THEORIE DES NOMBRES

BESANCON

Année 1978 - 1979

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

Georges GRAS

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 $\mathcal{T}(K)$ 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 $\mathcal{H}(K)$ 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 $a\theta^{-1}(a) \equiv 1 \bmod q$, pour tout a premier à p. On désigne par $\mathbb{Q}_\infty = \bigcup_{n \geq 0} \mathbb{Q}_n \left([\mathbb{Q}_n : \mathbb{Q}] = p^n\right)$ la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$, par $K_\infty = \bigcup_{n \geq 0} K_n \left(K_n = K\mathbb{Q}_n\right)$ celle de K, et par $\left(\gamma_n\right)_{n \geq 0}$ une famille de caractères de $\mathbb{Q}_\infty$, 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 $\Lambda(K), \overline{\Lambda}(K)$.

Rappel des formules analytiques.

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

(1.1) $|\mathcal{T}(K)| \approx p^{n_o(K)} \prod_{\alpha \neq 1} \frac{1}{2} L_p(1,\alpha)$, α parcourant l'ensemble des caractères de Dirichlet primitifs pairs $\neq 1$ de K, et où $p^{n_o(K)} = [K \cap \mathbb{Q}_\infty : \mathbb{Q}]$ (cf. [1], Appendix I, lemme 8 ; voir aussi [4], th. 2.1).

(1.2) $|\mathcal{H}(K)| \approx p^{m_o(K)} \prod_{\beta} -\frac{1}{2} B_1(\beta^{-1})$, où β 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) :

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

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 :

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

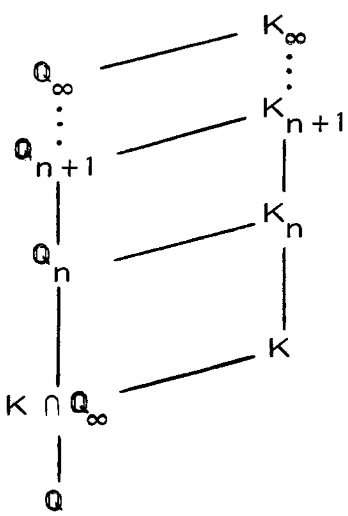
(1.3) $\quad -\frac{1}{2}B_1(\beta^{-1}) = \frac{1}{2}L_p(0,\theta\beta^{-1})$ si p divise le conducteur du caractère primitif impair β.

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

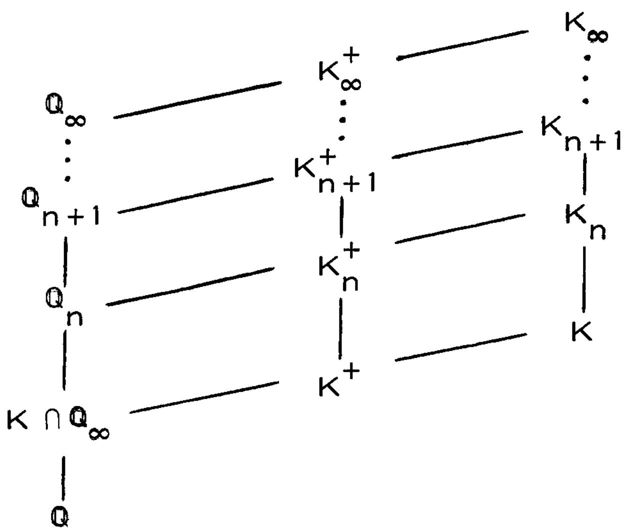
Soit ψ un caractère pair ; considérons les caractères $\gamma_n\psi$, pour tout $n \geq 0$; dans ce cas on sait que la valuation de $\frac{1}{2}L_p(s,\gamma_n\psi)$ (calculée dans $\mathbb{Z}_p(\gamma_n\psi)$) est, pour n assez grand, une constante $\lambda(\psi)$ qui ne dépend que de ψ, et non du choix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

<u>Formules d'Iwasawa.</u>

Considérons les schémas suivants :



<u>cas réel</u>



<u>cas imaginaire</u>

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) <u>K est réel</u> (cf. [4], prop. 4.1).

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

$\dfrac{|\mathcal{T}(K_{n+1})|}{|\mathcal{T}(K_n)|} \approx p \prod_{a,\psi} \frac{1}{2} L_p(1, \gamma_n^a \psi)$, $a \in (\mathbb{Z}/p^n\mathbb{Z})^*$, $\psi \in \tilde{\Psi}_K$, d'où, si l'on pose $\dfrac{|\mathcal{T}(K_{n+1})|}{|\mathcal{T}(K_n)|} = p^{\Lambda_n(K)}$, 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 $\mathcal{T}$ dans K_∞ :

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

(ii) <u>K est imaginaire</u>.

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

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

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

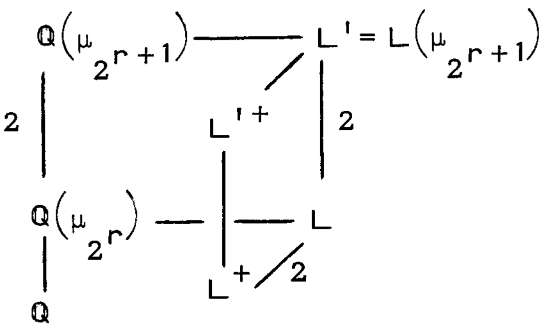
Il y a deux cas : ou bien $\mu_q \subset K_\infty$, ou bien $\mu_q \not\subset K_\infty$. Dans le premier cas, K_∞ contient $\bigcup_{n\geq 0} \mathbb{Q}\left(\mu_{qp^n}\right)$, dans le second cas, K_∞ ne contient pas de racines de l'unité d'ordre une puissance de p autres que 1 (resp. ± 1) dans le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

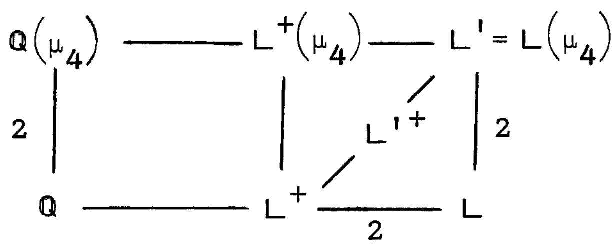
Dans le second cas, on a $W\left(K_{n+1}\right) = W\left(K_n\right)$ pour tout n assez grand.

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 $L' = L\left(\mu_{2^{r+1}}\right)$ 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 $\left(\text{i. e. s'il existe une unité } \varepsilon \in L^+ \text{ telle que } L'^+ = L^+(\sqrt{\varepsilon})\right)$.

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

α) <u>Cas où</u> $\mu_4 \subset K_\infty$.

