ANNALES DE L'INSTITUT FOURIER

GEORGES GRAS

Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés

Annales de l'institut Fourier, tome 27, n° 1 (1977), p. 1-66

<http://www.numdam.org/item?id=AIF_1977__27_1_1_0>

Ann. Inst. Fourier, Grenoble
27,1 (1977), 1- 66

CLASSES D'IDÉAUX DES CORPS ABÉLIENS ET NOMBRES DE BERNOULLI GÉNÉRALISÉS

par Georges GRAS

INTRODUCTION

Soit l un nombre premier impair fixé. Soit K/Q une extension abélienne dont le degré est premier à l et soit $\mathcal{H}_K$ le l-groupe des classes de K. Il existe un certain nombre d'"informations" numériquement accessibles sur l'arithmétique de K, permettant d'approcher la structure de $\mathcal{H}_K$ (considéré comme Gal(K/Q)-module), sans toutefois la déterminer systématiquement. Ces "informations" sont les suivantes :

i) Le résultat de Leopoldt sur l'interprétation arithmétique de la formule analytique du nombre de classes des corps abéliens réels [13], au moyen des unités cyclotomiques [19], [26] : Grâce à ce résultat, on peut atteindre le nombre de classes de ces corps en utilisant la méthode de "dévissage" des unités cyclotomiques [10], [11]. On peut alors se demander si les groupes d'unités ainsi rencontrés (unités modulo unités cyclotomiques) ne fournissent pas en réalité des précisions sur la structure de $\mathcal{H}_K$ (cf. Chap. V, § 2 et 3).

ii) Les nombres de Bernoulli généralisés : En effet, les nombres de Bernoulli de la forme $B_1(\underline{\chi}')$ ($\underline{\chi}'$ caractère de Dirichlet impair) permettent de calculer les nombres de classes relatives des corps imaginaires [13]. En outre, nous montrons (chap. I, § 2, f), que le théorème de Stickelberger [18], [7] sur l'annulation du groupe des classes relatives, s'exprime très simplement en terme de $B_1(\underline{\chi}')$; ceci permet d'obtenir des résultats partiels sur la structure de $\mathcal{H}_K^-$ (cf. [24], § 4 et 5). On peut aussi se demander, comme pour le cas réel, si ces résultats analytiques ne fournissent pas d'autres précisions sur la structure de $\mathcal{H}_K$ (cf. chap. V, § 2 et 3). Enfin les résultats de Leopoldt

[21], [22] et Fresnel [4], [5] sur les fonctions L_l l-adiques montrent que les nombres de Bernoulli $B_1(\underline{\chi}')$ donnent, sous certaines hypothèses supplémentaires, des conditions nécessaires de divisibilité par l des nombres de classes réelles : dans [21], Leopoldt suppose l non ramifié dans l'extension considérée ; les résultats de Fresnel permettent alors d'éliminer cette hypothèse dans tous les cas sauf un cas "spécial" ; ce cas sera défini dans le chap. III, § 2 (cf. Déf. III.4).

Nous avons établi, grâce à une méthode tout à fait différente, l'énoncé général pour cette question (cf. Th. IV .1 et Prop. IV.4).

iii) Le "Spiegelungssatz" de Leopoldt [23], [25] qui donne des relations entre les l-rangs de groupes de classes réelles et de groupes de classes imaginaires, constituant ainsi un lien partiel non trivial entre i) et ii) [22], [24].

Dans cet article, nous nous proposons de montrer que la juxtaposition de ces différentes "informations" permet d'obtenir des résultats partiels nouveaux sur la structure du groupe des classes des corps abéliens dans le cas "semi-simple".

Nous avons adopté le plan suivant :

Dans le chapitre I nous précisons tout le formalisme algébrique "semi-simple" qui est bien connu et qui permet de simplifier le problème posé et nous exprimons, dans ce cadre, les résultats classiques sur la structure des l-groupes de classes que nous venons de rappeler.

Dans le chapitre II, nous redonnons les définitions des nombres de Bernoulli généralisés et des sommes de Gauss et nous établissons un certain nombre de résultats techniques qui nous sont utiles dans les chapitres suivants.

Dans le chapitre III, nous caractérisons les unités cyclotomiques l-primaires au moyen des résultats de Fresnel afin de mettre en évidence le cas "spécial" dont nous avons parlé dans ii).

Dans le chapitre IV, nous décrivons une généralisation de la méthode utilisée dans [1] (chap. V, § 6) pour caractériser la régularité du nombre premier l ; c'est cette méthode (dite des séries formelles) qui nous permet d'englober le cas "spécial" et de donner un énoncé général. Comme nous le disons dans le chap. III, § 4, et dans le chap. IV, § 5, ce résultat doit pouvoir éclairer certains "défauts" inhérents à l'emploi des fonctions L_l classiques. A titre d'illustration de ce phénomène nous montrons que les congruences obtenues pour les corps quadratiques (et $l = 3$) par Ankeny, Artin et Chowla, dans le cas non "spécial" (cf. [17], pp. 155-156) existent aussi dans le cas "spécial".

Dans le chapitre V nous essayons de déduire des résultats précédents des précisions nouvelles sur la structure des $\mathcal{H}_K$ et nous donnons des illustrations diverses. Enfin nous posons quelques problèmes (que l'on pourrait énoncer sous forme de conjectures si la quantité d'exemples numériques dont on dispose à titre de vérification était plus importante).

Signalons pour terminer que le cas $l = 2$ est particulier et a fait l'objet des articles [8] et [9] (voir aussi [25]).

CHAPITRE PREMIER

RESULTATS GENERAUX SUR LA STRUCTURE DU l-GROUPE DES CLASSES DES EXTENSIONS ABELIENNES DE DEGRE PREMIER A l

1. Caractères abéliens.

Dans toute la suite, l est un nombre premier fixé impair. On appelle $\mathbf{Q}_0^a$ l'extension abélienne maximale de $\mathbf{Q}$ contenue dans une clôture algébrique $\overline{\mathbf{Q}}$ de $\mathbf{Q}$ et on appelle $\mathbf{Q}^a$ le composé de toutes les extensions abéliennes de $\mathbf{Q}$ de degré premier à l. On désigne par Ω_l une clôture algébrique de $\mathbf{Q}_l$ et par $\hat{\Omega}_l$ un complété de Ω_l ; on réalise une fois pour toutes un plongement $\overline{\mathbf{Q}} \to \Omega_l$ de telle sorte qu'on a le schéma d'extensions :

$$\begin{tikzcd}
 & \mathbf{Q}_l \arrow[r, -] \arrow[d, -] & \mathbf{Q}_l^a \arrow[rr, -] \arrow[d, -] & & \Omega_l \arrow[r, -] \arrow[d, -] & \hat{\Omega}_l \\
\mathbf{Q} \arrow[r, -] & \mathbf{Q}_l \cap \mathbf{Q}^a \arrow[r, -] & \mathbf{Q}^a \arrow[r, -] & \mathbf{Q}_0^a \arrow[r, -] & \overline{\mathbf{Q}} \arrow[r, -] & \mathbf{C}
\end{tikzcd}$$

où $\mathbf{Q}_l^a = \mathbf{Q}_l \mathbf{Q}^a$ est aussi le composé de toutes les extensions abéliennes de $\mathbf{Q}_l$ de degré premier à l. Ce procédé de plongement signifie en particulier que pour tout corps K de degré fini sur $\mathbf{Q}$, il existe une valuation $\mathfrak{L}$-adique sur K ($\mathfrak{L}$ idéal premier de K divisant l) unique pour laquelle un complété de K est contenu dans $\hat{\Omega}_l$. Par convention, nous noterons K_l ce complété bien déterminé au lieu de $K_{\mathfrak{L}}$ pour éviter une débauche d'idéaux premiers $\mathfrak{L}$.

