THEORIE DES NOMBRES

BESANCON

Années 1984/85-1985/86

Fascicule 2

RELATIONS CONGRUENTIELLES ADDITIVES ENTRE FONCTIONS L_p DE $\mathbb{Q}$

Georges GRAS

Relations congruentielles additives entre fonctions L_p de $\mathbb{Q}$

§ 0. Introduction :

Soit S un ensemble fini de nombres premiers, contenant ou non le nombre premier p, et soit $\mathbb{Q}_S$ l'extension abélienne maximale de $\mathbb{Q}$ non ramifiée en dehors de $S \cup \{\infty\}$. On a mis en évidence dans [G2, §3] les "$\mathbb{Z}_p$-distributions de Stickelberger" $\mu_{\mathbb{Q}_S}$ et rappelé leurs principales propriétés ; on sait que, uniquement lorsque $p \in S$, leur "transformée de Mellin" p-adique n'est autre que la $\mathbb{Z}_p$-pseudo-mesure de Deligne-Ribet $\lambda_{\mathbb{Q}_S}$, associée à la construction des fonctions L p-adiques de $\mathbb{Q}$.

Nous montrons ici que, d'une part la propriété de $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ d'être somme directe des groupes d'inertie des nombres premiers $q \in S$, et d'autre part les propriétés fonctionnelles des distributions $\mu_{\mathbb{Q}_S}$, conduisent à une famille de relations congruentielles additives entre différentes distributions μ attachées à des sous-corps L_I convenables de $L = \mathbb{Q}_S$ (essentiellement des corps d'inertie d'éléments de S) ; ces relations conduisent alors naturellement à des congruences additives entre nombres de Bernoulli $B_1(\chi_{L_I})$ et/ou fonctions L p-adiques $L_p(\chi_{L_I}, s)$, $s \in \mathbb{Z}_p$; ces congruences mettent en jeu différents caractères χ_{L_I} des sous-corps L_I et apparaissent comme entièrement nouvelles.

Avant d'énoncer les résultats obtenus, donnons toutes les notations nécessaires à leur utilisation pratique :

(0. 1) Notations. (i) Soit χ un caractère d'ordre fini de $\mathbb{Q}^{ab}$, et soit S_χ l'ensemble des diviseurs premiers du conducteur de χ ;

(ii) on fixe un nombre premier p et on désigne par S l'un des ensembles S_χ ou $S_\chi \cup \{p\}$;

(iii) on désigne par ω, $\langle\ \rangle$ et N les caractères habituels du corps $\mathbb{Q}_{\{p\}}$ (cf. [G1, (1.4)]), mais on les considère comme caractères de $\mathbb{Q}_{S \cup \{p\}}$ (c'est-à-dire que lorsque $p \notin S$, les restrictions de ω, $\langle\ \rangle$ et N à $\mathrm{Gal}(\mathbb{Q}_{S \cup \{p\}}/\mathbb{Q}_{\{p\}}) \simeq \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ sont le caractère unité) ;

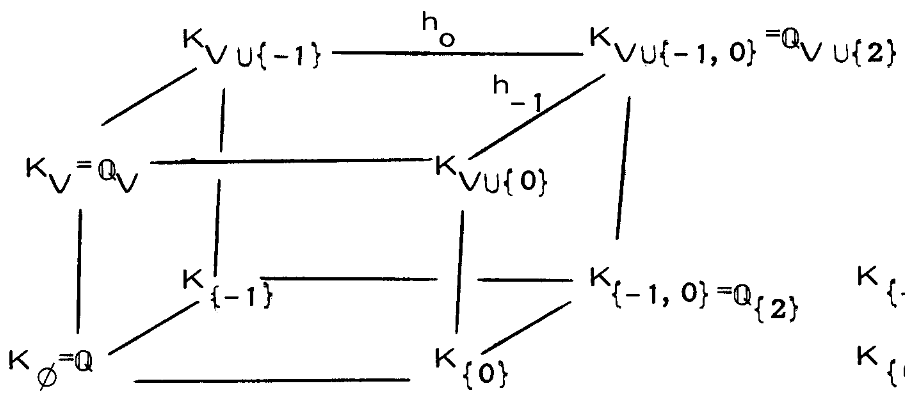
(iv) pour tout $q \neq 2$, $q \in S$, on désigne par h_q un progénérateur de

$H_q = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}_{S-\{q\}})$; pour $q = 2 \in S$, on désigne par h_{-1} (resp. h_o) un (pro) générateur de $H_{-1} = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}_{S-\{2\}}\mathbb{Q}_\infty)$ (resp. de $H_o = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}_{S-\{2\}}(\sqrt{-1}))$ ou $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}_{S-\{2\}}(\sqrt{-2}))$), où $\mathbb{Q}_\infty$ est la $\mathbb{Z}_2$-extension cyclotomique de $\mathbb{Q}$;

(v) lorsque $2 \notin S$, on pose $P = S$, sinon on pose $P = (S-\{2\}) \cup \{-1, 0\}$; on fixe une fois pour toutes une partie E de P.

Pour toute partie J de P on pose $H_J = \bigoplus_{t \in J} H_t$, et on désigne par K_J le sous-corps de $K_P = \mathbb{Q}_S$ fixe par H_{P-J} ;

si $2 \notin S$, on a $K_J = \mathbb{Q}_J$, pour tout $J \subseteq S$; si $2 \in S$, le schéma ci-dessous indique les relations entre les corps K_J, $J \subseteq P$, et les corps $\mathbb{Q}_V$, $V \subseteq S$ (on a pris ici $V \subseteq S - \{2\}$) :



$K_{\{-1\}} = \mathbb{Q}(\sqrt{-1})$ ou $\mathbb{Q}(\sqrt{-2})$

$K_{\{0\}} = \mathbb{Q}_\infty$

Pour tout $I \subseteq E$, on pose $L_I = K_{I\cup Q}$, $Q = P - E$ (L_I est fixe par H_{E-I}).

Comme $K_P = \mathbb{Q}_S$ est le composé direct sur $\mathbb{Q}$ des corps L_I et K_{E-I}, pour tout $I \subseteq E$, le caractère χ se décompose de façon unique sous la forme $\chi = \chi_{L_I}\chi_{K_{E-I}}$, où χ_{L_I} (resp. $\chi_{K_{E-I}}$) est un caractère de L_I (resp. K_{E-I}).

On désigne par $\mathbb{Q}_o$ le sous-corps de $\mathbb{Q}_{\{p\}}$ fixe par h_p^{p-1} (resp. h_o) si $p \neq 2$ (resp. $p = 2$) et on décompose $\chi_{\mathbb{Q}_{\{p\}}}$ sous la forme $\chi_{\mathbb{Q}_{\{p\}}} = \chi_o\chi_\infty$, χ_o (resp. χ_∞) caractère de $\mathbb{Q}_o$ (resp. de la $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ de $\mathbb{Q}$) ;

(vi) on désigne par $\mathbb{Z}_p(\chi)$ l'anneau engendré sur $\mathbb{Z}_p$ par les valeurs de χ ; on désigne par $\mathfrak{M}$ son idéal maximal et par v sa valuation d'image $\mathbb{Z} \cup \{\infty\}$;

(vii) on décompose χ sous la forme $\chi = \varphi\psi$, φ d'ordre étranger à p, ψ d'ordre puissance de p ; on désigne par M le sous-corps de $\mathbb{Q}^{ab}$ fixe par $\mathrm{Ker}(\omega^{-1}\chi)$ et on désigne par M_o le sous-corps de M fixe par $\mathrm{Ker}(\omega^{-1}\varphi)$ (resp. $\mathrm{Ker}(\varphi)$) lorsque $p \neq 2$ (resp. $p = 2$) ;

(viii) pour tout nombre premier q on désigne par p^{d_q} (resp. p^{f_q}) l'indice de décomposition (resp. le degré résiduel) de q dans M/M_o ; on pose $R=\sum_{\ell} p^{d_\ell+f_\ell}$, sommation sur les $\ell \in (E \cap S)-\{p\}$ non ramifiés dans $M_o/\mathbb{Q}$. D'une manière générale, q désigne un élément de S et ℓ un élément de S distinct de p.