On a le schéma suivant (compte tenu du fait qu'ici, pour n assez grand, $L = K_n$ contient $\mu_{4.2^n}$ et non $\mu_{4.2^{n+1}}$, et que $L' = L\left(\mu_{4.2^{n+1}}\right) = K_{n+1}$) :

$$\begin{tikzcd}
 & \mathbb{Q}_{n+1}(\mu_4) \arrow[rr, dash] \arrow[dd, dash] & & K_{n+1} = L' \arrow[dd, dash, "2"] \\
\mathbb{Q}_{n+1} \arrow[ur, dash, "2"] \arrow[rr, dash] \arrow[dd, dash, "2"'] & & K^+_{n+1} \arrow[ur, dash, "2"'] \arrow[dd, dash] & \\
 & \mathbb{Q}_n(\mu_4) \arrow[rr, dash] & & K_n = L \\
\mathbb{Q}_n \arrow[ur, dash, "2"] \arrow[rr, dash] & & K^+_n \arrow[ur, dash, "2"'] &
\end{tikzcd}$$

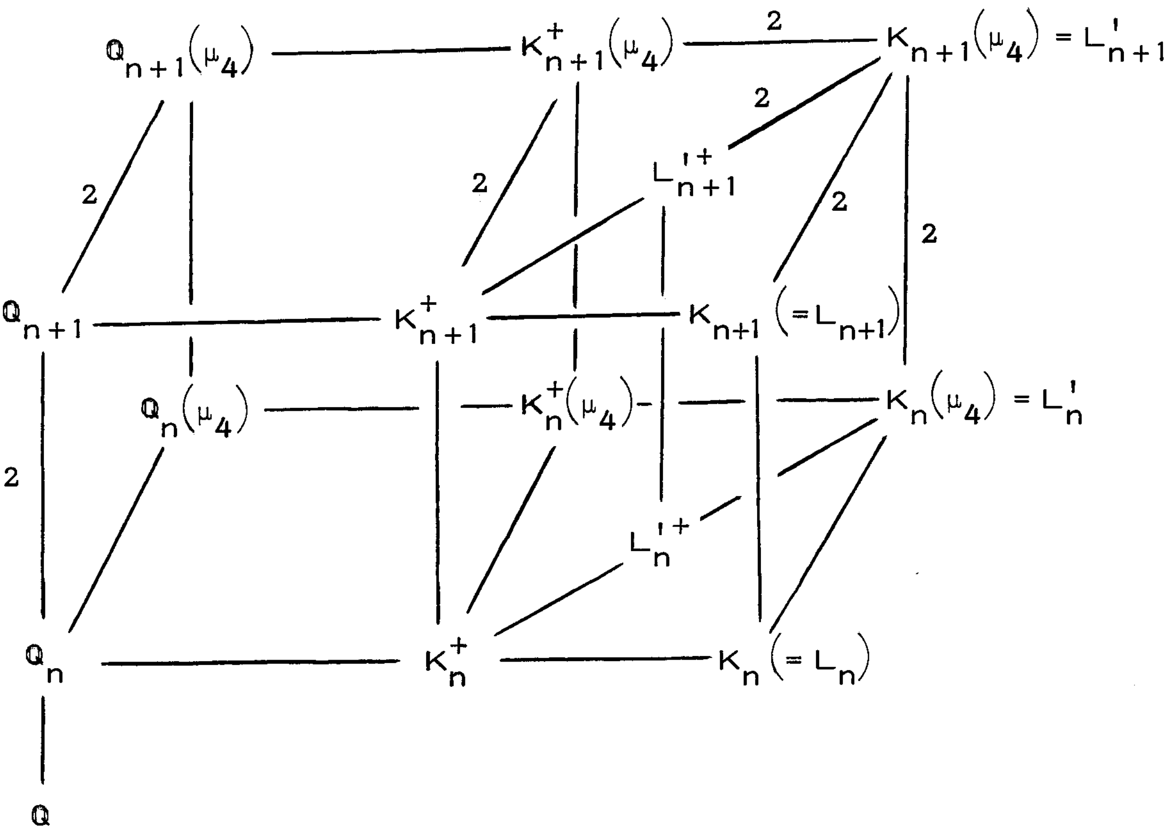
Il est bien connu que $\mathbb{Q}_{n+1} = \mathbb{Q}_n\left(\sqrt{\pi_n}\right)$, où π_n engendre l'idéal premier $\mathfrak{p}_n$ au-dessus de 2 dans $\mathbb{Q}_n$; on a donc $K^+_{n+1} = K^+_n\left(\sqrt{\pi_n}\right)$. Comme pour n assez grand 2 est ramifié dans K^+_{n+1}/K^+_n, et non ramifié dans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

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

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

β) <u>Cas où</u> $\mu_4 \not\subset K_\infty$.

Dans ce cas on a $\mu_4 \not\subset K_n$ pour tout n ; on a le schéma suivant :



Le critère de Hasse repose donc sur l'étude des extensions L'^+_n/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 $L'^+_n = K^+_n(\sqrt{-\alpha})$. Si pour un entier n_1 on a $-\alpha = \varepsilon_{n_1} u^2_{n_1}$,

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.

On a donc $\dfrac{|\mathcal{H}(K_{n+1})|}{|\mathcal{H}(K_n)|} \approx p^{\rho(K)} \prod_{\beta_{n+1}} \frac{1}{2} B_1(\beta^{-1}_{n+1})$, où $\rho(K) = 1$ 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 $\gamma^a_n\, \psi'$, $a \in (\mathbb{Z}/p^n\,\mathbb{Z})^*$, ψ' parcourant l'ensemble, noté $\widetilde{\Psi}^-_K$, des caractères impairs de $\widetilde{\Psi}_K$ ($\widetilde{\Psi}_K$ désignant comme précédemment un système exact de représentants de $\Psi_K/\Psi_{K \cap \mathbb{Q}_\infty}$) ; le résultat ne dépend pas du choix de $\widetilde{\Psi}_K$ car $\Psi_{K \cap \mathbb{Q}_\infty}$ est constitué de caractères pairs.

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

On a alors $\dfrac{|\mathcal{H}(K_{n+1})|}{|\mathcal{H}(K_n)|} = p^{\rho(K)} \prod_{b,\psi} \frac{1}{2} L_p(0, \gamma^b_n\, \psi)$, $b \in (\mathbb{Z}/p^n\,\mathbb{Z})^*$, $\psi \in \mathcal{M}(\widetilde{\Psi}^-_K)$, d'où, en posant $\dfrac{|\mathcal{H}(K_{n+1})|}{|\mathcal{H}(K_n)|} = p^{\overline{\lambda}_n(K)}$, pour tout n assez grand $\overline{\lambda}_n(K) = \overline{\lambda}(K)$ est indépendant de n, et on a :

(1.6) $\quad \overline{\lambda}(K) = \rho(K) + \sum_{\psi} \lambda(\psi)$, $\psi \in \mathcal{M}(\widetilde{\Psi}^-_K)$, et où $\rho(K) = 1$ ou 0 selon que K_∞ contient ou non μ_q.

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

(1.7) $\quad |\mathcal{H}(K_n)| = p^{\overline{\lambda}(K)n + \overline{c}}$, pour tout n assez grand, $\overline{c}$ 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 $\mathfrak{M}\left(\tilde{\Psi}_K^-\right) = \tilde{\Psi}_{K^+}$; il s'en suit que dans ce cas on a :

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

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

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

(1.8) Si $\mu_q \subset K$, alors $\Lambda\left(K^+\right) = \overline{\Lambda}(K)$.

On voit aussi que le cas général est inadéquat pour comparer Λ et $\overline{\Lambda}$; 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 $\Lambda(K)$ $\left(\text{resp. } \overline{\Lambda}(K)\right)$ dans le cas réel (resp. imaginaire) mais des invariants $\Lambda(\phi)$ $\left(\text{resp. } \overline{\Lambda}(\phi)\right)$, qui sont des termes convenables de $\Lambda(K)$ $\left(\text{resp. } \overline{\Lambda}(K)\right)$, 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 $\overline{\Lambda}$ 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 $\Lambda(L)$ $\left(\text{resp. } \overline{\Lambda}(M) \text{ et } \overline{\Lambda}(L)\right)$ 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 $p^{n_0} = [K \cap \mathbb{Q}_\infty : \mathbb{Q}]$) :

$$\begin{tikzcd}
\mathbb{Q}_\infty & K \arrow[r, dash] \arrow[d, dash] & L \arrow[dd, dash] \\
 & K \cap \mathbb{Q}_\infty \arrow[ul, dash] \arrow[d, dash] & \\
 & \mathbb{Q} \arrow[r, dash] & k
\end{tikzcd}$$

cas réel

$$\begin{tikzcd}
\mathbb{Q}_\infty & K \arrow[r, dash] \arrow[d, dash] & L^+ \arrow[r, dash] \arrow[dd, dash] & L \arrow[dd, dash] \\
 & K \cap \mathbb{Q}_\infty \arrow[ul, dash] \arrow[d, dash] & & \\
 & \mathbb{Q} \arrow[r, dash] & k^+ \arrow[r, dash] & k
\end{tikzcd}$$

cas imaginaire
($p \neq 2$)

$$\begin{tikzcd}
 & K \arrow[r, dash] \arrow[d, dash] & L \arrow[d, dash] \\
\mathbb{Q}_\infty & K^+ \arrow[r, dash] \arrow[d, dash] & L^+ \arrow[dd, dash] \\
 & K \cap \mathbb{Q}_\infty \arrow[ul, dash] \arrow[d, dash] & \\
 & \mathbb{Q} \arrow[r, dash] & k
\end{tikzcd}$$

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 $\ell \equiv 1 \bmod p$, d'où : la condition sur $\theta\psi_o^{-1}(\ell)$ équivaut à $\psi_o(\ell) = 1$ (i.e. ℓ totalement décomposé dans $K_{\psi_o} \subset k$).