On pose $\mathfrak{G}_0 = \mathrm{Gal}(\mathbf{Q}_0^a/\mathbf{Q})$ et $\mathfrak{G} = \mathrm{Gal}(\mathbf{Q}^a/\mathbf{Q})$

(On a $\mathfrak{G}_0 \simeq \varprojlim (\mathbf{Z}/n\mathbf{Z})^*$).

a) *Caractères de* $\mathfrak{G}_0$.

α) *Caractères de degré* 1. On appelle $\mathfrak{X}_0'$ l'ensemble des homomorphismes χ' de $\mathfrak{G}_0$ dans $\overline{\mathbf{Q}} \subset \hat{\Omega}_l$ dont le noyau $U_{\chi'}$ est fermé et d'indice fini dans $\mathfrak{G}_0$. On remarque que χ' est à valeurs dans le groupe des racines $g_{\chi'}^e$ de l'unité, où $g_{\chi'}$ est l'ordre de χ'.

β) *Caractères rationnels et l-adiques.* A partir de $\mathfrak{X}'_0$, on va définir plusieurs ensembles de caractères. Sur $\mathfrak{X}'_0$ on considère la relation d'équivalence suivante : on dit que χ' est équivalent à ψ' si les groupes engendrés par χ' et ψ' sont les mêmes ; il est équivalent de dire que $\mathrm{Ker}\ \chi' = \mathrm{Ker}\ \psi'$, ou encore que $\psi' = \chi'^k$ avec k premier à l'ordre de χ'. La deuxième caractérisation permet de définir la $\Gamma_{\mathbf{Q}}$-conjugaison [29], [27] : soit $g_{\chi'}$ l'ordre de χ' ; l'isomorphisme canonique de $\mathrm{Gal}(\mathbf{Q}^{(g_{\chi'})}/\mathbf{Q})$ sur $(\mathbf{Z}/g_{\chi'}\mathbf{Z})^*$ permet de donner un sens à la notation χ'^{σ} pour $\sigma \in \mathrm{Gal}(\mathbf{Q}^{(g_{\chi'})}/\mathbf{Q})$: on pose $\chi'^{\sigma} = \chi'^{a}$, où a est un représentant dans $\mathbf{Z}$ de l'image de σ par cet isomorphisme ; ainsi deux éléments de $\mathfrak{X}'_0$ sont équivalents si et seulement s'ils sont $\Gamma_{\mathbf{Q}}$-conjugués. Nous dirons que χ' et ψ' sont $\Gamma_{\mathbf{Q}_l}$-conjugués si $\psi' = \chi'^{\sigma}$, σ appartenant au sous-groupe de décomposition de l dans $\mathbf{Q}^{(g_{\chi'})}/\mathbf{Q}$. C'est une relation d'équivalence plus fine que la précédente. On posera :

$$\chi = \sum_{\psi' \sim \chi'} \psi' \quad \text{et} \quad \phi = \sum_{\psi' \sim \chi'} \psi',$$

respectivement pour la $\Gamma_{\mathbf{Q}}$ puis pour la $\Gamma_{\mathbf{Q}_l}$ équivalence, on notera $\widetilde{\chi}$ une $\Gamma_{\mathbf{Q}}$-classe et $\widetilde{\phi}$ une $\Gamma_{\mathbf{Q}_l}$-classe ; les applications χ et ϕ sont appelées respectivement les caractères rationnels (resp. l-adiques) irréductibles de $\mathfrak{G}_0$; on notera par $\mathfrak{X}_0$ (resp. Φ_0) l'ensemble des caractères χ (resp. ϕ). On remarque que χ est à valeurs dans $\mathbf{Z}$ et ϕ à valeurs dans $\mathbf{Z}_l \subset \hat{\Omega}_l$ (il suffit de constater que les valeurs de χ et ϕ sont des traces dans $\mathbf{Q}^{(g_{\chi'})}/\mathbf{Q}$ et $\mathbf{Q}_l^{(g_{\chi'})}/\mathbf{Q}_l$ respectivement).

Soit $\chi \in \mathfrak{X}_0$; pour $\chi' \in \widetilde{\chi}$, l'ordre $g_{\chi'}$, le noyau $\mathrm{U}_{\chi'}$, le sous-corps $\mathrm{K}_{\chi'}$ fixe par $\mathrm{U}_{\chi'}$, le groupe $\mathrm{G}_{\chi'} = \mathrm{Gal}(\mathrm{K}_{\chi'}/\mathbf{Q})$ ne dépendent pas du choix de χ' dans $\widetilde{\chi}$; ces quantités seront notées respectivement g_{χ}, U_{χ}, K_{χ} et G_{χ}. Enfin les relations $\widetilde{\phi} \subset \widetilde{\chi}$, $\chi' \in \widetilde{\phi}$ et $\chi' \in \widetilde{\chi}$ seront traduites respectivement par les notations $\phi | \chi$, $\chi' | \phi$ et $\chi' | \chi$ et nous dirons que χ est au-dessus de ϕ, ϕ au-dessus de χ' et χ au-dessus de χ'.

γ) *Caractères pairs et impairs.* Soit $\chi' \in \mathfrak{X}'_0$. Notons pour simplifier $-1 \in \mathfrak{G}_0$ la conjugaison complexe. Si $\chi'(-1) = 1$ (resp. $\chi'(-1) = -1$), nous dirons que χ' est pair (resp. impair) ; cette propriété se conserve par $\Gamma_{\mathbf{Q}}$ et $\Gamma_{\mathbf{Q}_l}$-conjugaison, d'où les notions de caractères rationnels et l-adiques pairs ou impairs. Nous noterons par un indice supérieur + ou − les sous-ensembles de caractères pairs et impairs que l'on peut définir à partir d'une partie quelconque de $\mathfrak{X}'_0$, Φ_0 et $\mathfrak{X}_0$.