(0. 2) <u>Théorème.</u> Si $p\neq 2$ ou si $p\notin S$, on a la congruence suivante :

$$\sum_{\substack{I\subseteq E\\ p \text{ ramifié}\\ \text{dans } L_I}} (-1)^{|I|} L_p(\chi_{L_I}, s) \prod_{\substack{\ell\in S \text{ non ramifié}\\ \text{dans } L_I}} (1-\omega^{-1}\chi_{L_I}(\ell)\langle \ell\rangle^{-s})$$

$$-\sum_{\substack{I\subseteq E\\ p \text{ non ramifié}\\ \text{dans } L_I}} (-1)^{|I|} B_1(\chi_{L_I}) \prod_{\substack{q\in S \text{ non ramifié}\\ \text{dans } L_I}} (1-\chi_{L_I}(q)) \equiv c_\chi \mod \mathfrak{m}_\chi ,$$

où c_χ et $\mathfrak{m}_\chi$ sont donnés par le tableau suivant :

	c_χ	$v(\mathfrak{m}_\chi)$
$p\neq 2$, $p\notin S$	0	R
$p=2\notin S$ et :		
$E\neq S$ ou il existe $\ell\in S$, $\ell\equiv 1(4)$	0	R
$E=S$, χ d'ordre 1 ou 2, $\ell\equiv -1(4)$ pour tout $\ell\in S$	$2^{\lvert S\rvert-1}$	$R(=\lvert S\rvert)$
$p\neq 2$, $p\in S$ et :		
$p\notin E$ ou p ramifié dans $M_o/\mathbb{Q}$, et $\chi_o\neq 1$ ou $P-E\not\subseteq \{p\}$	0	R
$p\in E$ non ramifié dans M_o ramifié dans M	0	$R+p^{d_p+f_p}$
$p\in E$ non ramifié dans M	0	$R+v(p\,s)$
$\chi_o=1$, $E=P$ ou $P-\{p\}$	$\dfrac{(-1)^{\lvert P-E\rvert+1}\log(1+p)\prod_{q\in S}(1-q^{-1})}{(1-\chi_\infty(1+p)(1+p)^{1-s})}$	R

(0. 3) <u>Théorème.</u> Si $p=2\in S$, on a la congruence suivante :

$$\sum_{\substack{I\subseteq E\\ \mathbb{Q}_{\{2\}}\subseteq L_I}} (-1)^{|I|} L_2(\chi_{L_I}, s) \prod_{\substack{\ell\in S \text{ non ramifié}\\ \text{dans } L_I}} (1-\omega^{-1}\chi_{L_I}(\ell)\langle \ell\rangle^{-s})$$

$$+ \sum_{\substack{I\subseteq E\\ \mathbb{Q}_\infty\subseteq L_I,\ \mathbb{Q}_0\not\subseteq L_I}} (-1)^{|I|} L_2(\omega_0^{-1}\chi_{L_I}, s) \prod_{\substack{\ell\in S \text{ non ramifié}\\ \text{dans } L_I}} (1-\omega_0^{-1}\chi_{L_I}(\ell)\langle \ell\rangle^{-s})$$

$$- \sum_{\substack{I\subseteq E\\ \mathbb{Q}_\infty\not\subseteq L_I,\ \mathbb{Q}_0\subseteq L_I}} (-1)^{|I|} B_1(\omega_0^{-1}\chi_{L_I}) \prod_{\substack{\ell\in S \text{ non ramifié}\\ \text{dans } L_I}} (1-\omega_0^{-1}\chi_{L_I}(\ell))$$

$$- \sum_{\substack{I\subseteq E\\ 2 \text{ non ramifié}\\ \text{dans } L_I}} (-1)^{|I|} B_1(\chi_{L_I})(1-\chi_{L_I}(2)) \prod_{\substack{\ell\neq 2\in S \text{ non ramifié}\\ \text{dans } L_I}} (1-\chi_{L_I}(\ell)) \equiv c_\chi \bmod \mathfrak{M}_\chi ,$$

où c_χ et $\mathfrak{M}_\chi$ sont donnés par le tableau suivant :

	c_χ	$v(\mathfrak{M}_\chi)$
$\chi_0 \neq 1$ ou $P-E \not\subseteq \{-1, 0\}$ et :		
$0\notin E$, $-1\notin E$	0	R
$0\notin E$, $-1\in E$	0	$R+v(2)$
$0\in E$, $-1\notin E$, $\omega\chi_\infty(h_0)\neq\pm 1$	0	$R+2^{d_2+f_2}$
" " $=-1$	0	$R+v(2)$
" " $=1$	0	$R+v(4s)$
$0\in E$, $-1\in E$, $\omega\chi_\infty(h_0)\neq\pm 1$	0	$R+2^{d_2+f_2}+v(2)$
" " $=-1$	0	$R+2v(2)$
" " $=1$	0	$R+v(4s)+v(2)$
$\chi_0 = 1$ et :		
$E=P-\{-1, 0\}$	$\dfrac{(-1)^{\lvert P-E\rvert}\log 5 \prod_{q\in S}(1-q^{-1})}{(1-\chi_\infty(5)\, 5^{1-s})}$	R
$E=P-\{0\}$		$R+v(2)$
$E=P-\{1\}$, $\omega\chi_\infty(h_0)\neq\pm 1$		$R+2^{d_2+f_2}$
" $=-1$	$(-1)^{\lvert P-E\rvert}\log 5 \prod_{q\in S}(1-q^{-1})\ \times$	$R+v(2)$
" $=1$		$R+v(4s)$
$E=P$, $\omega\chi_\infty(h_0)\neq\pm 1$	$\left(\dfrac{1}{1-\chi_\infty(5)\,5^{1-s}} - \dfrac{1}{1-5\omega(h_0)}\right)$	$R+2^{d_2+f_2}+v(2)$
" $=-1$		$R+2v(2)$
" $=1$		$R+v(4s)+v(2)$

<u>Remarques</u>. Il semble que le seul cadre où des résultats analytiques voisins (i.e. de type additif) aient été observés soit celui des corps quadratiques (voir notamment certaines formules dans [L] et [H]). Signalons que les con-

gruences que nous obtenons ici sont nouvelles et indépendantes des "congruences classiques" (cf. [W, 4. 17, 5. 24] ou leurs généralisations (cf. [G2, (0. 3)]), car ces dernières reviennent essentiellement à comparer $\frac{1}{2}L_p(\chi, t)$ et $\frac{1}{2}L_p(\chi, s)$, $s, t \in \mathbb{Z}_p$ convenables, ce qui conduit à des congruences entre les invariants arithmétiques correspondants.

Par contre, les résultats de divisibilités obtenus dans [G 1, (0. 3)] et [G2, (0. 2)] montrent que les congruences obtenues ici ne se réduisent pas, en général, à la congruence triviale. Pour $p = 2$ et à partir d'un caractère quadratique, les théorèmes (0. 2) et (0. 3) conduisent à des congruences additives générales entre nombres de classes et logarithmes 2-adiques d'unités fondamentales, de corps quadratiques réels et imaginaires.

§ 1. Groupes de Galois :

Soit S un ensemble fini de nombres premiers ; les considérations générales de ce paragraphe sont indépendantes du choix d'un nombre premier p ou d'un caractère χ.

(1. 1) Définitions générales. (i) Pour toute partie U de S, on désigne par $\mathbb{Q}_U$ l'extension maximale de $\mathbb{Q}$ dans $\mathbb{Q}^{ab}$, non ramifiée en dehors de $U \cup \{\infty\}$, et on pose $G_U = \mathrm{Gal}(\mathbb{Q}_U/\mathbb{Q})$; le corps $\mathbb{Q}_U$ est le composé direct sur $\mathbb{Q}$ des corps $\mathbb{Q}_{\{q\}}$, $q \in U$, et on a $G_U \simeq \prod_{q \in U} \mathbb{Z}_q^*$.

(ii) Pour tout $q \in S$, on désigne par H_q le groupe d'inertie de q dans $\mathbb{Q}_S/\mathbb{Q}$; c'est aussi le groupe de Galois $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}_{S-\{q\}})$. Les groupes H_q sont procycliques pour tout $q \neq 2$; si $2 \in S$, on peut écrire $H_2 = H_{-1} \oplus H_o$, où $H_{-1} = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}_{S-\{2\}}\mathbb{Q}_\infty)$ ($\mathbb{Q}_\infty$ désignant, dans ce cas, la $\mathbb{Z}_2$-extension cyclotomique de $\mathbb{Q}$), et $H_o = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}_{S-\{2\}}(\sqrt{-1}))$ ou $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}_{S-\{2\}}(\sqrt{-2}))$; on a donc finalement $G_S = \bigoplus_{q \in S} H_q$ (resp. $G_S = \bigoplus_{t \in (S-\{2\}) \cup \{-1, 0\}} H_t$) si $2 \notin S$ (resp. $2 \in S$).

Remarque. Le choix entre les deux possibilités concernant H_o pourra dépendre du caractère χ qui sera utilisé.

Certaines des notations suivantes ont déjà été données en (0. 1) :

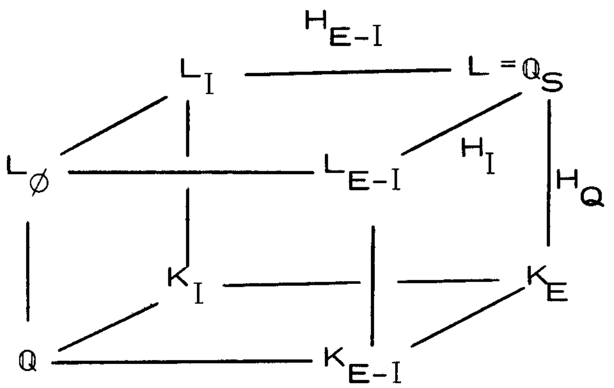
(1. 2) Notations. (i) On pose $P = S$ (resp. $P = (S-\{2\}) \cup \{-1, 0\}$) dans le cas où $2 \notin S$ (resp. $2 \in S$) ;

(ii) pour toute partie J de P on pose $H_J = \bigoplus_{t \in J} H_t$, et on appelle K_J le sous-corps de $\mathbb{Q}_S$ fixe par H_{P-J} ; on a en particulier $\mathbb{Q} = K_\emptyset$, $\mathbb{Q}_S = K_P$ et $H_P = H_J \oplus H_{P-J}$ (i. e. K_P est le composé direct sur $\mathbb{Q}$ de K_J et K_{P-J}) ;

(iii) on fixe une partie E de P, et on pose $Q = P-E$.