On a $\Lambda(L) = 1 + \sum_{\psi_p, \psi_o} \left(\lambda(\psi_o) + \sum_\ell p^{n(\ell)}\right)$

$$= 1 + \frac{[K:\mathbb{Q}]}{p^{n_o}} \sum_{\psi_o} \lambda(\psi_o) + \sum_{\psi_p, \psi_o} \sum_\ell p^{n(\ell)}, \quad \psi_p \in \tilde{\Psi}_K, \ \psi_o \in \Psi_k ;$$

posons $a(\ell) = \left| \{\psi \in \tilde{\Psi}_K \times \Psi_k, \ \ell \mid f_{\psi_p}, \ \psi_o(\ell) = 1\} \right|$ et remarquons que $\Lambda(k) = 1 + \sum_{\psi_o} \lambda(\psi_o)$, $\psi_o \in \Psi_k$; alors :

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

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

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

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) :

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

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.

<u>Remarque</u>. Si M/L est non ramifiée en dehors de p, alors on obtient $\Lambda(M) - 1 = \frac{[M : L]}{[M \cap \mathbb{Q}_\infty : L \cap \mathbb{Q}_\infty]} \big(\Lambda(L) - 1\big)$; donc en général $\big($i.e. lorsque $[M \cap \mathbb{Q}_\infty : L \cap \mathbb{Q}_\infty] = [M : L]\big)$, 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) <u>Cas imaginaire ($p \neq 2$)</u>.

D'après 1.6 on a $\overline{\Lambda}(L) = \rho(L) + \sum_{\psi} \lambda(\psi)$, ψ parcourant $\mathcal{M}(\widetilde{\Psi}_L^-)$, soit $\overline{\Lambda}(L) = \rho(L) + \sum_{\psi'} \lambda\big(\theta\, \psi'^{-1}\big)$, ψ' parcourant $\widetilde{\Psi}_L^-$. On a $\widetilde{\Psi}_L^- = \big(\widetilde{\Psi}_K \times \Psi_k\big)^- = \widetilde{\Psi}_K \times \Psi_k^-$, donc

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

$\psi'_p \in \widetilde{\Psi}_K$, $\psi'_o \in \Psi^-_k$, et où la dernière sommation est étendue aux premiers $\ell \neq p$ tels que $\ell \mid f_{\psi'_p}$, $\theta\left(\theta^{-1}\, \psi'_o\right)(\ell) = \psi'_o(\ell)$ soit une racine de l'unité d'ordre puissance de p, soit $\psi'_o(\ell) = 1$. On obtient alors

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

$a(\ell) = \left|\left\{\psi' \in \widetilde{\Psi}_K \times \Psi^-_k,\ \ell \mid f_{\psi'_p},\ \psi'_o(\ell) = 1\right\}\right|$. Comme, d'après **1.6**,

$\overline{\Lambda}(k) = \rho(k) + \sum_{\psi'_o} \lambda\left(\theta\, \psi'^{-1}_o\right)$, $\psi'_o \in \Psi^-_k$, il vient

$\overline{\Lambda}(L) = \rho(L) + \dfrac{[K:\mathbb{Q}]}{p^{n_o}} \left(\overline{\Lambda}(k) - \rho(k)\right) + \sum_{\ell \neq p} p^{n(\ell)}\, a(\ell)$. Le calcul de $a(\ell)$ 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 :

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

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 $(p \neq 2)$:

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

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 $\overline{\Lambda}(L) = \rho(L) + \sum_{\psi'} \lambda\left(\theta\, \psi'^{-1}\right)$, où ψ' parcourt $\widetilde{\Psi}_L^-$; comme ici les caractères ψ'_o sont pairs, on a $\widetilde{\Psi}_L^- = \left(\widetilde{\Psi}_K \times \Psi_k\right)^- = \widetilde{\Psi}_K^- \times \Psi_k$, d'où $\overline{\Lambda}(L) - \rho(L) = \sum_{\psi'_2, \psi'_o} \lambda\left(\theta\, \psi_2'^{-1}\, \psi_o'^{-1}\right)$, $\psi'_2 \in \widetilde{\Psi}_K^-$, $\psi'_o \in \Psi_k$. Ici le caractère $\theta\, \psi_2'^{-1}\, \psi_o'^{-1}$ ne peut plus être décomposé comme dans le cas (ii) ; on écrit que $\theta\, \psi_2'^{-1}\, \psi_o'^{-1}$ est le produit des caractères pairs $\theta\, \psi_2'^{-1}$ et $\psi_o'^{-1}$: $\lambda\left(\theta\, \psi_2'^{-1}\, \psi_o'^{-1}\right) = \lambda\left(\psi_o'^{-1}\right) + \sum_{\ell} 2^{n(\ell)}$, sommation sur les $\ell \neq 2$ tels que $\ell \mid f_{\psi'_2}$, $\theta\, \psi'_o(\ell)$ est une racine de l'unité d'ordre puissance de 2, soit $\psi'_o(\ell) = 1$. On a $\overline{\Lambda}(L) = \rho(L) + \sum_{\psi'_p, \psi'_o} \lambda\left(\psi_o'^{-1}\right) + \sum_{\ell \neq p} 2^{n(\ell)}\, a(\ell)$, où $a(\ell) = \left|\left\{\psi' \in \widetilde{\Psi}_K^- \times \Psi_k,\ \ell \mid f_{\psi'_2}, \psi'_o(\ell) = 1\right\}\right|$. Les caractères ψ'_o sont au nombre de $d(\ell)$; les caractères ψ'_2 sont impairs et doivent être non caractères du corps d'inertie pour ℓ dans $K/\mathbb{Q}$ donc il n'intervient que les premiers 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 $2\,\dfrac{e_{L/k}(\ell) - 1}{e_{L/k}(\ell)} - \dfrac{e^+_{L/k}(\ell) - 1}{e^+_{L/k}(\ell)}$ vaut $\dfrac{e_{L/k}(\ell) - 1}{e_{L/k}(\ell)}$ (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 $\sum_{\psi'_o} \lambda\left(\psi_o'^{-1}\right)$ n'est pas relié à $\overline{\Lambda}(k)$ (en effet k est réel) ; considérons pour cela $\overline{\Lambda}\left(k\left(\mu_4\right)\right) = 1 + \sum_{\psi''} \lambda\left(\theta\, \psi''^{-1}\right)$, $\psi'' \in \Psi^-_{k(\mu_4)}$, sachant que $\Psi^-_{k(\mu_4)} = \left\{\theta\, \psi'_o,\ \psi'_o \in \Psi_k\right\}$; on obtient $\overline{\Lambda}\left(k\left(\mu_4\right)\right) = 1 + \sum_{\psi'_o} \lambda\left(\psi'_o\right)$, et finalement :

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

et la formule de translation :

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

3. Les invariants $\Lambda(\phi)$, $\overline{\Lambda}(\phi)$.

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

Rappels sur les modules $\mathcal{T}(\phi)$ et $\mathcal{H}(\phi)$.