δ) *Conducteur d'un caractère.* Soit $\chi' \in \mathfrak{X}'_0$. Le conducteur du corps K_χ est appelé indifféremment le conducteur de χ', de ϕ ou de χ et est noté f_χ.

b) *Caractères d'un sous-corps.*

α) *Définitions.* Soit $K \subset \mathbf{Q}_0^a$ (de degré fini ou non sur $\mathbf{Q}$) ; alors on vérifie facilement que :

$$\mathfrak{X}'_K = \{\chi' \in \mathfrak{X}'_0 \,,\, K_\chi \subset K\}$$

s'identifie canoniquement, par passage au quotient, à l'ensemble des caractères de Gal(K/**Q**). La relation $\chi' \in \mathfrak{X}'_K$ entraîne $\widetilde{\chi} \subset \mathfrak{X}'_K$, on peut donc poser de même :

$$\mathfrak{X}_K = \{\chi \in \mathfrak{X}_0 \,,\, K_\chi \subset K\} \quad \text{et} \quad \Phi_K = \{\phi \in \Phi_0 \,,\, K_\chi \subset K\} \;.$$

Ces trois ensembles sont appelés les ensembles de caractères (complexes, rationnels et l-adiques) de K ; $\mathfrak{X}_K$ et Φ_K sont les ensembles de caractères rationnels et l-adiques au-dessus des éléments de $\mathfrak{X}'_K$. Par exemple, si $K = \mathbf{Q}^{(f)}$, $f \in \mathbf{N}^*$, $\mathfrak{X}'_{\mathbf{Q}^{(f)}}$ s'identifie canoniquement au groupe des caractères de $(\mathbf{Z}/f\mathbf{Z})^*$, ce qui permet de donner un sens à la notation $\chi'(\sigma_a)$, σ_a étant (pour $(a\,,f) = 1$) l'élément de $\mathrm{Gal}(\mathbf{Q}^{(f)}/\mathbf{Q})$ correspondant à la classe de a modulo f.

DEFINITION I.1. – *Dans le cas particulier où* $K = \mathbf{Q}^a$, *on posera pour simplifier* $\mathfrak{X}'_{\mathbf{Q}^a} = \mathfrak{X}'$, $\Phi_{\mathbf{Q}^a} = \Phi$ et $\mathfrak{X}_{\mathbf{Q}^a} = \mathfrak{X}$.

Remarque I.1. – L'application $K \to \mathfrak{X}'_K$ est une application croissante. Pour K, $L \subset \mathbf{Q}_0^a$, $\mathfrak{X}'_{KL}$ est le groupe engendré par $\mathfrak{X}'_K$ et $\mathfrak{X}'_L$; si K/**Q** et L/**Q** sont linéairement disjointes alors, on a $\mathfrak{X}'_{KL} = \mathfrak{X}'_K \oplus \mathfrak{X}'_L$; enfin $\mathfrak{X}'_{K\cap L} = \mathfrak{X}'_K \cap \mathfrak{X}'_L$.

β) *Le caractère* θ. Soit $\zeta_l \in \Omega_l$ une racine primitive l^e de l'unité. Pour tout $\sigma \in \mathfrak{G}_0$, $\zeta_l^\sigma = \zeta_l^{a_\sigma}$, $a_\sigma \in \mathbf{Z}$ défini modulo l, indépendant du choix de ζ_l ; il existe alors une racine $(l-1)^e$ de l'unité unique appartenant à $\mathbf{Q}_l$ congrue à a_σ modulo l ; on la note $\theta(\sigma)$. On définit ainsi un élément de $\mathfrak{X}'$ d'ordre $l-1$ dont le noyau laisse fixe le corps $\mathbf{Q}^{(l)}$ (donc $\theta \in \mathfrak{X}'_{\mathbf{Q}^{(l)}}$). Comme l est totalement décomposé dans $\mathbf{Q}^{(l-1)}$, il en résulte que θ est aussi un élément de Φ ; l'hypothèse $l \neq 2$ entraîne $\theta \in \Phi^-$.

γ) *Caractères unités.* L'élément unité de $\mathfrak{X}'_0$ est commun à tous les ensembles de la forme $\mathfrak{X}'_K$, $\mathfrak{X}_K$ et Φ_K ; on le notera 1 dans tous les cas (on a $K_1 = \mathbf{Q}$).

c) *Propriétés des caractères rationnels.* On vérifie facilement le résultat suivant :

PROPOSITION I.1. – *Soit* L *un sous-corps quelconque de* $\mathbf{Q}_0^a$. *L'application qui à* $\chi \in \mathfrak{X}_0$ *associe le corps* K_χ *donne par restriction une application bijective et canonique de* $\mathfrak{X}_L$ *sur l'ensemble des sous-corps de* L *cycliques sur* **Q**. *Dans cette bijection,* $\mathfrak{X}_L^+$ *(resp.* $\mathfrak{X}_L^-$*) correspond à l'ensemble des extensions cycliques réelles (resp. imaginaires) de* **Q** *contenues dans* L.

PROPOSITION I.2. – *Soit* L *un sous-corps de* $\mathbf{Q}_0^a$. *Soient* $(A_\chi)_{\chi \in \mathfrak{X}_L}$ *et* $(A'_\chi)_{\chi \in \mathfrak{X}_L}$ *deux familles de nombres indexées par* $\mathfrak{X}_L$. *Si pour tout corps* $K \subset L$, *on a les relations* $\prod_{\chi \in \mathfrak{X}_K} A_\chi = \prod_{\chi \in \mathfrak{X}_K} A'_\chi$, *alors* $A_\chi = A'_\chi$ *pour tout* $\chi \in \mathfrak{X}_L$.

Cette proposition est un cas particulier d'un résultat de [19] (I, § 1,1).

d) *Conducteur des caractères d'ordre premier à l.* On sera amené dans la suite à supposer $\chi \in \mathfrak{X}$ (i.e. $(g_\chi, l) = 1$) ; on utilisera alors le résultat suivant :

PROPOSITION I.3. – *Soit* $K \subset \mathbf{Q}^a$, *de conducteur* f. *Alors on a* $f \not\equiv 0$ *modulo* l^2. *En particulier, si* $\chi \in \mathfrak{X}$, *alors* $f_\chi \not\equiv 0$ *modulo* l^2.

COROLLAIRE I.1. – *L'indice de ramification de* l *dans* K/**Q** *est un diviseur de* $l - 1$.

DEFINITION I.2. – *Pour tout* $\chi \in \mathfrak{X}$, *nous poserons* $f_\chi = l f'_\chi$ *(resp.* $f_\chi = f'_\chi$*) si* l *divise* f_χ *(resp.* l *ne divise pas* f_χ*).*

2. Premiers résultats sur la structure du l-groupe des classes.

a) *Structures de* $\mathbf{Z}_l^{(g_\chi)}$*-modules.* Soit $\chi \in \mathfrak{X}$ et soit $\mathbf{Z}_l^{(g_\chi)}$ l'anneau des entiers du complété $\mathbf{Q}_l^{(g_\chi)} \subset \hat{\Omega}_l$ (déterminé de façon unique comme il a été dit au début du § 1).