Afin de faire jouer à E un rôle privilégié, on introduit les notations supplémentaires suivantes :

(1. 3) Notations. (i) On pose $L = \mathbb{Q}_S$, et pour tout $I \subseteq E$, on désigne par L_I le sous-corps de L fixe par H_{E-I} ; on a donc, en supposant que pour tout $I \subseteq E$ on pose systématiquement $J = I \cup Q$, l'égalité $L_I = K_J$; en particulier, on a $L_\emptyset = K_Q$, $L_E = K_P = L$. Pour tout $I \subseteq E$, on a $H_E = H_I \oplus H_{E-I}$, et L est le composé direct sur $L_\emptyset = K_Q$ de L_I et L_{E-I} ; en résumé on a le schéma suivant :



$L_I = K_{I \cup Q}$, $I \subseteq E$

(ii) on pose $\Gamma_I = \mathrm{Gal}(L_I/\mathbb{Q}) \simeq G_S/H_{E-I}$, pour tout $I \subseteq E$;

(iii) pour tout $t \in P$ on désigne par h_t un progénérateur de H_t, et on pose $y_t = 1 - h_t^{-1} \in \mathbb{Z}[G_S]$.

(1. 4) Remarque. Le choix de E est arbitraire et on obtiendra autant de relations congruentielles ; il sera toujours possible de prendre $E = P$, cependant, relativement au choix d'un nombre premier p, la partie E la plus intéressante (notamment en ce qui concerne le module de la congruence) sera constituée des $t \in P$ tels que $1 - \omega^{-1}\chi(h_t)$ est non inversible modulo p (i. e., si l'on écrit $\chi = \varphi\psi$, φ d'ordre étranger à p, ψ d'ordre puissance de p, la condition équivaut à $\omega^{-1}\varphi(h_t) = 1$ (resp. $\varphi(h_t) = 1$) si $p \neq 2$ (resp. $p = 2$), c'est-à-dire à des conditions élémentaires portant sur la ramification dans le sous-corps M_o de $\mathbb{Q}^{ab}$ correspondant au noyau de $\omega^{-1}\varphi$ (resp. φ)).

Avec ces notations on va pouvoir définir et étudier les mesures et distributions p-adiques sur G_S.

§ 2. Algèbres des $\mathbb{Z}_p$-mesures et distributions sur G_S - congruence générale.

On rappelle que l'algèbre Λ_{G_S} des $\mathbb{Z}_p$-mesures sur G_S est par définition $\varprojlim_{\Omega} \mathbb{Z}_p[G_S/\Omega]$, où Ω parcourt l'ensemble des sous-groupes ouverts de G_S ; on a appelé, dans [G2, (2. 11)], $\mathbb{Z}_p$-distribution, tout élément de l'anneau total des fractions Δ_{G_S} de Λ_{G_S}.

(2.1) Notations. Pour tout sous-corps F de $L = \mathbb{Q}_S$, on désigne par Λ_F l'algèbre des $\mathbb{Z}_p$-mesures sur $\mathrm{Gal}(F/\mathbb{Q})$, et on dit, par abus, qu'un élément de Λ_F est une $\mathbb{Z}_p$-mesure de F. De même, Δ_F désigne l'ensemble des $\mathbb{Z}_p$-distributions de F.

(2.2) Définitions. (i) Pour tout sous-corps F de L, on désigne par $\mathrm{proj}_{L,F} : \Lambda_L \to \Lambda_F$ l'application qui prolonge par $\mathbb{Z}_p$-linéarité et continuité l'application canonique $G_S \to \mathrm{Gal}(F/\mathbb{Q})$;

(ii) pour toute partie I de E, on désigne par $\mathrm{ext}_{L_I,L}$ l'isomorphisme canonique $\Lambda_{L_I} \to \Lambda_{H_Q \oplus H_I}$ (où $\Lambda_{H_I \oplus H_Q}$ est considérée comme sous-algèbre de $\Lambda_{G_S} = \Lambda_L$) et qui est induit par l'isomorphisme canonique $\Gamma_I \to H_Q \oplus H_I$ (cf. (1.2), (1.3)).

Remarque. On sait que $\mathrm{proj}_{L,F}$ ne s'étend pas nécessairement à l'ensemble Δ_L des $\mathbb{Z}_p$-distributions de L : il faut pour cela que le dénominateur des distributions considérées ait une projection non diviseur de 0 dans Λ_F, ce qui sera le cas en pratique, et ce, pour tout $F \subseteq L$; par contre l'application $\mathrm{ext}_{L_I,L}$ a cette propriété : en effet, si $\nu_{L_I} \delta_{L_I}^{-1}$ est une distribution de L_I ($\delta_{L_I} \in \Lambda_{L_I}$, non diviseur de 0 dans Λ_{L_I}), $\mathrm{ext}_{L_I,L}(\delta_{L_I})$ est non diviseur de 0 dans Λ_L, et ceci définit sans ambiguité la distribution $\mathrm{ext}_{L_I,L}(\nu_{L_I})(\mathrm{ext}_{L_I,L}(\delta_{L_I}))^{-1}$ de L.

(2.3) Notations. Pour toute mesure (ou distribution) ν_L de L, et tout $F \subseteq L$, on pose $\nu_{L,F} = \mathrm{proj}_{L,F}(\nu_L)$; de même, pour toute distribution ν_{L_I} de L_I, $I \subseteq E$, on pose $\nu_{L_I,L} = \mathrm{ext}_{L_I,L}(\nu_{L_I})$.

(2.4) Remarque. L'expression $\nu_{L,L_I,L}$ représente donc $\mathrm{ext}_{L_I,L} \circ \mathrm{proj}_{L,L_I}(\nu_L)$ qui est en général distincte de ν_L.

Les relations congruentielles que nous avons en vue reposent sur le résultat essentiel suivant :

(2.5) Théorème. Soit ν_L une $\mathbb{Z}_p$-mesure de L ; alors on a la congruence (cf. (1.3), (2.2), (2.3), (2.4)) :

$$\sum_{I \subseteq E} (-1)^{|I|} \nu_{L,L_I,L} \equiv 0 \text{ modulo } \Big(\prod_{t \in E} y_t\Big) \Lambda_L .$$

Démonstration.

Soit G' un sous-groupe ouvert de G_S, de la forme $G' = \bigoplus_{t \in P} H'_t$ (cf. (1.2)), H'_t

ouvert dans H_t. On considère le sous-corps $\bar{L}$ de L fixe par G' ; on pose $\bar{G}_S = \mathrm{Gal}(\bar{L}/\mathbb{Q}) \simeq G_S/G' = \bigoplus_{t\in P} \bar{H}_t$, où $\bar{H}_t = H_t/H'_t$.

On définit alors de façon évidente, $\bar{H}_J$, $\bar{K}_J$, pour tout $J \subseteq P$, $\bar{L}_I$, $\bar{\Gamma}_I$, $\Lambda_{\bar{L}_I}$, $\mathrm{proj}_{\bar{L},\bar{L}_I}$, $\mathrm{ext}_{\bar{L}_I,\bar{L}}$, pour tout $I \subseteq E$, puis $\bar{h}_t$, $\bar{y}_t$, pour tout $t \in P$ (cf. (1.2), (1.3)).

Pour toute partie J de P on pose $Y_J = (Y_t)_{t\in J}$ et $\bar{y}_J = (\bar{y}_t)_{t\in J}$. Ici on a $\Lambda_{\bar{L}} = \mathbb{Z}_p[\bar{G}_S] = \mathbb{Z}_p[\bar{y}_P]$, et de même, $\mathbb{Z}_p[\bar{H}_I] = \mathbb{Z}_p[\bar{y}_I]$, pour tout $I \subseteq E$. On remarque que $\Lambda_{\bar{L}} = \Lambda[\bar{y}_E]$, où $\Lambda = \mathbb{Z}_p[\bar{y}_Q]$ $(Q = P-E)$.

D'après [G2, (2.9)], si ν est un polynôme de $\Lambda[Y_E]$, tel que $\nu_{\bar{L}} = \nu(\bar{y}_E)$, il vient, en écrivant $\bar{y}_E = (\bar{y}_I, \bar{y}_{E-I})$, $\nu_{\bar{L}} \equiv (-1)^{|E|-1} \sum_{I \subsetneq E} (-1)^{|I|} \nu(\bar{y}_I, 0)$ modulo $(\prod_{t\in E} \bar{y}_t)\Lambda_{\bar{L}}$; or d'après [G2, (2.10)], on a $\nu(\bar{y}_I, 0) = \nu_{\bar{L},\bar{L}_I,\bar{L}}$ (cf. (2.3), (2.4)), pour tout $I \subseteq E$, d'où la congruence

$$\nu_{\bar{L}} \equiv (-1)^{|E|-1} \sum_{I \subsetneq E} (-1)^{|I|} \nu_{\bar{L},\bar{L}_I,\bar{L}} \quad \mathrm{mod}\,(\prod_{t\in E} \bar{y}_t)\Lambda_{\bar{L}} \, .$$

Comme $\nu_{\bar{L},\bar{L}_I,\bar{L}} = \mathrm{proj}_{L,\bar{L}}(\nu_{L,L_I,L})$, la compacité de Λ_L conduit immédiatement au résultat.