Si ψ est un caractère abélien, on appelle ϕ (resp. φ) le caractère p-adique au-dessus de ψ $\left(\text{resp. } \psi_o\right)$.

Considérons le schéma suivant :

$$\begin{tikzcd}
K_{\psi_p} \arrow[r, dash, "H"] \arrow[dd, dash, "p^r"'] & K_\psi \arrow[d, dash] \\
& K_{\psi^p} \arrow[d, dash] \\
\mathbb{Q} \arrow[r, dash] & K_{\psi_o}
\end{tikzcd}$$

On peut considérer φ comme caractère du groupe $H = \mathrm{Gal}\left(K_\psi / K_{\psi_p}\right)$; il existe alors un idempotent $e_\varphi = \frac{1}{|H|} \sum_{\tau \in H} \varphi\left(\tau^{-1}\right) \tau$ qui est dans $\mathbb{Z}_p[H]$.

Soit $\nu_\psi = \sum_{s_\psi} s_\psi$, s_ψ parcourant $\mathrm{Gal}\left(K_\psi / K_{\psi^p}\right)$.

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

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

On définit alors :

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

D'après [2], § I, on a aussi $\mathcal{T}(\phi) = \{\tau \in \mathcal{T}(K_\psi),\ \tau^{\nu_\psi} = 1\}^{e_\varphi}$.

De même dans le cas impair on pose :

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

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

Il résulte de ces définitions et propriétés que $\mathcal{T}(\phi)$ et $\mathcal{H}(\phi)$ sont des modules sur l'anneau $\mathbb{Z}_p(\psi)$ (par utilisation de l'application $\mathbb{Z}_p[\mathrm{Gal}(K_\psi/\mathbb{Q})] \to \mathbb{Z}_p(\psi)$ 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 $|\mathcal{T}(\phi)|$, $|\mathcal{H}(\phi)|$, en termes de fonctions L_p (on a des expressions conjecturales : cf. [2], § III et [4], § 3.5.3). Cependant les nombres $\prod_\phi |\mathcal{T}(\phi)|$, $\prod_\phi |\mathcal{H}(\phi)|$, où ϕ parcourt l'ensemble des caractères p-adiques divisant un caractère rationnel χ, peuvent s'interpréter comme ordres de modules $\mathcal{T}(\chi)$, $\mathcal{H}(\chi)$ convenables, qui admettent une telle formule (dans le cas de $\mathcal{T}$ voir [4], Th. 3.1, et dans celui de $\mathcal{H}$ voir [2], Th. II2) ; rappelons ces formules :

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

(3.5) $|\mathcal{H}(\chi)| \approx p^{m_o(\chi)} \prod_{\beta | \chi} \frac{1}{2} B_1(\beta^{-1})$, dans le cas où χ est un caractère rationnel impair, où $m_o(\chi)$ 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 $p = 2$, $m_o(\theta) = 2$, 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 $|\mathcal{T}(\chi_n)|$ (resp. $|\mathcal{H}(\chi_n)|$) est constant et ne dépend que du caractère rationnel 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 $\Lambda(\chi)$ $\left(\text{resp. } \overline{\Lambda}(\chi)\right)$ qui permettraient de décomposer les invariants $\Lambda(K)$ $\left(\text{resp. } \overline{\Lambda}(K)\right)$ par rapport aux caractères abéliens rationnels).

Outre cela, on voit que les nombres $|\mathcal{T}(\phi_n)|$ $\left(\text{resp. } |\mathcal{H}(\phi_n)|\right)$ sont bornés pour n assez grand $\left(\phi_n\right.$ désignant n'importe quel caractère p-adique divisant $\left.\chi_n\right)$. Nous utiliserons ce fait plus loin (cf. 4.1).

A partir de ceci nous avons démontré dans [4] que $|\mathcal{T}(\phi_n)|$ était constant pour n assez grand, ce qui définit l'invariant $\Lambda(\phi)$ par l'égalité :

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

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

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

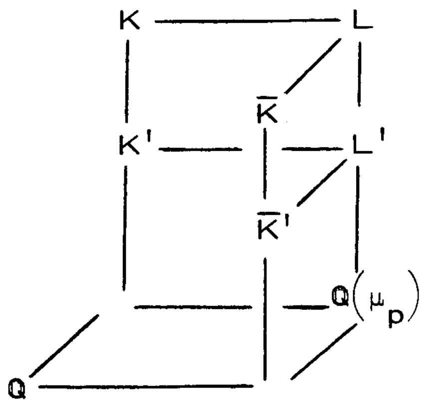
Nous ne le ferons pas ici car le théorème que nous avons en vue ci-après l'entraînera trivialement.

4. <u>Comparaison des modules</u> $\mathcal{T}(\phi_n)$ et $\mathcal{H}(\bar{\phi}_n)$.

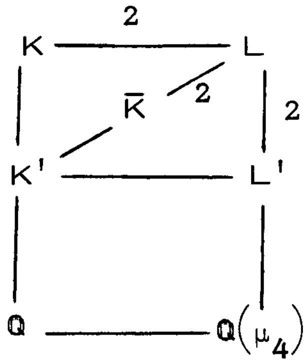
<u>Définitions et résultats préliminaires.</u>

Considérons un caractère pair quelconque ψ fixé, et un entier n assez grand. On appelle g l'ordre de ψ_o. On considère les caractères $\gamma_n\psi$ et $\theta\,\gamma_n^{-1}\,\psi^{-1}$, et on appelle φ, $\bar{\varphi}$, ϕ, $\bar{\phi}$, ϕ_n, $\bar{\phi}_n$ les caractères p-adiques au-dessus de ψ_o, $\theta\,\psi_o^{-1}$, ψ, $\theta\,\psi^{-1}$, $\gamma_n\psi$, $\theta\,\gamma_n^{-1}\,\psi^{-1}$ respectivement. Pour simplifier, on pose $K = K_{\gamma_n\psi}$ (qui est réel), $\overline{K} = K_{\theta\gamma_n^{-1}\psi^{-1}}$ (qui est imaginaire), et $L = K\overline{K}$. Il est clair que L contient μ_q puisque θ est un caractère de L ; on a aussi $L = K(\mu_q) = \overline{K}(\mu_q)$. Enfin on appelle K', $\overline{K}'$ et L' les uniques sous-corps d'indice p de K, $\overline{K}$ et L respectivement. Pour simplifier certains calculs, nous poserons parfois $\mathcal{T} = \mathcal{T}(\phi_n)$, et $\mathcal{H} = \mathcal{H}(\bar{\phi}_n)$.

On a les schémas suivants :



cas $p \neq 2$



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 $\mathrm{Gal}(L/L')$, 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]) :

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

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

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_o^{-1}.

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

$$\mathcal{T}(\phi_n) = \{\tau \in \mathcal{T}(K),\ \tau^{\nu} = \tau^{1-e_\varphi} = 1\} = \{\tau \in \mathcal{T}(K),\ \tau^{A} = 1\},$$

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

$$\mathcal{H}(\bar\phi_n) = \{h \in \mathcal{H}(\bar K),\ h^{\nu} = h^{1-e_{\bar\varphi}} = 1\} = \{h \in \mathcal{H}(\bar K),\ h^{\bar A} = 1\},$$

où $\bar A = \prod_{\beta \mid \bar\phi_n} (\bar t - \beta(\bar t))$ (cas $p \neq 2$),

$$\mathcal{H}(\bar\phi_n) = \{h \in \mathcal{H}(\bar K),\ h^{\nu} = h^{1-e_{\varphi^*}} = 1\} = \{h \in \mathcal{H}(\bar K),\ h^{\bar A} = 1\},$$

où $\bar A$ est inchangé (cas $p = 2$: en effet, ici le caractère de $\bar K$ est $\psi' = \theta\, \gamma_n^{-1}\, \psi_2^{-1}\, \psi_o^{-1}$ pour lequel le caractère ψ'_o associé est ψ_o^{-1} contrairement au cas $p \neq 2$ où ce caractère est $\theta\, \psi_o^{-1}$).

