$ et $w^{1+s} = w_1^\delta a^2$, $a \in K'$.

Supposons $\delta = 1$; alors on peut écrire $N(wa^{-1}) = w_1$ dans K/K' , soit, dans L/L' , $N(wa^{-1}) = -\zeta_1(1 - \zeta_1)^2$; comme $1 - \zeta_1 \in L'$ il vient $N(wa^{-1}(1 - \zeta_1)^{-1} \sqrt{-1}) = \zeta_1$ dans L/L' . Montrons que pour n assez grand ζ_1 ne peut être norme dans L/L' en calculant le symbole de Hilbert $(\omega, \zeta_1)_l$, où ω et l sont ainsi définis: ω est un élément du radical de L/L'

$(L = L'(\sqrt{\omega}), \omega \in L')$; l est un idéal premier de L' au-dessus d'un nombre premier $\ell \neq 2$ totalement ramifié dans K/\mathbb{Q}_{n-r} (ce qui existe puisque K/\mathbb{Q} est cyclique et non contenue dans \mathbb{Q}_∞).

On sait que $\omega \mathcal{O}_{L'}^l$ est divisible par une puissance impaire de l ;

il en résulte que $(\omega, \zeta_1)_l = \zeta_1^{(\ell^k - 1)/2}$, où k est le degré résiduel de ℓ dans L'/\mathbb{Q} . Posons $\ell \theta^{-1}(\ell) = 1 + 4 \cdot 2^{n(\ell)} u$, u impair ; le degré résiduel de ℓ dans L'/\mathbb{Q} est donc égal à celui de ℓ dans $\mathbb{Q}(\mu_{4 \cdot 2^{n-r}})/\mathbb{Q}$, soit $k = 2^{n-r-n(\ell)}$

(n toujours supposé assez grand), d'où $\frac{\ell^k - 1}{2} = \frac{4 \cdot 2^{n(\ell) + n - r - n(\ell)} u}{2} = 2 \cdot 2^{n-r} u$ et $\zeta_1^{(\ell^k - 1)/2} = -1$, d'où le fait que ζ_1 ne peut être norme. On a donc nécessairement $\delta = 0$, soit $w^{1+s} = a^2$, $a \in K'$.

On a donc $(\frac{w}{a})^{1+\sigma_\infty s} = (\frac{w}{a})^{1+s} = 1$, donc $\frac{w}{a} = c^{1-\sigma_\infty s}$ avec $c \in L$;

alors $(\frac{w}{c^2})^{\sigma_\infty s} = \frac{w^s}{2^{\sigma_\infty s}} = \frac{w^{-1} a^2 w^2}{c^2 a^2} = \frac{w}{c^2}$ qui est donc dans \bar{K} . Le repré-

sentant $w' = \frac{w}{c^2}$ de \tilde{w} est dans \mathcal{W}^* : en effet, $w' \in \mathcal{W}_\infty^* \cap \bar{K}$. Reste à vérifier que

$w' \mathcal{O}_{\bar{K}}$ est carré d'un idéal. On a $\bar{K}(\sqrt{w'})/\bar{K}$ qui est 2-ramifiée ($L_\infty(\sqrt{w'})/L_\infty$ l'est par hypothèse, et L_∞/\bar{K} est aussi 2-ramifiée), donc $w' \mathcal{O}_{\bar{K}} = a^2 \mathfrak{p}$

(\mathfrak{p} 2-idéal de \bar{K}) ; d'où $w'^{1+s} \mathcal{O}_{K'} = (\bar{N} a)^2 \bar{N} \mathfrak{p}$; or $w' \in \mathcal{W}^* \cap \bar{K}$ entraîne $w'^{1+s} = a_+^2$, $a_+ \in K'$, donc $\bar{N} \mathfrak{p}$ est un carré de 2-idéal dans K' ; comme K/K' est ramifiée en 2, ceci entraîne $\mathfrak{p} = \mathfrak{q}^2$ dans \bar{K} .

On a montré la surjectivité de g pour n assez grand.