§ 3. Distributions de Stickelberger. Faisons choix d'un nombre premier p non nécessairement dans S.

(3.1) Définition. Soit $\sigma \in G_{S\cup\{p\}}$, choisi de telle sorte que $\langle\sigma\rangle \neq 1$ (i.e. $N\sigma \notin \mathrm{tor}(\mathbb{Z}_p^*)$), et soit $\delta_{\mathbb{Q}_S} = 1 - N\sigma\,\sigma^{-1}$; on sait (cf. [G2, (3.4)]) que pour tout sous-corps F de $\mathbb{Q}_S$, $\delta_F = \mathrm{proj}_{\mathbb{Q}_S,F}(\delta_{\mathbb{Q}_S})$ est non diviseur de 0 dans $\Lambda_{\mathrm{Gal}(F/\mathbb{Q})}$.

On sait que pour tout $U \subseteq S$, il existe une distribution $\mu_{\mathbb{Q}_U}$ de $\mathbb{Q}_U$, de dénominateur $\delta_{\mathbb{Q}_U}$, que nous avons appelée dans [G2, §3] la distribution de Stickelberger de $\mathbb{Q}_U$. Rappelons les principales propriétés fonctionnelles de ces $\mathbb{Z}_p$-distributions (cf. [G2, (3.6) à (3.9)]) :

(3.2) $$\delta_{\mathbb{Q}_U}\,\mu_{\mathbb{Q}_U} \in \Lambda_{G_U} \, ;$$

(3.3) $$\mu_{\mathbb{Q}_U,\mathbb{Q}_V} = \mu_{\mathbb{Q}_V} \prod_{q\in U-V} \left(1 - \left(\frac{\mathbb{Q}_V/\mathbb{Q}}{q}\right)^{-1}\right), \text{ pour tout } V \subseteq U \, ,$$

où $\left(\frac{\mathbb{Q}_V/\mathbb{Q}}{q}\right)$ est le Frobenius de q dans $\mathbb{Q}_V/\mathbb{Q}$; plus généralement on a

(3. 4) $$\mu_{F,F'} = \mu_{F'} \prod_{q} \left(1-\left(\frac{F'/\mathbb{Q}}{q}\right)^{-1}\right),$$

pour tous sous-corps imaginaires F, F', $F' \subseteq F \subseteq \mathbb{Q}_S$, où q parcourt l'ensemble des nombres premiers ramifiés dans $F/\mathbb{Q}$ et non ramifiés dans $F'/\mathbb{Q}$, où l'on a posé d'une façon générale $\mu_F = \mu_{\mathbb{Q}_U, F}$, U étant le sous-ensemble minimum de S tel que $F \subseteq \mathbb{Q}_U$; lorsqu'on a en outre $[F:\mathbb{Q}]<\infty$, on sait que

(3. 5) $$\mu_F = -\sum_{\substack{a=1 \\ (a,U)=1}}^{f} \left(\frac{F/\mathbb{Q}}{a}\right)^{-1} \left(\frac{a}{f}-\frac{1}{2}\right),$$

où f désigne le conducteur de $F \subseteq \mathbb{Q}_U$; enfin on a

$$(\mu_F)_{F\subseteq \mathbb{Q}_U} \in \varprojlim_{F} \mathbb{Q}[\mathrm{Gal}(F/\mathbb{Q})] \text{ (où } [F:\mathbb{Q}]<\infty,\ F \not\subseteq \mathbb{Q}_V \text{ si } V \subsetneq U) ;$$

(3. 6) on a $m(\mu_{\mathbb{Q}_U}) = \lambda_{\mathbb{Q}_U}$, pour tout U contenant p, où $\lambda_{\mathbb{Q}_U}$ est la $\mathbb{Z}_p$-pseudo-mesure de Deligne-Ribet associée à la construction des fonctions L p-adiques des caractères de $\mathbb{Q}_U$, m étant la transformée de Mellin p-adique (cf. [G2, (3. 10)]), qui à $\tau \in G_U$ associe $N\tau\, \tau^{-1}$.

Si $p \in S$, et si l'on choisit $\sigma \in G_S$ tel que $G_S = A_S \oplus \sigma^{\mathbb{Z}_p}$, où $A_S = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}_\infty)$ (choix qui est compatible avec (3. 1)), on a (cf. [S , (1. 15)]):

(3. 7) $$\lambda_{\mathbb{Q}_S} \equiv c_{\mathbb{Q}_S}\, \alpha_{A_S} (1-\sigma)^{-1} \bmod \Lambda_{\mathbb{Q}_S},\quad c_{\mathbb{Q}_S} \in \mathbb{Z}_p^*,$$

où α_{A_S} est la mesure de Haar sur A_S, normalisée de telle sorte que $\langle 1, \alpha_{A_S}\rangle = |A_{S,p}|$ (l'ordre du p-Sylow de A_S).

(3. 8) <u>Lemme</u>. L'unité p-adique $c_{\mathbb{Q}_S}$ est la composante sur $\mathbb{Z}_p^*$ de

$$\log\langle\sigma\rangle \prod_{q\in S} (1-q^{-1}),$$

considéré dans $\mathbb{Z}_p - \{0\} = p^{\mathbb{N}} \times \mathbb{Z}_p^*$.

<u>Remarque</u>. Ultérieurement on prendra σ tel que $N\sigma = 1+p$ si $p \neq 2$, $N\sigma = 5$ si $p=2$.

Démonstration du lemme (voir aussi [S]).

Il suffit de calculer le résidu en $s=1$ de la fonction zéta p-adique (non primitive) $\langle \langle\ \rangle^{1-s}, \lambda_{\mathbb{Q}_S}\rangle = \langle \langle\ \rangle^{1-s}, \lambda_{\mathbb{Q}_{\{p\}}}\rangle \prod_{\ell \in S-\{p\}} (1-\langle \ell\rangle^{1-s}\ell^{-1})$, d'après les propriétés eulériennes de $\lambda_{\mathbb{Q}_S}$ (cf. [G. 1, (4.6)]) ; or la seconde intégrale est $L_p(1,s)$ (fonction zéta p-adique de $\mathbb{Q}$) dont le résidu en s=1 est $1-\frac{1}{p}$. D'où le résidu cherché égal à $\prod_{q\in S}(1-q^{-1})$. Par ailleurs, d'après (3.7), on a $\langle\langle\,\rangle^{1-s}, \lambda_{\mathbb{Q}_S}\rangle \equiv c_{\mathbb{Q}_S}|A_{S,p}|(1-\langle\sigma\rangle^{1-s})^{-1} \bmod 1$ et le résidu précédent est aussi égal à $c_{\mathbb{Q}_S}|A_{S,p}|(\log\langle\sigma\rangle)^{-1}$;

$$\text{or } |A_{S,p}| = \prod_{\ell\in S-\{p\}}(1-\ell^{-1})_p \quad \text{si } p\neq 2$$

$$= 2\prod_{\ell\in S-\{2\}}(1-\ell^{-1})_2 \quad \text{si } p=2 \quad (\text{cf. } (3.9), (iv)).$$

D'où

$$c_{\mathbb{Q}_S} = \log\langle\sigma\rangle\,\frac{p-1}{p'}\prod_{\ell\in S-\{p\}}\frac{1-\ell^{-1}}{(1-\ell^{-1})_p}, \quad \text{où } p'=p \text{ ou } 4 \;;$$

d'où le résultat.

(3.9) <u>Définitions.</u> (i) On désigne par $\mathbb{Q}_\infty$ la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$ (on a évidemment $\mathbb{Q}_\infty \subseteq \mathbb{Q}_S$ si et seulement si $p\in S$) ;

(ii) pour tout sous-corps F de $\mathbb{Q}_S$, on pose $G_F = \mathrm{Gal}(F/\mathbb{Q})$ et on définit le sous-groupe A_F de G_F de la manière suivante : on pose $A_F = G_F$ si le p-Sylow $G_{F,p}$ de G_F est fini (ce qui équivaut à $\mathbb{Q}_\infty \not\subseteq F$), dans le cas contraire, on a $\mathbb{Q}_\infty \subseteq F$ et on pose $A_F = \mathrm{Gal}(F/\mathbb{Q}_\infty)$; lorsque $F=\mathbb{Q}_U$, on pose aussi $A_{\mathbb{Q}_U} = A_U$ (puisqu'alors $G_{\mathbb{Q}_U}$ a toujours été noté G_U) ;

(iii) on désigne par α_{A_F} la $\mathbb{Z}_p$-mesure de Haar sur A_F, normalisée de telle sorte que $\langle 1, \alpha_{A_F}\rangle = |A_{F,p}|$;

(iv) pour tout rationnel $c\neq 0$, $(c)_p$ désigne la p-partie de c.