On utilisera ce qui précède sous la forme suivante :

$$\mathcal{T}(\phi_n) = \{\tau \in \mathcal{T}(K),\ \tau^{\omega} = 1,\ \text{pour tout } \omega \in (\nu, 1 - e_\varphi)\},$$

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

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

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

Démontrons maintenant :

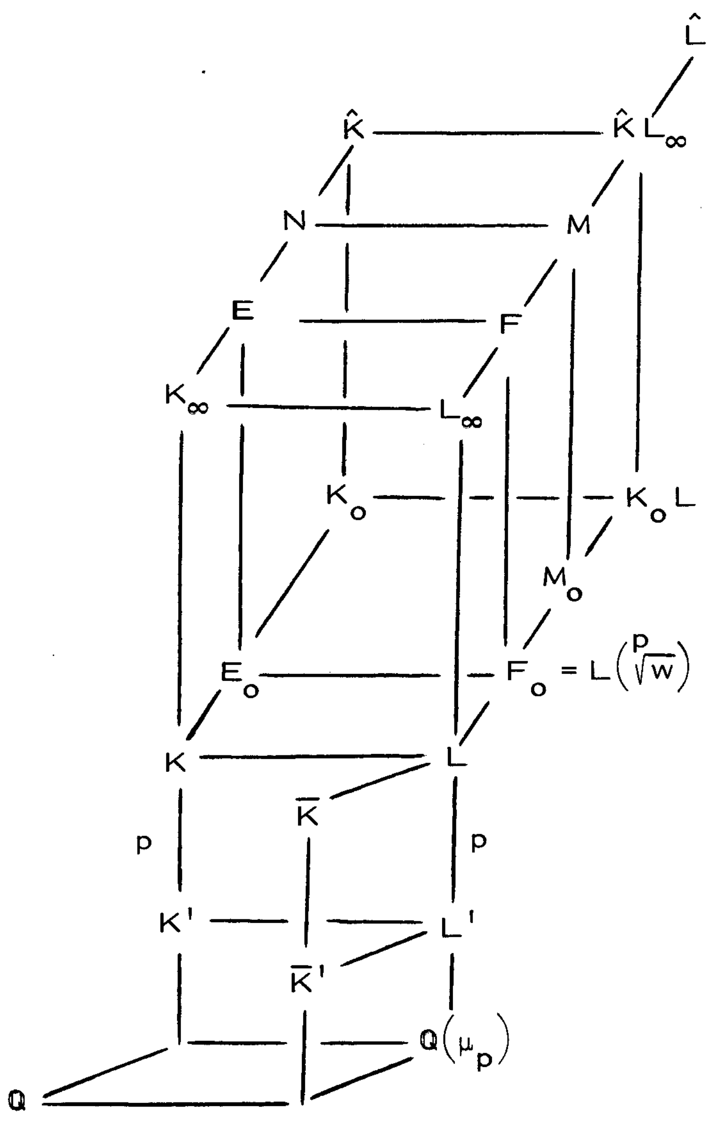
(4.1) Les groupes $\mathrm{Gal}(N/K_\infty) \simeq \mathcal{T}(K)/\mathcal{T}(K)^A$ et $\mathcal{H}(\bar\phi_n)$ sont d'exposants diviseurs de p.

Soit $\mathfrak{P}_n$ l'idéal maximal de $\mathbb{Z}_p(\gamma_n\psi)$; alors $\mathcal{T}(K)/\mathcal{T}(K)^A$, qui est annulé 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 $\mathcal{T}(K)/\mathcal{T}(K)^A$ est borné sur n ; par conséquent comme $\mathbb{Z}_p(\gamma_n\psi)/\mathfrak{P}_n$ est d'ordre $p^{\varphi(1)}$

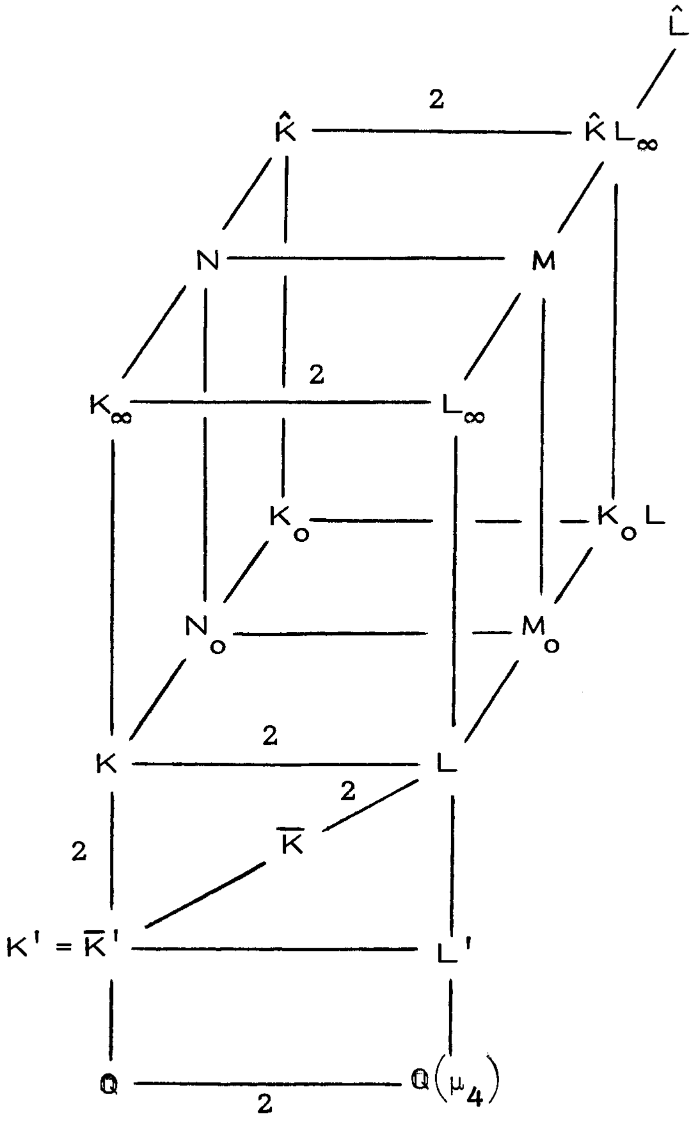
(indépendant de n), les a_n^i sont uniformément bornés sur n et i par une constante a ; d'où l'annulation par p d'un tel module pour tout n assez grand.

La démonstration est identique pour $\mathcal{H}(\bar{\phi}_n)$, 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 $\mathcal{W}_\infty$ 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 $\widetilde{\mathcal{W}}_\infty = \mathcal{W}_\infty / L_\infty^p$, et on appelle $\widetilde{w}$ les éléments de $\widetilde{\mathcal{W}}_\infty$. Plus généralement on pose $\widetilde{L}_\infty = L_\infty / L_\infty^p$: $\widetilde{\mathcal{W}}_\infty$ est une partie de $\widetilde{L}_\infty$.

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 $\bigcup_{n \geq 0} \mu_{qp^n}$. 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 $\widetilde{w} \in \widetilde{\mathcal{W}}_\infty$ a un représentant dans L (resp. un représentant totalement positif dans K) dans le cas $p \neq 2$ (resp. $p = 2$). Enfin $\widetilde{\mathcal{W}}_\infty$ est un G-module annulé par $\mathfrak{M}(\nu, 1 - e_\varphi)$.