On a donc les suites exactes :

$$1 \longrightarrow \{\pm 1\} u^+ \bar{K}^2 \longrightarrow \mathcal{W}^* \xrightarrow{f} \mathcal{H}^1$$

$$1 \longrightarrow \langle -1, w_1 \rangle \bar{K}^2 \longrightarrow \mathcal{W}^* \xrightarrow{g} \tilde{\mathcal{W}}_\infty \longrightarrow 1,$$

qui conduisent aux suivantes :

$$1 \longrightarrow u^+ / u^2 \longrightarrow \mathcal{W}^* / \{\pm 1\} \bar{K}^2 \xrightarrow{f} \mathcal{H}^1$$

$$1 \longrightarrow \langle w_1 \rangle / \{\pm 1\} \bar{K}^2 \cap \langle w_1 \rangle \longrightarrow \mathcal{W}^* / \{\pm 1\} \bar{K}^2 \xrightarrow{g} \tilde{\mathcal{W}}_\infty \longrightarrow 1.$$

Si $w_1 \in \{\pm 1\} \bar{K}^2$, $w_1 = \pm a^2$, $a \in \bar{K}$; nécessairement on a $a \in K'$ sinon on aurait $\bar{K} = K'(\sqrt{\pm w_1})$, ce qui est absurde; donc $w_1 = b^2$, $b \in K'$ ($w_1 \gg 0$ conduit au signe +). Comme w_1 n'est pas un carré dans \mathbb{Q}_{n-r} , $\mathbb{Q}_{n-r}(b)$ est une extension quadratique de \mathbb{Q}_{n-r} contenue dans K' ; étant 2-ramifiée sur \mathbb{Q}_{n-r} et cyclique sur \mathbb{Q} , elle ne peut être que \mathbb{Q}_{n+1-r} , ce qui est absurde. Donc $\{\pm 1\} \bar{K}^2 \cap \langle w_1 \rangle = \langle w_1^2 \rangle$. D'où la suite exacte :

$$1 \longrightarrow \langle w_1 \rangle / \langle w_1^2 \rangle \longrightarrow \mathcal{W} / \{\pm 1\} \bar{K}^2 \xrightarrow{g} \tilde{\mathcal{W}}_\infty \longrightarrow 1.$$

$$\text{On a donc } |\mathcal{C}| = |\tilde{\mathcal{W}}_\infty| = \frac{(\mathcal{W} : \{\pm 1\} \bar{K}^2)}{2} = \frac{(U^+ : U^2) |\text{Im} f|}{2}.$$

On a toujours les suites exactes :

$$1 \longrightarrow \mathcal{H}' \longrightarrow \mathcal{H} \longrightarrow SK'/SU \longrightarrow 1,$$

$$1 \longrightarrow U^+/U^2 \longrightarrow U/U^2 \longrightarrow SU \longrightarrow 1,$$

et l'égalité $(SK' : SU) = (U^+ : U^2)$, d'où :

$$|\mathcal{C}| = \frac{(U^+ : U^2) |\mathcal{H}'|}{2(\mathcal{H}' : \text{Im} f)} = \frac{|\mathcal{H}|}{2(\mathcal{H}' : \text{Im} f)}.$$

Le résultat analytique du § 4 entraîne alors $\text{Im} f = \mathcal{H}'$ dès que n est assez grand.

Interprétation arithmétique du coefficient 2 dans $|\mathcal{H}| = 2|\mathcal{C}|$. On démontre facilement que les conditions suivantes sont équivalentes :

(i) $f(w_1) = 1$ (i. e. dans l'écriture $w_1 \mathcal{O}_{\bar{K}} = \mathfrak{p}^2$, \mathfrak{p} 2-idéal de \bar{K} , \mathfrak{p} est principal).