<u>Congruences générales entre les distributions de Stickelberger.</u>

Par commodité, on distingue les cas $p\neq 2$ et $p=2$; on revient aux notations introduites dans les paragraphes 1 et 2 (cf. (1.2), (1.3), (2.1), (2.2.), (2.3)) :

(i_p) <u>cas $p\neq 2$.</u> On suppose dans (3.1) σ choisi tel que $N\sigma\equiv 1 \bmod p$, $N\sigma\not\equiv 1 \bmod p^2$ (i.e. $(N\sigma)^{\mathbb{Z}_p} = 1+p\mathbb{Z}_p$). On rappelle que l'on a posé $P=S$ si $2\notin S$ et $P=(S-\{2\})\cup\{-1,0\}$ si $2\in S$, et que l'on fixe une partie E de P.

(3.10) <u>Lemme</u>. (i) Si $p\neq 2$ et $p\notin S$, on a $\mu_L\in\Lambda_L$;

(ii) si $p\neq 2$ et $p\in S$, on a $\mu_L \equiv c_L\, m(\alpha_{A_L})\,\delta_L^{-1} \bmod \Lambda_L$.

Le cas (i) provient directement de (3.5) appliqué à $U = S$ lorsque $p \neq 2$ et $p \notin S$; le cas (ii) provient du théorème de structure de Serre rappelé en (3.7), compte-tenu du choix de σ : il suffit de transformer (3.7) par m.

Dans le cas (i) de (3.10), le théorème (2.5) conduit à la congruence suivante :

$$\sum_{I \subseteq E} (-1)^{|I|} \mu_{L,L_I,L} \equiv 0 \bmod (\prod_{t \in E} y_t)\Lambda_L \ ;$$

or on a $\mu_{L,L_I} = \mu_{L_I} \prod_{H_q \subseteq H_{E-I}} (1 - (\frac{L_I/\mathbb{Q}}{q})^{-1})$ d'après (3.4), d'où la congruence ($p \neq 2, p \notin S$) :

$$(3.11) \qquad \sum_{I \subseteq E} (-1)^{|I|} \mu_{L_I,L} \prod_{H_q \subseteq H_{E-I}} (1 - (\frac{L_I/\mathbb{Q}}{q})_L^{-1}) \equiv 0 \bmod (\prod_{t \in E} y_t)\Lambda_L .$$

Dans le cas (ii) de (3.10), écrivons

$$\mu_L = c_L\, m(\alpha_{A_L})\, \delta_L^{-1} + \nu_L \ , \ \nu_L \in \Lambda_L ,$$

et appliquons le théorème (2.5) à ν_L ; il conduit à la congruence

$$\sum_{I \subseteq E} (-1)^{|I|} \nu_{L,L_I,L} \equiv 0 \bmod (\prod_{t \in E} y_t)\Lambda_L ,$$

soit

$$\sum_{I \subseteq E} (-1)^{|I|} (\mu_{L,L_I,L} - c_L\, m(\alpha_{A_L})_{L_I,L}\, \delta_{L_I,L}^{-1}) \equiv 0 \bmod (\prod_{t \in E} y_t)\Lambda_L ,$$

d'où, en utilisant (3.4),

$$\sum_{I \subseteq E} (-1)^{|I|} \mu_{L_I,L} \prod_{H_q \subseteq H_{E-I}} (1 - (\frac{L_I/\mathbb{Q}}{q})_L^{-1}) \equiv$$

$$c_L \sum_{I \subseteq E} (-1)^{|I|}\, m(\alpha_{A_L})_{L_I,L}\, \delta_{L_I,L}^{-1} \bmod (\prod_{t \in E} y_t)\Lambda_L .$$

Posons $\Omega = \mathrm{Gal}(L/\mathbb{Q}_{S-\{p\}}\mathbb{Q}_\infty)$; alors on a

$$A_L = \Omega \oplus B_L \ , \ \text{où } B_L = \mathrm{Gal}(L/\mathbb{Q}_{\{p\}}),$$

et il vient

$$\alpha_{A_L} = \alpha_\Omega \alpha_{B_L} = \frac{1}{p-1} (\sum_{\tau \in \Omega} \tau)\alpha_{B_L} ,$$

d'où

$$m(\alpha_{A_L}) = \frac{1}{p-1} (\sum_{\tau \in \Omega} \omega(\tau)\tau^{-1})\alpha_{B_L} \quad (\text{cf. } (3.6)).$$

Si $p \in E-I$ (ce qui implique $L_I \subseteq \mathbb{Q}_{S-\{p\}}$) il est clair que $m(\alpha_{A_L})_{L_I} = 0$; si

$p \notin E-I$, on a $\mathbb{Q}_{\{p\}} \subseteq L_I$ et on a donc

$$m(\alpha_{A_L})_{L_I} = \frac{1}{p-1}\left(\sum_{\tau\in\Omega} \omega(\tau)\,\tau_{L_I}^{-1}\right)\alpha_{B_{L_I}} \prod_{\ell\in(E-I)\cap S} (1-\ell^{-1})_p ,$$

où $B_{L_I} = \mathrm{Gal}(L_I/\mathbb{Q}_{\{p\}})$; mais $\tau_{L_I, L} = \tau$, et par conséquent, on obtient la congruence ($p \neq 2$, $p\in S$) :

$$(3.12)\qquad \sum_{I\subseteq E} (-1)^{|I|}\,\mu_{L_I, L} \prod_{H_q \subseteq H_{E-I}} \left(1-\left(\frac{L_I/\mathbb{Q}}{q}\right)_L^{-1}\right) \equiv$$

$$\frac{c_L}{p-1}\left(\sum_{\tau\in\Omega} \omega(\tau)\,\tau^{-1}\right) \sum_{\substack{I\subseteq E\\ p\notin E-I}} (-1)^{|I|} \prod_{\ell\in(E-I)\cap S} (1-\ell^{-1})_p\, \alpha_{B_{L_I}L}\, \delta_{L_I, L}^{-1}$$

$$\bmod \left(\prod_{t\in E} y_t\right)\Lambda_L .$$

(i_2) <u>Cas $p=2$.</u> On suppose dans (3. 1) σ choisi tel que l'on ait $N\sigma \equiv \pm 1 \bmod 4$, $N\sigma \not\equiv \pm 1 \bmod 8$.

On a toujours $E \subseteq S$ si $p=2\notin S$ et $E\subseteq P=(S-\{2\})\cup\{-1, 0\}$ si $p=2\in S$.

(3. 13) <u>Lemme</u>. (i) Si $p=2\notin S$, on a $\mu_L \equiv \frac{1}{2}\alpha_{A_L} \bmod \Lambda_L$;

(ii) si $p=2\in S$, on a $\mu_L \equiv c_L\, m(\alpha_{A_L})\,\delta_L^{-1} \bmod \Lambda_L$.

Le cas (i) résulte facilement de (3. 5), et le cas (ii) de (3. 7) compte-tenu du choix de σ.

Dans le cas (i) de (3. 13), posons

$$\mu_L = \frac{1}{2}\alpha_{A_L} + \nu_L , \quad \nu_L \in \Lambda_L ;$$

le théorème (2. 5), appliqué à ν_L, conduit à la congruence

$$\sum_{I\subseteq E} (-1)^{|I|}\,\nu_{L, L_I, L} \equiv \sum_{I\subseteq E} (-1)^{|I|}\Big(\mu_{L_I, L} \prod_{\ell\in E-I} \left(1-\left(\frac{L_I/\mathbb{Q}}{\ell}\right)_L^{-1}\right) -$$

$$\frac{1}{2}\alpha_{A_L, L_I, L}\Big) \equiv 0 \bmod \left(\prod_{\ell\in E} y_\ell\right)\Lambda_L ,$$

d'où la congruence ($p=2\notin S$) :

$$(3.14)\qquad \sum_{I\subseteq E} (-1)^{|I|}\,\mu_{L_I, L} \prod_{\ell\in E-I} \left(1-\left(\frac{L_I/\mathbb{Q}}{\ell}\right)_L^{-1}\right) \equiv$$

$$\frac{1}{2}\sum_{I\subseteq E} (-1)^{|I|} \prod_{\ell\in E-I} (1-\ell^{-1})_2\, \alpha_{A_{L_I}, L} \bmod \left(\prod_{\ell\in E} y_\ell\right)\Lambda_L .$$