On a $\mathrm{Gal}(\hat{K}/K) \simeq \mathbb{Z}_p \oplus \mathcal{T}(K)$; 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_oL/L et L_∞/L sont linéairement disjointes. Il existe donc une extension M_o de L contenue dans K_oL telle que $M_oL_\infty = M$; 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 $\mathrm{Gal}(N/K_\infty)$ est annulé par l'idéal $(\nu, 1 - e_\varphi)$, donc $\mathrm{Gal}(M/L_\infty)$ est annulé 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 $\widetilde{\mathcal{W}}_\infty$.

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, $\mathcal{O}_\Omega$ 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 $\widetilde{\mathcal{W}}_\infty$: Soit $h \in \mathcal{H}$; on a $h^p = 1$, donc si $\mathfrak{a} \in h$, $\mathfrak{a}^p = a\mathcal{O}_{\overline{K}}$, $a \in \overline{K}$. On pose $\widetilde{w} = \widetilde{a}^{e_{\overline{\varphi}}}$ dans $\widetilde{L}_\infty$. Si $\mathfrak{b} \in h$, $\mathfrak{b} = \mathfrak{a}\, c\mathcal{O}_{\overline{K}}$, $c \in \overline{K}$, soit, en posant $\mathfrak{b}^p = b\mathcal{O}_{\overline{K}}$, $b = ac^p\varepsilon$, ε unité de $\overline{K}$, et $\widetilde{w}$ est aussi défini par $(\widetilde{a}\,\widetilde{\varepsilon})^{e_{\overline{\varphi}}}$. Or $\overline{K}$ est imaginaire et cyclique ; d'après [5], § 25, Satz 24, on peut écrire $\varepsilon = \varepsilon_o \zeta$, ε_o unité réelle de $\overline{K}$, $\zeta \in \mu_{\overline{K}}$. On a $\widetilde{\varepsilon}_o^{\,e_{\overline{\varphi}}} = \widetilde{1}$ car $\overline{\varphi}$ est impair, et $\widetilde{\zeta} = \widetilde{1}$. L'application est donc bien définie.

Calcul du noyau. Supposons que $\widetilde{w} = \widetilde{a}^{e_{\overline{\varphi}}} = \widetilde{1}$; soit e un représentant mod p de $e_{\overline{\varphi}}$ 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 : $\mathfrak{a}^{ep}\mathcal{O}_L = b^p\mathcal{O}_L$, soit $\mathfrak{a}^e\mathcal{O}_L = b\mathcal{O}_L$; comme $[L : \overline{K}]$ est premier à p, ceci entraîne $h = 1$.

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

et $\tau e_{\overline{\varphi}} = \theta(\tau) e_{\overline{\varphi}}$. Il résulte de ceci que dans $\overline{K}^*/\overline{K}^{*p}$ l'image de w vérifie $(w\overline{K}^{*p})^{\tau - \theta(\tau)} = \overline{K}^{*p}$, pour tout $\tau \in \mathrm{Gal}(L/K)$: ceci est le critère classique de décomposition qui montre que $F_o = L(\sqrt[p]{w})$ est décomposée sur K par une extension cyclique E_o de K telle que $E_o L = F_o$. Comme $w\mathcal{O}_{\overline{K}} = \mathfrak{a}^{ep}$ dans $\overline{K}$, la théorie élémentaire de Kummer montre que F_o/L, donc E_o/K, est p-ramifiée, donc $E = E_o K_\infty$ est contenue dans $\hat{K}$. Vérifions qu'elle est contenue dans N ; pour cela il suffit de prouver que $F = F_o L_\infty$ est contenue dans M. Ceci revient à montrer que $\mathrm{Gal}\left(F/L_\infty\right)$ est annulé par $\left(\nu, 1-e_\varphi\right)$, soit que $\langle\tilde{w}\rangle$ est annulé par $\left(\nu, 1-e_{\bar{\varphi}}\right)$. L'annulation par $1-e_{\bar{\varphi}}$ est évidente par construction de $\tilde{w}$ $\left(\tilde{w} = \tilde{a}^{e_{\bar{\varphi}}}\right)$. On étudie ensuite $\tilde{w}^\nu = a^{\nu e_{\bar{\varphi}}}$: comme $h^\nu = 1$, on a $\mathfrak{a}^\nu = c\mathcal{O}_{\bar{K}}$, $c \in \bar{K}$, et $a^\nu = c^p \varepsilon$, ε unité de $\bar{K}$; donc $\tilde{w}^\nu = \tilde{\varepsilon}^{e_{\bar{\varphi}}} = \tilde{1}$ comme on l'a déjà prouvé plus haut.

<u>Surjectivité</u>. Soit $\tilde{w}_1 \in \tilde{\mathcal{W}}_\infty$ représenté par un élément $w_1 \in L$ tel que $F_o = L\left(\sqrt[p]{w_1}\right) \subset M_o$; soit $\nu' = \sum_\tau \tau$, τ parcourant $\mathrm{Gal}(L/\bar{K})$, alors $e_{\bar{\varphi}}\nu' = \bar{d}\, e_{\bar{\varphi}}$, 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 $\bar{d}$ mod 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 $\left(\nu, 1-e_{\bar{\varphi}}\right)$: on a $\tilde{w}^\nu = \tilde{1}$ soit $w^\nu \in L_\infty^p \cap L$, donc, d'après 4.2, $w^\nu = \zeta a^p$, $\zeta \in \mu_L$, 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 $k\left(\mu_{p^n}\right)$ et $k\left(\mu_{p^{n+1}}\right)$ respectivement, où $k = K_{\psi_o}$. 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, $a^p \in \overline{K}'$, et $\zeta \in \overline{K}'$.

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

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

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

Comme l'extension $\overline{K}/\overline{K}'$ 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 $\overline{K}$, et $w\mathcal{O}_{\overline{K}} = \mathfrak{b}^p$ dans $\overline{K}$. On vérifie facilement que la classe h de $\mathfrak{b}$ est telle que $h^{e_{\overline{\varphi}}} \in \mathcal{H}$ et redonne $\tilde{w}$ par l'application étudiée.

On a donc obtenu l'isomorphisme de G-modules $\widetilde{\mathcal{W}}_\infty \simeq \mathcal{H}$; il en résulte que les G-structures de $\mathcal{H}$ et $\mathcal{T}(K)/\mathcal{T}(K)^A$ sont reliées par la "Spiegelungs-relation".

(ii) <u>Cas p = 2</u>. On peut écarter provisoirement le cas où $\psi_o = 1$: 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 $\overline{\phi}_n$ sont rationnels, et dans ce cas les ordres de $\mathcal{T}$ et $\mathcal{H}$ sont donnés par les formules analytiques 3.4 et 3.5 :

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

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

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

D'où $\quad |\mathcal{H}| = 2^{1-\delta}\,|\mathcal{T}|$, 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

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

Soit $a \in \Omega^*$ tel que $\left(a\,\Omega^{*2}\right)^{1-e_{\varphi^*}} = \Omega^{*2}$, et tel que $\tilde{a} = \tilde{1}$ dans $\tilde{L}^*_\infty$; 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 $\tau \in \mathrm{Gal}(L/\Omega)$; 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, $\mathrm{Gal}\left(M/L_\infty\right)$ est annulé par l'idéal $\left(1+s, 1-e_\varphi\right)$, donc, par la "Spiegelungsrelation", $\tilde{\mathcal{W}}_\infty$ est annulé par l'idéal $\left(1+s, 1-e_{\varphi^*}\right)$.

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

Soit $\mathcal{W} = \{w \in \left(\mathcal{W}_\infty \cap \overline{K}\right)^e,\ w\mathcal{O}_{\overline{K}} = \mathfrak{a}^2 \text{ dans } \overline{K}\}$. On a donc la relation $\left(w\overline{K}^{*2}\right)^{1-e_{\varphi^*}} = \overline{K}^{*2}$.