(ii) l'indice des unités $Q(L')$ est égal à 2 :

En effet, comme 2 est ramifié dans \bar{K}/K' , on a bien $w_1 \mathcal{O}_{\bar{K}} = \mathfrak{p}^2$, où \mathfrak{p} est un 2-idéal de \bar{K} : ceci justifie le fait que $w_1 \in \mathcal{W}$; si on suppose $f(w_1) = 1$, c'est que \mathfrak{p} est principal dans \bar{K} : on a $\mathfrak{p} = \pi \mathcal{O}_{\bar{K}}$, $\pi \in \bar{K}$, et $w_1 = \pi^2 \varepsilon$, ε unité de \bar{K} (donc $\varepsilon \in U$); comme $\pi^2 = w_1 \varepsilon^{-1} \in K'$, $\pi \in K'$ sinon \bar{K}/K' serait 2-ramifiée; donc $w_1 = \varepsilon \pi^2$, $\pi \in K'$. Il en résulte que dans L' on peut écrire $-\zeta_1^{-1}(1 - \zeta_1)^2 = \varepsilon \pi^2$, soit, de façon évidente, puis-

que -1 est un carré : $\epsilon = \zeta_1 \gamma^2$, $\gamma \in L'$; γ est donc une unité de L' , et si on suppose $Q(L') = 1$, il existe $\xi \in \mu_{L'}$, $\eta \in U$, tels que $\gamma = \xi \eta$ soit $\epsilon = \zeta_1 \xi^2 \eta^2$, soit $\zeta_1 \xi^2 \in K'$, ce qui est absurde car ζ_1 est un générateur de $\mu_{L'}$, et $\zeta_1 \xi^2$ est toujours d'ordre $4 \cdot 2^{n-r}$. D'où $Q(L') = 2$.

Inversement, si $Q(L') = 2$, alors il existe une unité γ de L' , et $\xi \in \mu_{L'}$, tels que $\gamma \notin \mu_{L'} U$ et $\xi \gamma^2 \in U$. Posons $\epsilon = \xi \gamma^2$; on a $\xi = \zeta_1^\lambda$ avec λ impair sinon ϵ serait un carré dans L' et il en résulterait $\epsilon = \pm \eta^2$, $\eta \in U$, soit encore $\eta = \xi' \gamma$, $\xi' \in \mu_{L'}$, ce qui n'est pas. On a donc $\epsilon = \zeta_1 \alpha^2$, α unité de L , et ceci conduit à $\epsilon = w_1 u^2$ dans L' soit à $\epsilon = \pm w_1 v^2$, $v \in K'$, et $w_1 \mathcal{O}_{\bar{K}}$ est, a fortiori, le carré d'un idéal principal de \bar{K} .

Considérons alors les deux éventualités :

(i) $w_1 \mathcal{O}_{\bar{K}} = \mathfrak{p}^2$, \mathfrak{p} non principal dans \bar{K} . On a donc la classe de \mathfrak{p} qui contribue à \mathcal{H}' tandis que w_1 ne donne aucune contribution correspondante à \mathcal{C} puisque $\tilde{w}_1 = \tilde{1}$.

(ii) $w_1 \mathcal{O}_{\bar{K}} = \mathfrak{p}^2$, \mathfrak{p} principal dans \bar{K} . Dans ce cas on sait que $Q(L') = 2$, et, d'après les calculs ci-dessus, il existe une unité $\epsilon \in U^+ \setminus U^2$ qui est, dans L' , de la forme $\xi \alpha^2$, donc carré dans L_∞ . Donc, alors que normalement U^+/U^2 contribue toujours non trivialement à \mathcal{C} , ici il y a un défaut de contribution représenté par cette unité de U^+ qui devient un carré dans L_∞ .

Conclusion.

Les résultats obtenus dans le cas $p = 2$ (ψ non caractère de \mathbb{Q}_∞) montrent quels sont les éléments à introduire pour étudier les groupes $\mathcal{H}(\bar{K})$ et $\mathcal{C}(K)$ en termes de théorie d'Iwasawa, par comparaison avec le cas $p \neq 2$ bien connu. Rappelons à cet effet les suites exactes de G -modules et relations obtenues (Sp indique que les G -structures sont reliées par la "Spiegelungsrelation") :

(i) Cas $p \neq 2$:

$$\begin{aligned} 1 &\longrightarrow \mathcal{C} \longrightarrow \mathcal{C}(K) \xrightarrow{A} \mathcal{C}(K)^A \longrightarrow 1, \\ \mathcal{C}(K)/\mathcal{C}(K)^A &\xleftarrow{Sp} \tilde{W}_\infty, \\ 1 &\longrightarrow \tilde{W}_\infty \longrightarrow \mathcal{H} \longrightarrow 1. \end{aligned}$$