Pour tout $\phi \mid \chi$, considérons $\mathbf{Z}_l[\mathrm{G}_\chi]\, e_\phi$, où e_ϕ est l'idempotent $\dfrac{1}{g_\chi} \displaystyle\sum_{\sigma \in \mathrm{G}_\chi} \phi(\sigma^{-1})\, \sigma$ de l'algèbre semi-simple $\mathbf{Q}_l[\mathrm{G}_\chi]$. Soit σ_χ un générateur de G_χ.

Proposition I.4. – *Il existe un isomorphisme i_ϕ (non canonique) de $\mathbf{Z}_l[\mathrm{G}_\chi]\, e_\phi$ sur $\mathbf{Z}_l^{(g_\chi)} \subset \hat{\Omega}_l$ réalisé de la façon suivante : Soit γ_ϕ une racine du polynôme cyclotomique local $\mathrm{P}_\phi = \displaystyle\prod_{\chi' \mid \phi} (\mathrm{X} - \chi'(\sigma_\chi))$ de $\mathbf{Z}_l[\mathrm{X}]$; alors à $\sigma_\chi e_\phi$, on associe $\gamma_\phi \in \mathbf{Z}_l^{(g_\chi)}$* (cf. [27], § I, 2).

Remarque I.2. – Nous faisons une fois pour toutes le choix d'un système $(\sigma_\chi)_{\chi \in \mathfrak{X}}$ et d'un système $(\gamma_\phi)_{\phi \in \Phi}$. Ceci détermine les isomorphismes i_ϕ.

Definition I.3. – *Soit* M *un* $\mathbf{Z}_l[\mathrm{G}_\chi]$*-module ; on aura la décomposition :* $\mathrm{M} = \displaystyle\bigoplus_{\phi \in \Phi_{\mathrm{K}_\chi}} \mathrm{M}^{e_\phi}$. *Les sous-modules* $\mathrm{M}_\phi = \mathrm{M}^{e_\phi}$ *sont donc, de façon canonique, des* $\mathbf{Z}_l[\mathrm{G}_\chi]\, e_\phi$*-modules, donc des* $\mathbf{Z}_l^{(g_\chi)}$*-modules, d'après la prop. I.4.*

Par définition, la loi de $\mathbf{Z}_l^{(g_\chi)}$-module définie sur M_ϕ sera celle définie par l'isomorphisme i_ϕ de la prop. I.4.

Remarque I.3. – On démontre de la même manière qu'un $\mathbf{Z}[\mathrm{G}_\chi]\, e_\chi$-module M $\left(e_\chi = \dfrac{1}{g_\chi} \displaystyle\sum_{\sigma \in \mathrm{G}_\chi} \chi(\sigma^{-1})\, \sigma\right.$ étant un idempotent de l'algèbre semi-simple $\left.\mathbf{Q}[\mathrm{G}_\chi]\right)$ est un $\mathbf{Z}^{(g_\chi)}$-module, en utilisant un isomorphisme $i_\chi : \mathbf{Z}[\mathrm{G}_\chi]\, e_\chi \to \mathbf{Z}^{(g_\chi)}$ défini par exemple par $i_\chi(\sigma_\chi e_\chi) = \gamma_\chi$ où γ_χ est une racine du polynôme cyclotomique $\mathrm{P}_\chi = \displaystyle\prod_{\chi' \mid \chi} (\mathrm{X} - \chi'(\sigma_\chi))$ (cf. [27], § I, 2).

b) *Définition des groupes $\mathcal{H}_\phi$ et $\mathcal{H}_\chi$*. Soit $L \subset \mathbf{Q}^a$ de degré fini sur $\mathbf{Q}$ et soit $G = \mathrm{Gal}(L/\mathbf{Q})$; les algèbres $\mathbf{Z}_{(l)}[G]$ et $\mathbf{Z}_l[G]$ sont semi-simples et admettent chacune une famille d'idempotents irréductibles orthogonaux que l'on peut indicer respectivement par $\mathfrak{X}_L$ et Φ_L, à savoir : $(e_\chi^L)_{\chi \in \mathfrak{X}_L}$ et $(e_\phi^L)_{\phi \in \Phi_L}$; on a $e_\chi^L = \dfrac{1}{g} \sum\limits_{\sigma \in G} \chi(\sigma^{-1})\, \sigma$ et $e_\phi^L = \dfrac{1}{g} \sum\limits_{\sigma \in G} \phi(\sigma^{-1})\, \sigma$, où $g = |G|$; il en résulte, compte tenu des inclusions $\mathbf{Z}_{(l)} \subset \mathbf{Z}_l \subset \hat{\Omega}_l$, que $e_\chi^L = \sum\limits_{\phi | \chi} e_\phi^L$ et $e_\phi^L = \sum\limits_{\chi' | \phi} e_{\chi'}^L$ avec $e_{\chi'}^L = \dfrac{1}{g_\chi} \sum\limits_{\sigma \in G} \chi'(\sigma^{-1})\, \sigma$ qui peut être considéré comme idempotent de $\Omega_l[G]$.

Soit $\mathcal{H}_L$ le l-groupe des classes de L, $\mathcal{H}_L$ est, de façon canonique, un $\mathbf{Z}_{(l)}[G]$-module et un $\mathbf{Z}_l[G]$-module ; on posera $\mathcal{H}_\chi = \mathcal{H}_L^{e_\chi^L}$ et $\mathcal{H}_\phi = \mathcal{H}_L^{e_\phi^L}$, pour tout $\chi \in \mathfrak{X}_L$ et $\phi \in \Phi_L$. Ces notations (ne faisant pas référence au corps L) sont justifiées par le résultat suivant :

Proposition I.5. – *Les groupes $\mathcal{H}_\chi$ et $\mathcal{H}_\phi$ ainsi définis ne dépendent, à isomorphisme canonique près, que des caractères $\chi \in \mathfrak{X}$ et $\phi \in \Phi$ respectivement et non de l'extension* L *considérée* (cf. [19] et [27]).