Dans le cas (ii) de (3. 13), on pose

$$\mu_L = c_L\, m(\alpha_{A_L})\,\delta_L^{-1} + \nu_L \quad , \quad \nu_L \in \Lambda_L ,$$

et on applique toujours le théorème (2. 5) à ν_L :

on obtient la congruence

$$\sum_{I \subseteq E} (-1)^{|I|}\, \nu_{L,L_I,L} \equiv 0 \bmod (\prod_{t\in E} y_t)\Lambda_L$$

soit

$$\sum_{I \subseteq E} (-1)^{|I|} (\mu_{L_I,L} \prod_{H_q \subseteq H_{E-I}} (1-(\frac{L_I/\mathbb{Q}}{q})_L^{-1}) -$$

$$c_L\, m(\alpha_{A_L})_{L_I,L}\, \delta_{L_I,L}^{-1}) \equiv 0 \bmod (\prod_{t\in E} y_t)\Lambda_L ,$$

d'où

$$\sum_{I \subseteq E} (-1)^{|I|}\, \mu_{L_I,L} \prod_{H_q \subseteq H_{E-I}} (1-(\frac{L_I/\mathbb{Q}}{q})_L^{-1}) \equiv$$

$$c_L \sum_{I \subseteq E} (-1)^{|I|}\, m(\alpha_{A_L})_{L_I,L}\, \delta_{L_I,L}^{-1} \bmod (\prod_{t\in E} y_t)\Lambda_L .$$

On a $\alpha_{A_L} = (1+h_{-1})\alpha_{B_L}$, où $B_L = \mathrm{Gal}(L/\mathbb{Q}_{\{2\}})$, d'où $m(\alpha_{A_L}) = (1-h_{-1})\alpha_{B_L}$; donc si $-1 \in E-I$, $m(\alpha_{A_L})_{L_I} = 0$; si $-1 \notin E-I$, on a $m(\alpha_{A_L})_{L_I} = (1-h_{-1,L_I})\,\alpha_{B_L,L_I} =$ $(1-h_{-1,L_I})\alpha_{B_{L_I}} \prod_{\ell \in (E-I)\cap S} (1-\ell^{-1})_2$, où $B_{L_I} = \mathrm{Gal}(L_I/\mathbb{Q}_{\{2\}})$, et $m(\alpha_{A_L})_{L_I,L} =$ $(1-h_{-1})\,\alpha_{B_{L_I}L} \prod_{\ell \in (E-I)\cap S} (1-\ell^{-1})_2$.

Dans ce cas, on obtient la congruence ($p=2 \in S$) :

$$\sum_{I \subseteq E} (-1)^{|I|}\, \mu_{L_I,L} \prod_{H_q \subseteq H_{E-I}} (1-(\frac{L_I/\mathbb{Q}}{q})_L^{-1}) \equiv \tag{3. 15}$$

$$c_L(1-h_{-1}) \sum_{\substack{I \subseteq E \\ -1 \notin E-I}} (-1)^{|I|} \prod_{\ell \in (E-I)\cap S} (1-\ell^{-1})_2\, \alpha_{B_{L_I}L}\, \delta_{L_I,L}^{-1}$$

$$\bmod (\prod_{t\in E} y_t)\Lambda_L .$$

<u>Remarque</u>. Lorsque $2 \notin S$, la condition $H_q \subseteq H_{E-I}$, dans (3. 11), (3. 12), (3. 15), équivaut à $q \in E-I$, et lorsque $2 \in S$, on a

$$\prod_{H_q \subseteq H_{E-I}} (1-(\frac{L_I/\mathbb{Q}}{q})^{-1}) = \prod_{\ell \in (E-I)\cap S} (1-(\frac{L_I/\mathbb{Q}}{\ell})^{-1}) \quad \text{si} \quad \{-1, 0\} \not\subseteq E-I ,$$

$$= (1-(\frac{L_I/\mathbb{Q}}{2})^{-1}) \prod_{\ell \in (E-I)\cap S} (1-(\frac{L_I/\mathbb{Q}}{\ell})^{-1}) \quad \text{sinon}.$$

<u>Caractères</u>. Soit X_L le groupe des caractères d'ordre fini de $L = \mathbb{Q}_S$; on peut écrire (cf. (1.2)) :

(3.16) $$X_L = \bigoplus_{t\in P} X_{K_{\{t\}}},$$

où $X_{K_{\{t\}}}$ est le groupe des caractères du corps $K_{\{t\}}$ fixe par $H_{P-\{t\}}$.

Tout caractère $\chi \in X_L$ se décompose donc de façon unique, dans

$X_L = \bigoplus_{t\in Q\cup I} X_{K_{\{t\}}} \bigoplus_{t\in E-I} X_{K_{\{t\}}} = X_{L_I} \oplus X_{K_{E-I}}$, sous la forme

(3.17) $$\chi = \chi_{L_I}\, \chi_{K_{E-I}},$$

où χ_{L_I} (resp. $\chi_{K_{E-I}}$) est un caractère de L_I (resp. K_{E-I}).

§4. <u>Intégrations.</u>

(4.1) <u>Définitions</u>. (i) On fixe un nombre premier p et un caractère χ d'ordre fini de $\mathbb{Q}^{ab}$, de parité quelconque, et on désigne par S_χ l'ensemble des diviseurs premiers du conducteur de χ. Enfin on pose $S = S_\chi$ ou $S = S_\chi \cup \{p\}$ (autrement dit, si $p \in S_\chi$ on a $S = S_\chi$, si $p \notin S_\chi$, on conserve les 2 possibilités $S = S_\chi$ ou $S = S_\chi \cup \{p\}$).

(ii) On fixe une partie E de $P = S$ (resp. de $P = (S-\{2\}) \cup \{-1, 0\}$) si $2 \notin S$ (resp. $2 \in S$).

<u>Intégrales</u>. On a rappelé dans [G2, (3.8),(3.2)] que si $p \in S$, on a $L_p(\chi, s) = \langle \chi\langle\ \rangle^{1-s}, \lambda_L\rangle = \langle \omega\chi^{-1}\langle\ \rangle^s, \mu_L\rangle$, pour tout $s \in \mathbb{Z}_p$ (cf. (3.6)). D'après (0.1), (iii), si $p \notin S$, on a alors $\langle \omega\chi^{-1}\langle\ \rangle^s, \mu_L\rangle = \langle \chi^{-1}, \mu_L\rangle = -B_1(\chi)$, où $B_1(\chi)$ est le premier nombre de Bernoulli généralisé (primitif) du caractère χ (cf. [W, ch. 4]) : en effet, si f_χ est le conducteur de χ, on obtient à partir de (3.5) l'expression :

(4.2) $$\langle \chi^{-1}, \mu_L\rangle = -\sum_{\substack{a=1\\(a,f_\chi)=1}}^{f_\chi} \chi(a)\left(\frac{a}{f_\chi} - \frac{1}{2}\right) = -B_1(\chi).$$

On considère maintenant les différentes congruences générales (3.11), (3.12), (3.14) et (3.15) ; on intègre le caractère $\omega\chi^{-1}\langle\ \rangle^s$ par rapport aux deux membres de ces congruences, et en tenant compte de (3.17).

(4. 3) Notations. (i) On désigne par c_χ (resp. $\mathfrak{M}_\chi$) l'intégrale de $\omega\chi^{-1}\langle\ \rangle^s$ par rapport au second membre de ces congruences (resp. par rapport au module les définissant) ;

(ii) on pose $R=\sum_\ell p^{d_\ell+f_\ell}$, où ℓ parcourt l'ensemble des éléments de $E\cap S$, distincts de p et non ramifiés dans $M_o/\mathbb{Q}$ (cf. (0. 1), (vi) à (viii)).

(i) Congruence (3. 11) ($p\neq 2$, $p\notin S$). Comme $\omega\langle\ \rangle^s$ est, sur $\mathrm{Gal}(\mathbb{Q}_{S\cup\{p\}}/\mathbb{Q}_{\{p\}})\simeq \mathrm{Gal}(L/\mathbb{Q})$, le caractère unité, on obtient

$$\sum_{I\subseteq E}(-1)^{|I|}(-B_1(\chi_{L_I}))\prod_{H_q\subseteq H_{E-I}}(1-\chi_{L_I}(q))\equiv 0 \bmod \mathfrak{M}_\chi ,$$

où $\mathfrak{M}_\chi=\prod_{t\in E}(1-\chi(h_t))\,\mathbb{Z}_p(\chi)$; on a $1-\chi(h_t)\in\mathbb{Z}_p(\chi)^*$ si et seulement si $\varphi(h_t)=1$; si $2\in S$, $1-\chi(h_{-1})$ et $1-\chi(h_o)$ sont inversibles ($p\neq 2$), et par conséquent, on peut se resteindre aux $\ell\in E\cap S$ tels que $\varphi(h_\ell)=1$; comme par ailleurs $\omega(\ell)=1$ pour de tels ℓ (ramifiés nécessairement dans M/M_o), on obtient facilement $v(\mathfrak{M}_\chi)=R$.

D'où la congruence ($p\neq 2$, $p\notin S$) :

(4. 4)
$$\sum_{I\subseteq E}(-1)^{|I|}B_1(\chi_{L_I})\prod_{H_q\subseteq H_{E-I}}(1-\chi_{L_I}(q))\equiv 0 \bmod \mathfrak{M}^R$$

(cf. (4. 3), (ii)).

(ii) Congruence (3. 12) ($p\neq 2$, $p\in S$). On a de même $\mathfrak{M}_\chi=\mathfrak{M}^R$ si p n'est pas dans E ou si $p\in E$ se ramifie dans $M_o/\mathbb{Q}$; on a $\mathfrak{M}_\chi=(1-\psi(h_p)\langle h_p\rangle^{-s})\mathfrak{M}^R$ si $p\in E$ est non ramifié dans $M_o/\mathbb{Q}$.