(ii) Cas $p = 2, \varphi, \varphi^* \neq 1$:

$$\begin{aligned} 1 &\longrightarrow \mathcal{C} \longrightarrow \mathcal{C}(K) \xrightarrow{A} \mathcal{C}(K)^A \longrightarrow 1, \\ \mathcal{C}(K)/\mathcal{C}(K)^A &\xleftarrow{Sp} \tilde{W}_\infty, \\ 1 &\longrightarrow (u^+/u^2)^{e\varphi^*} \longrightarrow \tilde{W}_\infty \longrightarrow \mathcal{H}' \longrightarrow 1, \\ 1 &\longrightarrow \mathcal{H}' \longrightarrow \mathcal{H} \longrightarrow (SK'/SU)^{e\varphi^*} \longrightarrow 1, \\ 1 &\longrightarrow (u^+/u^2)^{e\varphi^*} \longrightarrow (u/u^2)^{e\varphi^*} \longrightarrow (SU)^{e\varphi^*} \longrightarrow 1. \end{aligned}$$

(iii) Cas $p = 2, \varphi = \varphi^* = 1$:

$$\begin{aligned} 1 &\longrightarrow \mathcal{C} \longrightarrow \mathcal{C}(K) \xrightarrow{A} \mathcal{C}(K)^A \longrightarrow 1, \\ \mathcal{C}(K)/\mathcal{C}(K)^A &\xleftarrow{Sp} \tilde{W}_\infty, \\ 1 &\longrightarrow \langle w_1 \rangle / \langle w_1^2 \rangle \longrightarrow \mathcal{W} / \{\pm 1\} \bar{K}^2 \longrightarrow \tilde{W}_\infty \longrightarrow 1, \\ 1 &\longrightarrow u^+/u^2 \longrightarrow \mathcal{W} / \{\pm 1\} \bar{K}^2 \longrightarrow \mathcal{H}' \longrightarrow 1, \\ 1 &\longrightarrow \mathcal{H}' \longrightarrow \mathcal{H} \longrightarrow SK'/SU \longrightarrow 1, \\ 1 &\longrightarrow u^+/u^2 \longrightarrow u/u^2 \longrightarrow SU \longrightarrow 1. \end{aligned}$$

BIBLIOGRAPHIE

=====

- [1] Coates J., p -adic L -functions and Iwasawa's theory, Proc. of Durham Symposium (1975).
- [2] Gras G., Etude d'invariants relatifs aux groupes des classes des corps abéliens, Astérisque 41-42 (1977).
- [3] Gras G., Sur la construction des fonctions L p -adiques abéliennes, Sémin. Delange-Pisot-Poitou (1978-79), exposé du 19 Mars 1979.
- [4] Gras G., Module de torsion de la p -extension abélienne p -ramifiée maximale d'un corps abélien réel, et fonctions L p -adiques, (à paraître).
- [5] Hasse H., Über die Klassenzahl abelscher Zahlkörper, Akad. Verlag Berlin (1952).
- [6] Kida Y., On cyclotomic \mathbb{Z}_2 -extensions of imaginary quadratic fields, Tôhoku Math. J. 31 (1979).
- [7] Kida Y., ℓ -Extensions of CM-Fields and Cyclotomic Invariants, (à paraître).
- [8] Leopoldt H.-W., Zur Struktur der ℓ -Klassengruppe galoischer Zahlkörper, Journ. für die reine und ang. Math. 199 (1958).
- [9] Oriat B., et Satgé P., Un essai de généralisation du "Spiegelungssatz", Journ. für die reine und ang. Math. 307 (1979).

- [10] Ribet K., p -adic L -functions attached to characters of p -power order, Sém. Delange-Pisot-Poitou 9 (1977-78).

Georges GRAS
Faculté des Sciences
Mathématiques
25030 BESANCON CEDEX
FRANCE