Corollaire I.2. – *Pour tout corps* $L \subset \mathbf{Q}^a$, *on a :*

$$\mathcal{H}_L \simeq \bigoplus_{\phi \in \Phi_L} \mathcal{H}_\phi = \bigoplus_{\chi \in \mathfrak{X}_L} \mathcal{H}_\chi .$$

Remarque I.4. – On peut convenir que $\mathcal{H}_\phi$ et $\mathcal{H}_\chi$ sont les sous-groupes de $\mathcal{H}_{K_\chi}$ définis par $\mathcal{H}_{K_\chi}^{e_\chi}$ et $\mathcal{H}_{K_\chi}^{e_\phi}$ où $e_\chi = \dfrac{1}{g_\chi} \sum\limits_{\sigma \in G_\chi} \chi(\sigma^{-1})\, \sigma$ et $e_\phi = \dfrac{1}{g_\chi} \sum\limits_{\sigma \in G_\chi} \phi(\sigma^{-1})\, \sigma$; $\mathcal{H}_\phi$ et $\mathcal{H}_\chi$ sont, d'après la Déf. I.3 et la Rem. I.3, respectivement des $\mathbf{Z}_l^{(g_\chi)}$ et $\mathbf{Z}^{(g_\chi)}$-modules. On vérifie facilement que la connaissance de la structure de $\mathcal{H}_L$ (en tant que $\mathrm{Gal}(L/\mathbf{Q})$-module) est équivalente à celle de la structure des $\mathcal{H}_\phi$, $\phi \in \Phi_L$ (en tant que $\mathbf{Z}_l^{(g_\chi)}$-modules).

c) *Définition des groupes* $\mathcal{E}_\chi$ *et* $\mathcal{E}_\phi$. On suppose dans ce sous-paragraphe que $\chi \in \mathfrak{X}^+$. Pour tout corps L, désignons par E_L le groupe des unités de L. On définit, en suivant Leopoldt, les groupes $E_\chi = \{\epsilon \in E_{K_\chi},\ N_{K_\chi/k}\,\epsilon = \pm 1,$ pour tout sous-corps strict k de $K_\chi\}$ (unités dites χ-relatives) ; pour $\chi = 1$, on a $E_1 = \{\pm 1\}$.

On considère $|E_\chi|$ (groupe des valeurs absolues) comme G_χ-module en posant $|\epsilon|^\sigma = |\epsilon^\sigma|$. On montre [19], § 5, 2 que pour $\chi \neq 1$, $|E_\chi|$ est un $\mathbf{Z}$-module libre de dimension $\varphi(g_\chi)$, que pour tout corps réel L, $\bigoplus_{\chi \in \mathfrak{X}_L} |E_\chi|$ est d'indice fini dans le groupe E_L et enfin que pour tout $\epsilon \in E_\chi$, $|\epsilon|$ est invariant par e_χ [19], § 5, 1. On peut donc considérer $|E_\chi|$ comme un $\mathbf{Z}[G_\chi]\,e_\chi$-module, donc (Rem. I.3) comme un $\mathbf{Z}^{(g_\chi)}$-module (il sera donc de rang 1 sur $\mathbf{Z}^{(g_\chi)}$).

DEFINITION I.4. – *On pose* $\mathcal{E}_\chi = \mathbf{Z}_l \otimes_{\mathbf{Z}} |E_\chi|$; $\mathcal{E}_\chi$ *est un* $\mathbf{Z}_l$*-module libre de dimension* $\varphi(g_\chi)$ *et c'est, canoniquement, un* $\mathbf{Z}_l[G_\chi]\,e_\chi$*-module, ce qui fait qu'on a la décomposition* $\mathcal{E}_\chi = \bigoplus_{\phi | \chi} \mathcal{E}_\chi^{e_\phi}$ *; on pose* $\mathcal{E}_\chi^{e_\phi} = \mathcal{E}_\phi$. *Les sous-modules* $\mathcal{E}_\phi$ *sont des* $\mathbf{Z}_l^{(g_\chi)}$*-modules (Déf. I.3). Le théorème sur les unités de Dirichlet conduit au résultat suivant* [27] :

PROPOSITION I.6. – *On a* $\mathcal{E}_\phi \simeq \mathbf{Z}_l^{(g_\chi)}$, *pour tout* $\phi \in \Phi^+$, $\phi \neq 1$.

Remarque I.5. – Si F_χ est un sous-G_χ-module de E_χ, $\mathbf{Z}_l \otimes_{\mathbf{Z}} |F_\chi|$ s'identifie canoniquement à un sous-module de $\mathcal{E}_\chi$, que l'on notera $\mathcal{F}_\chi$; on posera $\mathcal{F}_\phi = \mathcal{F}_\chi^{e_\phi}$ pour tout $\phi | \chi$. Alors dans l'isomorphisme $\mathcal{E}_\phi \simeq \mathbf{Z}_l^{(g_\chi)}$, l'image de $\mathcal{F}_\phi$ est une puissance de l'idéal maximal de $\mathbf{Z}_l^{(g_\chi)}$ ou (0).

d) *Formule analytique du nombre de classes.* Soit $L \subset \mathbf{Q}^a$ et soit h_L le nombre de classes (au sens ordinaire) de L. D'après Hasse [13] et Leopoldt [19], on a, lorsque L est imaginaire : $h_L = h_L^- h_L^+$, avec :

$$h_L^- = W_L Q_L^- \prod_{\chi \in \mathfrak{X}_L^-} \left(\prod_{\chi' | \chi} \frac{-1}{2 f_\chi} \sum_{a=1}^{f_\chi}{}^{*} \chi'^{-1}(\sigma_a)\, a \right),$$

où le symbole $\sum_{a=1}^{f_\chi}{}^{*}$ désigne la sommation restreinte aux a premiers à

f_χ, où W_L est le nombre de racines de l'unité contenues dans L, $Q_L^- = 1$ ou 2 est l'indice du groupe des unités du sous-corps réel maximal L_0 de L dans le groupe des unités de L, f_χ est le conducteur de χ. Le nombre h_L^+ est le nombre de classes du sous-corps réel maximal L_0 (on a donc $h_L^+ = h_{L_0}$) ; h_L^+ se met sous la forme suivante :

$$Q_L^+ h_L^+ = \prod_{\chi \in \mathfrak{X}_L^+} (E_\chi : F_\chi) ,$$

où Q_L^+ est, à une puissance de 2 près, un entier rationnel dont l'ensemble des diviseurs premiers est inclus dans l'ensemble des diviseurs premiers de $[L : \mathbf{Q}]$ (donc, si $L \subset \mathbf{Q}^a$, Q_L^+ est premier à l).