On a donc (cf. (4. 3), (ii)) le tableau suivant :

(4. 5)

	$v(\mathfrak{M}_\chi)$
$p\notin E$	R
$p\in E$, p ramifié dans $M_o/\mathbb{Q}$	R
$p\in E$, p non ramifié dans $M_o/\mathbb{Q}$ et ramifié dans M/M_o	$R+p^{d_p+f_p}$
$p\in E$, p non ramifié dans $M/\mathbb{Q}$	$R+v(ps)$

Considérons le corps $\mathbb{Q}_o$ des racines p-ièmes de l'unité et décomposons $\chi_{\mathbb{Q}_{\{p\}}}$ sous la forme $\chi_o\chi_\infty$ produit d'un caractère de $\mathbb{Q}_o$ et d'un caractère de $\mathbb{Q}_\infty$;

on remarque alors que $\langle \omega\chi^{-1}\langle\ \rangle^s, \sum_{\tau\in\Omega} \omega(\tau)\tau^{-1}\rangle = \langle \omega\chi_o^{-1}, \sum_{\tau\in\Omega}\omega(\tau)\tau^{-1}\rangle = 0$ si et seulement si $\chi_o \neq 1$.

Ensuite, pour $I \subseteq E$, $p \notin E-I$, on a $\langle \omega\chi^{-1}\langle\ \rangle^s, \alpha_{B_{L_I}}{}_{L}\rangle = \langle \chi_{L_I}^{-1}, \alpha_{B_{L_I}}\rangle = 0$, sauf si χ_{L_I} est le caractère unité sur B_{L_I} (i.e. si χ_{L_I} est un caractère de $\mathbb{Q}_{\{p\}}$) ; or par hypothèse on a $\mathbb{Q}_{\{p\}} \subseteq L_I$ et la seule possibilité est $L_I = \mathbb{Q}_{\{p\}}$, auquel cas $B_{L_I} = \{1\}$ et χ_{L_I} est caractère de $\mathbb{Q}_{\{p\}}$; ceci ne peut se produire que si $E = P$ $(I = \{p\})$ ou $E = P-\{p\}$ $(I = \emptyset)$.

Enfin, en supposant $\chi_o = 1$, on a $\langle \omega\chi^{-1}\langle\ \rangle^s, \delta_{\mathbb{Q}_{\{p\}},L}\rangle = \langle \omega\chi^{-1}\langle\ \rangle^s, 1-N\sigma\sigma^{-1}_{\mathbb{Q}_{\{p\}},L}\rangle = 1-\chi_\infty(\sigma)\langle\sigma\rangle^{1-s}$. D'où finalement, compte-tenu de (3. 8) :

(4. 6)

	c_χ
$\chi_o \neq 1$	0
$\chi_o = 1$, $P-E \nsubseteq \{p\}$	0
$\chi_o = 1$, $E=P$ ou $P-\{p\}$	$(-1)^{\lvert P-E\rvert+1}\log(1+p)\prod_{q\in S}(1-q^{-1})(1-\chi_\infty(1+p)(1+p)^{1-s})^{-1}$

D'où la congruence $(p \neq 2,\ p \in S)$:

(4. 7)
$$\sum_{\substack{I\subseteq E\\ p\in E-I}} (-1)^{|I|}(-B_1(\chi_{L_I}))\prod_{H_q\subseteq H_{E-I}}(1-\chi_{L_I}(q))$$
$$+\sum_{\substack{I\subseteq E\\ p\notin E-I}} (-1)^{|I|} L_p(\chi_{L_I}, s)\prod_{H_\ell\subseteq H_{E-I}}(1-\omega^{-1}\chi_{L_I}(\ell)\langle\ell\rangle^{-s})$$
$$\equiv c_\chi \bmod \mathfrak{M}_\chi \quad \text{(cf. (4. 5), (4. 6)).}$$

(4. 8) Remarque. On vérifie sans peine que si $\psi = \chi_\infty\psi'$, ψ' de conducteur étranger à p, avec $\chi_\infty \neq 1$ et $\psi' \neq 1$, alors le second membre c_χ est nul modulo $\mathfrak{M}_\chi$.

(iii) congruence (3. 14) $(p = 2 \notin S)$. Comme dans le cas (i), $\omega\langle\ \rangle^s$ est, sur $\mathrm{Gal}(\mathbb{Q}_{S\cup\{2\}}/\mathbb{Q}_{\{2\}})$, le caractère unité, et par conséquent l'intégrale du premier membre de (3. 14) est (puisqu'ici $E \subseteq S$) :

$$\sum_{I\subseteq E} (-1)^{|I|} (-B_1(\chi_{L_I})) \prod_{\ell\in E-I} (1-\chi_{L_I}(\ell)).$$

On a facilement $v(\mathfrak{M}_\chi)=R$ (cf. (4.3), (ii)).

Pour le second membre c_χ, les intégrales $\langle \chi_{L_I}^{-1}, \alpha_{A_{L_I}} \rangle$ sont nulles pour tout $I\subseteq E$ sauf dans l'unique cas où $E=S$, $I=\emptyset$, auquel cas on obtient $c_\chi = \frac{1}{2} \prod_{\ell\in S} (1-\ell^{-1})_2$.

S'il existe au moins un $\ell\in S$, $\ell\equiv 1 \bmod 4$, alors $c_\chi \equiv 0 \bmod 2^{|S|}$, soit $c_\chi \equiv 0 \bmod \mathfrak{M}_\chi$.

Supposons tout $\ell\in S$ congru à $-1 \bmod 4$; alors $c_\chi = 2^{|S|-1}$ et ψ est nécessairement d'ordre 1 ou 2. On a dans ce cas $R=|S'|$, où $S'=\{\ell\in S, \ell$ non ramifié dans $M_o/\mathbb{Q}\}$, et on a $2^{|S|-1}\equiv 0 \bmod 2^{|S'|}$ sauf dans l'unique cas où $S'=S$ qui implique $\varphi=1$ (en effet, $M_o/\mathbb{Q}$ est toujours ramifiée si $\varphi\neq 1$). D'où la congruence ($p=2\notin S$) :

(4.9)
$$\sum_{I\subseteq E} (-1)^{|I|} B_1(\chi_{L_I}) \prod_{\ell\in E-I} (1-\chi_{L_I}(\ell)) \equiv c_\chi \bmod \mathfrak{M}^R$$

(cf. (4.3), (ii)), où $c_\chi=0$ sauf dans l'unique cas suivant : $E=S$, $\varphi=1$ et ψ d'ordre 1 ou 2, et tout $\ell\in S$ congru à $-1 \bmod 4$, où $c_\chi = 2^{|S|-1}$.

<u>Remarque</u>. Soit χ_3 (resp. χ_7) le caractère quadratique de conducteur 3∞ (resp. 7∞) ; la congruence précédente conduit, pour $\chi=\chi_3$ ou χ_7, à $B_1(\chi)\equiv 1 \bmod 2$. Or on vérifie facilement que $B_1(\chi_3) = -\frac{1}{3}$ et que $B_1(\chi_7)=-1$, et la congruence (4.9) ne peut être améliorée.

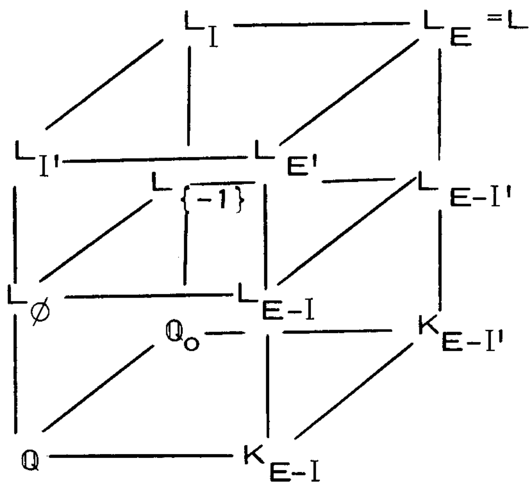
(iv) <u>Congruence (3.15)</u> ($p=2\in S$). Le calcul de $v(\mathfrak{M}_\chi)$ repose sur les facteurs $1-\omega\psi(h_\ell)$ ($\ell\in E\cap S$ non ramifié dans $M_o/\mathbb{Q}$), qui apportent la contribution R, et, le cas échéant, sur les facteurs $1-\omega\chi^{-1}\langle\ \rangle^s(h_{-1}) = 1+\chi(h_{-1})$ si $-1\in E$, et $1-\omega\chi^{-1}\langle\ \rangle^s(h_o^{-1})$ si $0\in E$.

Soit $\mathbb{Q}_o$ le sous-corps de $\mathbb{Q}_{\{2\}}$ fixe par h_o (cf. (1.1)) (on a $\mathbb{Q}_o=\mathbb{Q}(\sqrt{-1})$ ou $\mathbb{Q}(\sqrt{-2})$) ; si on décompose χ sous la forme $\chi=\chi_o\chi_\infty$, χ_o caractère de $\mathbb{Q}_o$, χ_∞ caractère de $\mathbb{Q}_\infty$, les facteurs ci-dessus s'écrivent respectivement $1+\chi_o(h_{-1})$ (=0 ou 2) et $1-\omega\chi_\infty(h_o)\langle h_o\rangle^{-s}$.