On a le résultat suivant :

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

En effet, on peut trouver (d'après 4.3) $w_o \in K$ représentant $\tilde{w}$ $\left(w_o \gg 0\right)$; 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 $w^{1+\sigma_\infty} = w_o^2\left(u^{1+\sigma_\infty}\right)^2 = a^2$, 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 nécessairement, $a^s = -a$, 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 $\mathfrak{a}$: cette application est définie de $\mathcal{W}$ dans le groupe des classes de $\overline{K}$ annulées par 2 et $1-e_{\varphi^*}$. Elle induit grâce à 4.4 une application f de $\widetilde{\mathcal{W}} \simeq \mathcal{W}/\mathcal{W} \cap \overline{K}^{*2}$ dans le groupe des classes de $\overline{K}$ annulées par 2 et $1-e_{\varphi^*}$.

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

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

Image de f. Si $w \in \mathcal{W}$, on a $w\mathcal{O}_{\overline{K}} = \mathfrak{a}^2$, et, d'après 4.5, $w^{1+\sigma_\infty} = a_+^2$, $a_+ \gg 0$ dans K' ; d'où par $\overline{N}$: $\overline{N}w\mathcal{O}_{K'} = \left(a_+\mathcal{O}_{K'}\right)^2 = \left(\overline{N}\mathfrak{a}\right)^2$, soit $\overline{N}\mathfrak{a} = a_+\mathcal{O}_{K'}$, et la classe h de $\mathfrak{a}$ 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 $\widetilde{\mathcal{W}}$ n'est pas restrictif pour notre problème :

(4.6) On a $\widetilde{\mathcal{W}} = \widetilde{\mathcal{W}}_\infty$.

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

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

Prenons w_o dans K, $w_o \gg 0$ (cf. 4.3) et posons $w = w_o^e$; 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 $\overline{K}$: on a $\left(w/b\right)^{1+\sigma_\infty s} = w^{1+s}/b^2 = 1$, 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 $w' \in \mathcal{W}_\infty \cap \overline{K}$. Etudions maintenant la décomposition en idéaux de $w'\mathcal{O}_{\overline{K}}$.

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

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

$$(4.7) \qquad 1 \longrightarrow \left(U^+/U^2\right)^{e_{\varphi^*}} \longrightarrow \widetilde{\mathcal{W}}_\infty \xrightarrow{\ f\ } \mathcal{H}'.$$

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 $\sigma\, S(\alpha) = S\left(\alpha^\sigma\right)$ pour tout $\sigma \in G$) :

$$(4.8) \qquad 1 \longrightarrow \mathcal{H}' \longrightarrow \mathcal{H} \xrightarrow{\ g\ } \left(S(K')/S(U)\right)^{e_{\varphi^*}} \longrightarrow 1\,.$$

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

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

On a $h \in \operatorname{Ker} g$ si et seulement si $S(a) \in S(U)$, soit $S(a) = S(\varepsilon)$, $\varepsilon \in U$, et $a = \varepsilon a_+$, $a_+ \in K'$, $a_+ \gg 0$; on a donc $\overline{N}\mathfrak{a} = a\mathcal{O}_{K'} = a_+\mathcal{O}_{K'}$, et $h \in \mathcal{H}'$.

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

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

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

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

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

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 $\mathcal{U}_o \simeq \mathbb{Z}_2$ sur lequel G opère trivialement ; alors le théorème de Dirichlet sur les unités entraîne que l'on a l'isomorphisme de G-modules :
$\mathbb{Q}_2 \otimes_{\mathbb{Z}_2} (\mathcal{U} \oplus \mathcal{U}_o) \simeq \mathbb{Q}_2[G']$.

Comme $\mathcal{U} = \bigoplus_{\varphi' \neq 1} \mathcal{U}^{e_{\varphi'}}$, φ' parcourant l'ensemble des caractères 2-adiques irréductibles de $k = K_{\psi_o}$, on en déduit $\mathbb{Q}_2 \otimes \mathcal{U}^{e_{\varphi'}} \simeq \mathbb{Q}_2[G']e_{\varphi'}$, pour $\varphi' \neq 1$. Appelons encore H le plus grand sous-groupe de G' d'ordre impair, et soit $\Gamma = \mathrm{Gal}(K'/k)$; on a $\mathbb{Q}_2[G'] \simeq \mathbb{Q}_2[H][\Gamma]$ et dans cet isomorphisme on a $\mathbb{Q}_2[G']e_{\varphi'} \simeq (\mathbb{Q}_2[H]e_{\varphi'})[\Gamma]$, en considérant $e_{\varphi'}$ comme élément de $\mathbb{Q}_2[H]$; or $\mathbb{Q}_2[H]e_{\varphi'}$ est un corps de degré $\varphi'(1)$ sur $\mathbb{Q}_2$, par conséquent $\mathbb{Q}_2[G']e_{\varphi'}$ est un $\mathbb{Q}_2$-espace vectoriel de dimension $|\Gamma|\,\varphi'(1)$. Il en résulte que $\mathcal{U}^{e_{\varphi'}}$ est de $\mathbb{Z}_2$-dimension $|\Gamma|\,\varphi'(1)$, donc que $(U/U^2)^{e_{\varphi'}}$ est de $\mathbb{F}_2$-dimension $|\Gamma|\,\varphi'(1)$; appliqué à $\varphi' = \varphi^* \neq 1$ 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 $|\mathcal{H}| = |(S(K')/S(U))^{e_{\varphi^*}}|\,|\mathcal{H}'| = |(U^+/U^2)^{e_{\varphi^*}}|\,|\mathcal{H}'| = |\widetilde{\mathcal{W}}_\infty|\,|\mathcal{H}'|\,/\,|\mathrm{Im} f| \geq |\widetilde{\mathcal{W}}_\infty|$; on a donc obtenu universellement les inégalités (même lorsque $\psi_o = 1$) :

$$|\mathcal{C}(\phi_n)| \leq |\mathcal{H}(\bar{\phi}_n)| \text{, pour tout } \psi \text{ pair, et tout } n \text{ assez grand.}$$

Soit χ_o le caractère rationnel au-dessus de ψ_o ; comme ici θ est d'ordre 2, les sommes $\sum_a \sum_{\psi_o | \chi_o} \gamma_n^a \psi_p^a \psi_o$ et $\sum_a \sum_{\psi_o | \chi_o} (\theta\, \gamma_n^{-1} \psi_p^{-1})^a \psi_o^{-1}$, a parcourant $(\mathbb{Z}/p^n\mathbb{Z})^*$, sont les deux caractères rationnels χ_n et $\overline{\chi}_n$ associés à K et $\overline{K}$ respectivement. Donc les ensembles $\{\phi'_n \mid \chi_n\}$ et $\{\bar{\phi}'_n \mid \overline{\chi}_n\}$ se correspondent bijectivement, ce qui donne, en faisant le produit des inégalités précédentes : $\prod_{\phi'_n \mid \chi_n} |\mathcal{T}(\phi'_n)| \leq \prod_{\bar{\phi}'_n \mid \bar{\chi}_n} |\mathcal{H}(\bar{\phi}'_n)|$ soit $|\mathcal{T}(\chi_n)| \leq |\mathcal{H}(\bar{\chi}_n)|$. 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 $v_p(|\mathcal{T}(\chi_n)|) = v_p\left(\prod_{a,\psi_o} \frac{1}{2} L_2(1, \gamma_n^a \psi_p^a \psi_o)\right)$, et $v_p(|\mathcal{H}(\bar{\chi}_n)|) = v_p\left(\prod_{a,\psi_o} \frac{1}{2} L_2(0, \gamma_n^a \psi_p^a \psi_o)\right)$. Les valuations de chacun des seconds membres ci-dessus sont égales (pour n assez grand), et il en résulte les égalités $|\mathcal{T}(\phi_n)| = |\mathcal{H}(\bar{\phi}_n)|$.