Rappelons la définition des groupes F_χ [19], § 8 : Soit $\chi \in \mathfrak{X}^+$, soit f_χ le conducteur de χ, soit V_χ le noyau commun des $\chi' \in \widetilde{\chi}$ considérés comme caractères de $\mathrm{gal}(\mathbf{Q}^{(f_\chi)}/\mathbf{Q})$ et soit :

$$D_\chi = \frac{1}{|V_\chi|} \Big(\sum_{\tau \in V_\chi} \tau \Big) \prod_{p \mid g_\chi} (1 - \tau_\chi^{g_\chi / p}) \ (p \text{ premier}) ,$$

où τ_χ est un élément de $\mathrm{Gal}(\mathbf{Q}^{(f_\chi)}/\mathbf{Q})$ dont l'image dans G_χ est génératrice (égale à σ_χ par exemple). Soit $\Theta'_\chi = \prod_{a \in \mathfrak{A}_\chi} (\xi_\chi'^{a} - \xi_\chi'^{-a})$, $\xi'_\chi = \exp(i\pi/f_\chi)$, où $\mathfrak{A}_\chi$ désigne un système de représentants dans $\mathbf{Z}$ de $\mathrm{Gal}(\mathbf{Q}_0^{(f_\chi)}/K_\chi)$; alors $\eta_\chi = \Theta_\chi'^{D_\chi}$ est une unité de E_χ engendrant un sous-groupe F_χ d'indice fini dans E_χ ; F_χ qui ne dépend que de χ est appelé le groupe des unités cyclotomiques χ-relatives.

e) *Définition de certains invariants.* Soit $\chi \in \mathfrak{X}$, et soit $\mathfrak{L}_\chi$ l'idéal premier au-dessus de l dans $\mathbf{Q}^{(g_\chi)}$ qui est associé au plongement $\overline{\mathbf{Q}} \to \hat{\Omega}_l$ (autrement dit, le complété de $\mathbf{Q}^{(g_\chi)}$ contenu dans $\hat{\Omega}_l$ (et que nous avons noté $\mathbf{Q}_l^{(g_\chi)}$) est le complété en $\mathfrak{L}_\chi$ de $\mathbf{Q}^{(g_\chi)}$). Soit enfin $\mathfrak{L}_\chi$ la fermeture de $\mathfrak{L}_\chi$ dans $\mathbf{Z}_l^{(g_\chi)}$ (puisque l ne divise pas g_χ, on a $\mathfrak{L}_\chi = l\,\mathbf{Z}_l^{(g_\chi)}$).

α) *Invariants "classes".* Soit $\phi \mid \chi$; on rappelle (Déf. I.3 et Prop. I.4) que $\mathcal{H}_\phi$ est un $\mathbf{Z}_l^{(g_\chi)}$-module ; on peut donc écrire

$$\mathcal{H}_\phi \simeq \prod_{i \geqslant 1} \mathbf{Z}_l^{(g_\chi)}/\mathfrak{L}_\chi^{n_{\phi,i}(\mathcal{H})} ;$$

les $n_{\phi,i}(\mathcal{H})$, étant supposés décroissants et nuls à partir d'un certain rang, sont alors uniques.

DEFINITION I.5. – *On pose*

$$m_\phi(\mathcal{H}) = \sum_{i \geqslant 1} n_{\phi,i}(\mathcal{H}),\ m_\chi(\mathcal{H}) = \sum_{\phi \mid \chi} m_\phi(\mathcal{H})\ ;$$

$n_{\phi,i}(\mathcal{H})$, $m_\phi(\mathcal{H})$ *et* $m_\chi(\mathcal{H})$ *sont dits les invariants "classes" ; ils ne dépendent pas du choix des isomorphismes* i_ϕ.

Avec cette définition, on remarque que $|\mathcal{H}_\phi| = l^{\phi(1)m_\phi(\mathcal{H})}$ et que $|\mathcal{H}_\chi| = l^{\phi(1)m_\chi(\mathcal{H})}$ (en effet, le nombre d'éléments de l'anneau $\mathbf{Z}_l^{(g_\chi)}\,\mathcal{P}_\chi^{\,n}$ est égal à $l^{n\phi(1)}$).

β) *Invariants "analytiques".* Soit $\phi \mid \chi$. Nous distinguons les cas $\phi \in \Phi^+$ et $\phi \in \Phi^-$.

i) $\phi \in \Phi^+$. On a donc K_χ réel, $\mathrm{K}_\chi \subset \mathbf{Q}^a$; on considère le groupe $\mathrm{E}_\chi/\mathrm{F}_\chi$ dont le l-Sylow s'identifie canoniquement à $\mathcal{E}_\chi/\mathcal{F}_\chi$ qui est somme directe des $\mathbf{Z}_l^{(g_\chi)}$-modules $\mathcal{E}_\phi/\mathcal{F}_\phi$. D'après la Prop. I.6 et la Rem. I.5, les modules $\mathcal{E}_\phi$ et $\mathcal{F}_\phi$ sont monogènes (donc libres de dimension 1 pour $\phi \neq 1$) sur $\mathbf{Z}_l^{(g_\chi)}$:

DEFINITION I.6. – *On convient d'identifier* $\mathcal{E}_\phi$ *à* $\mathbf{Z}_l^{(g_\chi)}$ *; dans cette identification, on aura* $\mathcal{F}_\phi \simeq \mathcal{P}_\chi^{\,m_\phi(h)}$, $m_\phi(h) \geqslant 0$. *On pose*

$$m_\chi(h) = \sum_{\phi \mid \chi} m_\phi(h)\,.$$

On remarque que $|\mathcal{E}_\phi/\mathcal{F}_\phi| = l^{\phi(1)m_\phi(h)}$ et que $|\mathcal{E}_\chi/\mathcal{F}_\chi| = l^{\phi(1)m_\chi(h)}$.

ii) $\phi \in \Phi^-$. On a donc K_χ imaginaire $\mathrm{K}_\chi \subset \mathbf{Q}^a$. Si $\chi' \neq \theta$, on pose $\mathrm{B}_{\chi'} = \dfrac{1}{f_\chi}\sum_{a=1}^{f_\chi}{}^{*}\,\chi'^{-1}(\sigma_a)\,a$ et pour $\chi' = \theta$, on pose $\mathrm{B}_\theta = \sum_{a=1}^{l-1} \theta^{-1}(\sigma_a)a$; on définit ensuite $\mathrm{B}_\phi = \prod_{\chi' \mid \phi} \mathrm{B}_{\chi'}$ *et* $\mathrm{B}_\chi = \prod_{\phi \mid \chi} \mathrm{B}_\phi = \prod_{\chi' \mid \chi} \mathrm{B}_{\chi'}$. Les nombres B_ϕ sont des éléments de $\mathbf{Q}_l$ et les nombres B_χ des rationnels (B_ϕ est une norme dans l'extension $\mathbf{Q}_l^{(g_\chi)}/\mathbf{Q}_l$ et B_χ est une norme dans l'extension $\mathbf{Q}^{(g_\chi)}/\mathbf{Q}$:

DEFINITION I.7. – *On pose* $\mathrm{B}_{\chi'}\mathbf{Z}_l^{(g_\chi)} = \mathcal{P}_\chi^{\,m_\phi(h)}$ *(l'exposant ne dépend pas du choix de* $\chi' \mid \phi$*) ; on a donc* $\mathrm{B}_\phi\,\mathbf{Z}_l = (l)^{\phi(1)m_\phi(h)}$ *et* B_χ *a pour l-participation* $l^{\phi(1)m_\chi(h)}$ *avec* $m_\chi(h) = \sum_{\phi \mid \chi} m_\phi(h)$.

PROPOSITION I.7. – *Pour tout* $\chi' \in \mathfrak{X}'^-$, *le nombre* $B_{\chi'}$ *est l-entier* (i.e. $m_\phi(h) \geqslant 0$).