<u>Lemme</u>. Si $-1\in E$ et si $\chi_o\neq 1$, alors l'intégration de $\omega\chi^{-1}\langle\ \rangle^s$ par rapport à (3.15) conduit à $0\equiv 0 \bmod \mathfrak{M}_\chi$.

Posons $E'=E-\{-1\}$, et pour tout $I'\subseteq E'$, posons $I=I'\cup\{-1\}$. Le premier membre de (3.15) s'écrit sous la forme suivante :

$\sum_{I'\subsetneq E'} (-1)^{|I'|}(\mu_{L,L_{I'},L} - \mu_{L,L_I,L})$; or pour tout $I'\subsetneq E'$, on a $\mu_{L,L_{I'}} = (\mu_{L,L_I})_{L_{I'}}$ (car 2 est ramifié dans $L_I/L_{I'}$, (cf. (3.4)) ; considérons le schéma suivant :



On vérifie alors facilement que :

$$(\mu_{L,L_{I'},L} - \mu_{L,L_I,L})_{L_{E'}} = 0,$$

et on en déduit que le terme $\mu_{L,L_{I'},L} - \mu_{L,L_I,L}$ est dans $(1-h_{-1})\Delta_L$; d'où le lemme par intégration.

On peut donc désormais supposer que si $-1\in E$, alors $\chi_0 = 1$.

Le tableau suivant donne alors $v(\mathfrak{M}_\chi)$ en fonction des différentes situations possibles (cf. (4.3)) :

(4.10)

	$v(\mathfrak{M}_\chi)$
$\{-1, 0\}\cap E = \emptyset$	R
$0\notin E$, $-1\in E(\chi_0 = 1)$	$R + v(2)$
$0\in E$, $-1\notin E$,	
$\omega\chi_\infty(h_0) \neq \pm 1$	$R + 2^{d_2+f_2}$
$\omega\chi_\infty(h_0) = -1$	$R + v(2)$
$\omega\chi_\infty(h_0) = 1$	$R + v(4s)$
$\{-1, 0\}\subseteq E(\chi_0 = 1)$,	
$\omega\chi_\infty(h_0) \neq \pm 1$	$R + v(2) + 2^{d_2+f_2}$
$\omega\chi_\infty(h_0) = -1$	$R + 2v(2)$
$\omega\chi_\infty(h_0) = 1$	$R + v(2) + v(4s)$

Calculons maintenant c_χ ; on a $c_\chi=0$ dès que $\chi_o\neq 1$ et il reste à étudier le cas où $\chi_o=1$. Pour $I\subseteq E$ telle que $-1\notin E-I$, les intégrales $\langle \omega\chi^{-1}\langle\ \rangle^s, \alpha_{B_{L_I}}\rangle = \langle \chi_{L_I}^{-1}, \alpha_{B_{L_I}}\rangle$ sont nulles sauf si χ_{L_I} est, sur B_{L_I}, le caractère unité, ce qui équivaut à $L_I\subseteq \mathbb{Q}_{\{2\}}$; ceci conduit aux possibilités suivantes :

$E=P$ ($I=\{-1\}, \{-1,0\}$; $L_I=\mathbb{Q}_o, \mathbb{Q}_{\{2\}}$),

$E=P-\{-1\}$ ($I=\emptyset, \{0\}$; $L_I=\mathbb{Q}_o, \mathbb{Q}_{\{2\}}$),

$E=P-\{0\}$ ($I=\{-1\}$; $L_I=\mathbb{Q}_{\{2\}}$),

$E=P-\{-1,0\}$ ($I=\emptyset$; $L_I=\mathbb{Q}_{\{2\}}$) ;

on vérifie facilement que $\langle \omega\chi^{-1}\langle\ \rangle^s, 1-N\sigma\,\sigma^{-1}_{\mathbb{Q}_o,L}\rangle = 1-\omega(h_o)\langle\sigma\rangle$ et que $\langle \omega\chi^{-1}\langle\ \rangle^s, 1-N\sigma\,\sigma_{\mathbb{Q}_{\{2\}},L}\rangle = 1-\chi_\infty(\sigma)\langle\sigma\rangle^{1-s}$; d'où c_χ :

(4. 11) $$c_\chi=\varepsilon_1\, 2c_L \prod_{\ell\in S-\{2\}}(1-\ell^{-1})_2\left(\frac{-1}{1-\omega(h_o)\langle\sigma\rangle}+\frac{1}{1-\chi_\infty(\sigma)\langle\sigma\rangle^{1-s}}\right),$$

dans les deux premiers cas,

$$c_\chi=\varepsilon_2\, 2c_L \prod_{\ell\in S-\{2\}}(1-\ell^{-1})_2\,\frac{1}{1-\chi_\infty(\sigma)\langle\sigma\rangle^{1-s}},$$

dans les deux derniers,

où $\varepsilon_1=+1$ si $E=P$, $\varepsilon_1=-1$ si $E=P-\{-1\}$,

$\varepsilon_2=-1$ si $E=P-\{0\}$, $\varepsilon_2=+1$ si $E=P-\{-1,0\}$.

Comme dans le cas (ii), la congruence obtenue comporte des nombres de Bernoulli et des fonctions L_2, l'expression des caractères χ_{L_I} étant compliquée par le fait que $H_2=H_{-1}\oplus H_o$, et que le groupe H_E utilisé peut contenir H_2, ou seulement H_{-1} ou H_o ; désignons par ω_o le caractère non trivial de $\mathbb{Q}_o$, on obtient la congruence ($p=2\in S$) :

(4. 12) $$\sum_{\substack{I\subseteq E\\ \{-1,0\}\subseteq E-I}}(-1)^{|I|}(-B_1(\chi_{L_I}))(1-\chi_{L_I}(2))\prod_{\ell\in(E-I)\cap S}(1-\chi_{L_I}(\ell))$$
$$+\sum_{\substack{I\subseteq E\\ 0\in E-I\\ -1\notin E-I}}(-1)^{|I|}(-B_1(\omega_o^{-1}\chi_{L_I}))\prod_{\ell\in(E-I)\cap S}(1-\omega_o^{-1}\chi_{L_I}(\ell))$$
$$+\sum_{\substack{I\subseteq E\\ -1\in E-I\\ 0\notin E-I}}(-1)^{|I|}L_2(\omega_o^{-1}\chi_{L_I},s)\prod_{\ell\in(E-I)\cap S}(1-\omega_o^{-1}\chi_{L_I}(\ell)\langle\ell\rangle^{-s})$$

$$+ \sum_{\substack{I \subseteq E \\ \{-1,0\} \cap (E-I) = \emptyset}} (-1)^{|I|} L_2(\chi_{L_I}, s) \prod_{\ell \in (E-I) \cap S} (1-\omega^{-1}\chi_{L_I}(\ell)\langle \ell \rangle^{-s})$$

$\equiv c_\chi \bmod \pi_\chi$, où π_χ est donné par le tableau (4. 10) et c_χ par le tableau suivant (cf. (3. 8), (4. 11)) :

(4. 13)

	c_χ
$\chi_o \neq 1$	0
$\chi_o = 1$, $P-E \not\subseteq \{-1, 0\}$	0
$\chi_o = 1$ et :	
$E = P$ ou $P-\{-1\}$	$(-1)^{\lvert P-E \rvert} \log 5 \prod_{q \in S} (1-q^{-1})((1-\chi_\infty(5)5^{1-s})^{-1}-(1-5\omega(h_o))^{-1})$
$E = P-\{0\}$ ou $P-\{-1, 0\}$	$(-1)^{\lvert P-E \rvert} \log 5 \prod_{q \in S} (1-q^{-1})(1-\chi_\infty(5)\,5^{1-s})^{-1}$

Les énoncés des théorèmes (0. 2) et (0. 3) se reconstituent alors à partir des résultats résumés dans les points (4. 4), (4. 7), (4. 9) et (4. 12).

Références

[G1] Gras G., Théorie des genres analytique des fonctions L p-adiques des corps totalement réels, Inv. Math. 86, 1-17 (1986).

[G2] Gras G., Pseudo-mesures p-adiques associées aux fonctions L de $\mathbb{Q}$, à paraître dans Manuscripta Mathematica.

[H] Hikita M., On the congruences for the class numbers of the quadratic fields whose discriminants are divisible by 8, J. of Number theory 23, 86-101 (1986).

[L] Lang H., Über die Klassenzahl quadratischer Zahlkörper, deren Diskriminanten nur ungerade Primteiler $p \equiv 1 \bmod 4$ besitzen Abh. Math. Sem. Univ. Hamburg 55, 147-150 (1985).

[W] Washington L. C., Introduction to cyclotomic fields, Grad. t. in Math., 83, Springer-Verlag, 1982.

Georges Gras
Université de Franche-Comté Besançon
Faculté des Sciences
Mathématiques
U.A. 0741
F - 25030 Besançon Cedex