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

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

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 $\mathbb{Q}_\infty$ 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 $|\mathcal{H}(\bar{\phi}_n)| = |\mathcal{T}(\phi_n)|$ sauf dans le cas particulier où $p = 2$, ψ est un caractère d'ordre puissance de 2 non caractère de $\mathbb{Q}_\infty$, auquel cas $|\mathcal{H}(\bar{\phi}_n)| = 2\,|\mathcal{T}(\phi_n)|$.

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 $|\mathcal{H}(\phi_n)| = p^{\bar{\Lambda}(\bar{\phi})}$, 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 $\mathbb{Q}_\infty$), 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 $\Lambda(\phi) = \lambda(\phi)$ $\left(\phi \text{ non caractère de } \mathbb{Q}_\infty\right)$ est vraie dès que l'un au moins des caractères ϕ ou $\overline{\phi}$ est rationnel (dans le second cas, $\overline{\phi}_n$ 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 $\overline{\phi}$ est un caractère 5-adique issu d'un caractère d'ordre 4.

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

Nous avons comparé analytiquement les ordres de $\mathcal{T}$ et $\mathcal{H}$ lorsque $\psi_o = 1$ $\left(\text{i. e. } \varphi = \varphi^* = 1\right)$. 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 $\mathbb{Q}_\infty$ $\left(\text{sinon on a } \mathcal{T} = \mathcal{H} = (1)\right)$.

Ici $\widetilde{\mathcal{W}}_\infty = \mathcal{W}_\infty / L_\infty^2$ est annulé par $1+s$. On a toujours le fait que tout élément $\widetilde{w}$ de $\widetilde{\mathcal{W}}_\infty$ a un représentant w_o dans K totalement positif, et le fait que pour tout $w \in \mathcal{W}_\infty \cap \overline{K}$, $w^{1+s} = a_+^2$, $a_+ \in K'$, $a_+ \gg 0$. 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 $\mathbb{Q}_\infty$ $(r \geq 1)$, 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} $\left(\zeta_1 \text{ engendre } \mu_L\right)$, et soit $w_1 = -\zeta_1^{-1}(1-\zeta_1)^2$. On a $w_1 = 2 - \left(\zeta_1^{-1} + \zeta_1\right)$ 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 $\alpha = \zeta_1^\lambda u^2 = \left(-w_1^{-1}\right)^\lambda \left(1-\zeta_1\right)^{2\lambda} u^2$, 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 $L = K\left(\sqrt{-1}\right)$, 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 $\overline{K}$:

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

On désigne encore par $\mathcal{H}'$ le sous-groupe de $\mathcal{H}$ formé des classes des idéaux $\mathfrak{a}$ de $\overline{K}$ tels que $N\mathfrak{a}$ soit principal au sens restreint dans K', et par $\mathcal{W} = \{w \in \mathcal{W}_\infty \cap \overline{K}, w\mathcal{O}_{\overline{K}} = \mathfrak{a}^2$ dans $\overline{K}\}$. 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 $\overline{K}$, g est l'application qui à $w \in \mathcal{W}$ associe $\widetilde{w}$ dans $\widetilde{\mathcal{W}}_\infty$.

On peut maintenant étudier f et g.

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

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

Image de g. Soit $\widetilde{w} \in \widetilde{\mathcal{W}}_\infty$ 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 $(a^2)\mathcal{O}_{K'} = (N w\, w_1^{-\delta})\mathcal{O}_{K'}$; or l'extension $K(\sqrt{w})$ est 2-ramifiée par hypothèse $\left(L_\infty(\sqrt{w})/L_\infty\right.$ l'est par définition, et L_∞/K est aussi 2-ramifiée$\left.\right)$, donc $w\mathcal{O}_K = \mathfrak{a}^2\, \mathfrak{p}$, dans K, où $\mathfrak{p}$ est un 2-idéal de K, soit $N w\mathcal{O}_{K'} = (N\mathfrak{a})^2\, N\mathfrak{p}$; 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 $N\left(wa^{-1}(1-\zeta_1)^{-1}\sqrt{-1}\right) = \zeta_1$ dans L/L'. Montrons que pour n assez grand ζ_1 ne peut être norme dans L/L' en calculant le symbole de Hilbert $(\omega, \zeta_1)_{\mathfrak{l}}$, où ω et $\mathfrak{l}$ sont ainsi définis : ω est un élément du radical de L/L'

$\left(L = L'(\sqrt{\omega}),\ \omega \in L'\right)$; $\mathfrak{l}$ 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 $\mathbb{Q}_\infty$).

On sait que $\omega \mathcal{O}_{L'}$ est divisible par une puissance impaire de $\mathfrak{l}$; il en résulte que $(\omega, \zeta_1)_{\mathfrak{l}} = \zeta_1^{(\ell^k-1)/2}$, où k est le degré résiduel de ℓ dans $L'/\mathbb{Q}$. Posons $\ell\,\theta^{-1}(\ell) = 1 + 4.2^{n(\ell)}u$, u impair ; le degré résiduel de ℓ dans $L'/\mathbb{Q}$ est donc égal à celui de ℓ dans $\mathbb{Q}(\mu_{4.2^{n-r}})/\mathbb{Q}$, soit $k = 2^{n-r-n(\ell)}$ (n toujours supposé assez grand), d'où $\frac{\ell^k-1}{2} = \frac{4.2^{n(\ell)+n-r-n(\ell)}u}{2} = 2.2^{n-r}u$ 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 $\left(\frac{w}{a}\right)^{1+\sigma_\infty s} = \left(\frac{w}{a}\right)^{1+s} = 1$, donc $\frac{w}{a} = c^{1-\sigma_\infty s}$ avec $c \in L$; alors $\left(\frac{w}{c^2}\right)^{\sigma_\infty s} = \frac{w^s}{c^{2\sigma_\infty s}} = \frac{w^{-1}a^2w^2}{c^2a^2} = \frac{w}{c^2}$ qui est donc dans $\overline{K}$. Le représentant $w' = \frac{w}{c^2}$ de $\tilde{w}$ est dans $\mathcal{W}$: en effet, $w' \in \mathcal{W}_\infty \cap \overline{K}$. Reste à vérifier que $w'\mathcal{O}_{\overline{K}}$ est carré d'un idéal. On a $\overline{K}(\sqrt{w'})/\overline{K}$ qui est 2-ramifiée ($L_\infty(\sqrt{w'})/L_\infty$ l'est par hypothèse, et $L_\infty/\overline{K}$ est aussi 2-ramifiée), donc $w'\mathcal{O}_{\overline{K}} = \mathfrak{a}^2\mathfrak{p}$ ($\mathfrak{p}$ 2-idéal de $\overline{K}$) ; d'où $w'^{1+s}\mathcal{O}_{K'} = (\overline{N}\mathfrak{a})^2\overline{N}\mathfrak{p}$; or $w' \in \mathcal{W} \cap \overline{K}$ entraîne $w'^{1+s} = a_+^2$, $a_+ \in K'$, donc $\overline{N}\mathfrak{p}$ est un carré de 2-idéal dans K' ; comme K/K' est ramifiée en 2, ceci entraîne $\mathfrak{p} = \mathfrak{q}^2$ dans $\overline{K}$.

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

On a donc les suites exactes :

$$1 \longrightarrow \{\pm 1\}\, U^+ \overline{K}^2 \longrightarrow \mathcal{W} \xrightarrow{\ f\ } \mathcal{H}'$$

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

qui conduisent aux suivantes :

$$1 \longrightarrow U^+/U^2 \longrightarrow \mathcal{W}/\{\pm 1\}\overline{K}^2 \xrightarrow{\ f\ } \mathcal{H}'$$

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