Démonstration. – Il suffit d'examiner le cas $f_\chi \equiv 0 \bmod l$ et $\chi' \neq \theta$ et de montrer que $\sum_{a=1}^{f_\chi}{}^* \chi'^{-1}(\sigma_a)\, a \equiv 0 \bmod l$. Comme l divise f_χ, on a, pour tout $a (a, f_\chi) = 1$, $a \equiv \theta(\sigma_a) \bmod l$, d'où,

$$\sum_{a=1}^{f_\chi}{}^* \chi'^{-1}(\sigma_a)\, a \equiv \sum_{a=1}^{f_\chi}{}^* \chi'^{-1}\, \theta(\sigma_a) \ ;$$

or le caractère $\chi'^{-1}\theta$ n'est pas trivial sur $\mathrm{Gal}(\mathbf{Q}^{(f_\chi)}/\mathbf{Q})$ puisque $\chi' \neq \theta$. D'où la proposition.

Le résultat suivant constitue la première relation entre invariants "classes" et invariants "analytiques" :

THEOREME I.1. – *Pour tout* $\chi \in \mathfrak{X}$, *on a* $|\mathcal{H}_\chi| = l^{\phi(1) m_\chi(h)}$. *Il en résulte l'égalité* $m_\chi(\mathcal{H}) = m_\chi(h)$, *pour tout* $\chi \in \mathfrak{X}$.

Démonstration. – Posons $A_\chi = l^{\phi(1) m_\chi(h)}$ et $A'_\chi = l^{\phi(1) m_\chi(\mathcal{H})}$; on a $|\mathcal{H}_\chi| = A'_\chi$, d'où, d'après le Corol. I.2 $|\mathcal{H}_L| = \prod_{\chi \in \mathfrak{X}_L} A'_\chi$; il suffit alors de montrer que pour tout corps $L \subset \mathbf{Q}^a$, on a $|\mathcal{H}_L| = \prod_{\chi \in \mathfrak{X}_L} A_\chi$, la Prop. I.2 entraînant le résultat. Notons $(\ )_l$ la l-participation d'un rationnel l-adique ; celle de h_L est donc, en vertu du § 2, *d* la suivante :

i) L est réel ; alors $(h_L)_l = \prod_{\chi \in \mathfrak{X}_L^+} (E_\chi : F_\chi)_l = \prod_{\chi \in \mathfrak{X}_L} A_\chi$ (car dans notre cas, Q_L^+ est premier à l).

ii) L est imaginaire mais ne contient pas $\mathbf{Q}^{(l)}$. Dans ce cas, $(W_L)_l = 1$ et $\mathfrak{X}'^-_L$ ne contient pas θ, d'où

$$(h_L)_l = h_L^- h_L^+ = \prod_{\chi \in \mathfrak{X}_L^-} A_\chi \prod_{\chi \in \mathfrak{X}_L^+} A_\chi = \prod_{\chi \in \mathfrak{X}_L} A_\chi \,.$$

iii) L est imaginaire et contient $\mathbf{Q}^{(l)}$. On a alors $(W_L)_l = l$ (l'hypothèse $L \subset \mathbf{Q}^a$ implique que L ne contient pas $\mathbf{Q}^{(l^2)}$) et $\theta \in \mathfrak{X}'^-_L$; on constate alors que $B_\chi = (W_L)_l \left(\prod_{\theta' | \chi} \frac{1}{l} \sum_{a=1}^{l-1} \theta'^{-1}(a)\, a \right)_l$ (où $\theta' | \chi$), d'où encore la relation $(h_L)_l = \prod_{\chi \in \mathfrak{X}_L} A_\chi$, d'où le théorème.

Remarque I.6. – Les invariants $m_\phi(h)$ et $m_\chi(h)$ sont dits des invariants "analytiques" car ils sont définis à partir des résultats donnés par les formules analytiques des nombres de classes "h" (cas réel et cas imaginaire). Les invariants $n_{\phi,i}(\mathcal{H})$, $m_\phi(\mathcal{H})$ et $m_\chi(\mathcal{H})$ sont par définition des invariants définis directement à partir de la structure des groupes de classes "$\mathcal{H}$". Il est intéressant de chercher à comparer ces deux sortes d'invariants dans le but d'avoir des informations sur $n_{\phi,i}(\mathcal{H})$ et $m_\phi(\mathcal{H})$ à partir des $m_\phi(h)$ qui, contrairement aux précédents, peuvent se calculer ($m_\phi(h)$, dans le cas pair se calcule par "dévissage" des unités cyclotomiques [10], [11] et $m_\phi(h)$ dans le cas impair par le simple calcul de nombres de Bernoulli).

f) *Conséquences du théorème de Stickelberger.* On rappelle le résultat bien connu suivant [7], [18], [2] ; voir aussi [24] :

PROPOSITION I.8. – *Soit* K/**Q** *une extension abélienne imaginaire de conducteur f et de groupe de Galois* G *d'ordre g. Soit*

$$S_K = \frac{1}{f} \sum_{a=1}^{f}{}^{*} a\,\overline{\sigma}_a^{-1} \in \mathbf{Q}[G]\,,$$

où $\overline{\sigma}_a$ est l'image de $\sigma_a \in \mathrm{Gal}(\mathbf{Q}^{(f)}/\mathbf{Q})$ dans G ; *alors tout élément de* $\mathbf{Z}[G] \cap S_K\mathbf{Z}[G]$ *annule le groupe des classes de* K *et tout élément de* $\mathbf{Z}_l[G] \cap S_K\mathbf{Z}_l[G]$ *annule le l-groupe des classes de* K.

Nous allons en déduire le résultat suivant :

THEOREME I.2. – *Soit $\phi \in \Phi^-$ et soit $\chi' \mid \phi$. Alors $\mathcal{H}_\phi$ (considéré comme $\mathbf{Z}_l^{(g_\chi)}$-module) est annulé par $B_{\chi'} \in \mathbf{Z}_l^{(g_\chi)}$. Il en résulte les inégalités : $n_{\phi,i}(\mathcal{H}) \leqslant m_\phi(h)$, pour tout $i \geqslant 1$.*

Démonstration. – Appliquons la Prop. I.8 au cas d'un corps K_χ, $\chi \in \mathfrak{X}^-$. Calculons

$$e_{\chi'} S_{K_\chi} = \frac{1}{g_\chi} \sum_{\sigma \in G_\chi} \chi'(\sigma^{-1})\,\sigma\, \frac{1}{f_\chi} \sum_{a=1}^{f_\chi}{}^{*} a\,\overline{\sigma}_a^{-1} =$$

$$= \frac{1}{f_\chi g_\chi} \sum_{a=1}^{f_\chi}{}^{*} \sum_{\sigma \in G_\chi} a\chi'(\sigma^{-1})\,\overline{\sigma}_a^{-1}\,\sigma\,,$$

ce qui devient, en posant : $\overline{\sigma}_a^{-1}\,\sigma = \tau$:

$$\frac{1}{f_\chi g_\chi} \sum_{a=1}^{f_\chi}{}^{*} \sum_{\tau \in G_\chi} a\,\chi'(\overline{\sigma}_a^{-1}\tau^{-1})\tau = B_{\chi'} e_{\chi'} .$$

On aura en particulier $e_\phi S_{K_\chi} = \sum_{\chi' | \phi} e_{\chi'} B_{\chi'}$. Distinguons les cas $\phi \neq \theta$ et $\phi = \theta$:

i) Supposons $\phi \neq \theta$. D'après la Prop. I.7, $e_\phi S_{K_\chi}$ est un élément de $\mathbf{Z}_l[G_\chi]$; d'après la Prop. I.8, $e_\phi S_{K_\chi}$ annule $\mathcal{H}_\phi$. Reste à déterminer l'image de $e_\phi S_{K_\chi}$ par i_ϕ pour trouver un entier de $\mathbf{Z}_l^{(g_\chi)}$ qui annule $\mathcal{H}_\phi$: on a $i_\phi(e_\phi S_{K_\chi}) = i_\phi\left(\sum_{\chi'|\phi} B_{\chi'} e_{\chi'}\right) = \sum_{\chi'|\phi} B_{\chi'} i_\phi(e_{\chi'})$; or $i_\phi(e_{\chi'}) = \frac{1}{g_\chi} \sum_{k=1}^{g_\chi} \chi'(\sigma_\chi^{-k})\gamma_\phi^k$ (après avoir écrit $\sigma = \sigma_\chi^k$) et cette somme est nulle pour tout $\chi' | \phi$ sauf pour un unique $\chi' | \phi$ tel que $\gamma_\phi = \chi'(\sigma_\chi)$ (cf. choix de γ_ϕ), d'où $i_\phi(e_\phi S_{K_\chi}) = B_{\chi'}$ pour un certain $\chi' | \phi$. Comme les $B_{\chi'}$, $\chi' | \phi$, sont conjugués dans l'extension $\mathbf{Q}_l^{(g_\chi)}/\mathbf{Q}_l$, ils sont égaux (à des unités l-adiques près). En résumé, comme on a posé $B_{\chi'}\mathbf{Z}_l^{(g_\chi)} = \hat{\mathfrak{L}}_\chi^{m_\phi(h)}$ et que $\mathcal{H}_\phi \simeq \prod_{i \geqslant 1} \mathbf{Z}_l^{(g_\chi)} / \hat{\mathfrak{L}}_\chi^{n_{\phi,i}(\mathcal{H})}$, on aura bien $n_{\phi,i}(\mathcal{H}) \leqslant m_\phi(h)$, pour tout i.

ii) Supposons $\phi = \theta$. On obtient $e_\theta S_{K_\chi} = e_\theta \frac{1}{l} \sum_{a=1}^{l-1} \theta^{-1}(\sigma_a)a$ qui n'est pas l-entier car $\sum_{a=1}^{l-1} \theta^{-1}(\sigma_a)a \equiv -1 \bmod l$; donc

$$e_\theta \sum_{a=1}^{l-1} \theta^{-1}(\sigma_a)a$$

annule $\mathcal{H}_\theta$. L'image de cet élément par i_θ est égale à

$$B_\theta = \sum_{a=1}^{l-1} \theta^{-1}(\sigma_a)a \not\equiv 0 \bmod l ,$$

d'où $\mathcal{H}_\theta = \{1\}$.

Corollaire I.3. — *Soit $\chi \in \mathfrak{X}^-$, si pour $\phi | \chi$, on a $m_\phi(h) = 0$ alors $\mathcal{H}_\phi = (1)$. En particulier, si pour tout $\phi | \chi$, $\phi \neq \phi_0 | \chi$, $m_\phi(h) = 0$, alors $m_\phi(\mathcal{H}) = m_\phi(h)$, pour tout $\phi | \chi$* [24], § V, 2.

COROLLAIRE I.4. – *Soit* $\chi \in \mathfrak{X}^-$. *Si pour tout* $\phi \mid \chi, \mathcal{H}_\phi$ *est* $\mathbf{Z}_l^{(g_\chi)}$-*monogène alors* $m_\phi(\mathcal{H}) = m_\phi(h)$ *pour tout* $\phi \mid \chi$ [24], § V, 2.

En effet, dans ce cas $n_{\phi,i}(\mathcal{H}) = 0$ pour $i \geqslant 2$. D'après le Th. I.1 on $|\mathcal{H}_\chi| = l^{\phi(1) m_\chi(h)}$, d'où l'égalité $\sum_{\phi \mid \chi} n_{\phi,1}(\mathcal{H}) = \sum_{\phi \mid \chi} m_\phi(h)$ et les inégalités $n_{\phi,1}(\mathcal{H}) \leqslant m_\phi(h)$ entraînent l'égalité.

Remarque I.7. – On vérifie que pour $\chi' \in \mathfrak{X}'^-$, $\chi' \neq \theta$, on a $B_{\chi'} = B_1(\chi'^{-1})$ (nombre de Bernoulli primitif d'indice 1 : cf. chap. II, § 2).

g) *Conséquences du "Spiegelungssatz" de Leopoldt.*

α) *Définitions préliminaires.* Soit M un $\mathbf{Z}_l[G_\chi]\, e_\phi$-module ; on peut écrire $M \cong \prod_{i=1}^{r} (\mathbf{Z}_l^{(g_\chi)} \hat{\mathfrak{L}}_\chi^{n_i}) \times (\mathbf{Z}_l^{(g_\chi)})^n$, avec $r \geqslant 0, n_1 \geqslant n_2 \geqslant \ldots$ $\ldots n_r > 0$, $n \geqslant 0$; nous noterons $\dim_\phi(M) = r + n$ (le $\mathbf{Z}$-rang de M est alors égal à $\phi(1) \dim_\phi(M)$).

On déduit de la Prop. I.6 et de la définition des unités cyclotomiques le résultat suivant :

PROPOSITION I.9. – *Soit* $\phi \in \Phi$. *Les nombres* $\dim_\phi(\mathcal{E}_\phi)$ *et* $\dim_\phi(\mathcal{F}_\phi)$ *ont les valeurs suivantes :*

i) $\phi \in \Phi^-$, $\phi \neq \theta$, $\dim_\phi(\mathcal{E}_\phi) = \dim_\phi(\mathcal{F}_\phi) = 0$,

ii) $\phi \in \Phi^+$, $\phi \neq 1$, $\dim_\phi(\mathcal{E}_\phi) = \dim_\phi(\mathcal{F}_\phi) = 1$,

iii) $\phi = 1$, $\dim_1(\mathcal{E}_1) = \dim_1(\mathcal{F}_1) = 0$.

β) *l-primarité.* Soit α un élément d'un corps K ; on dit que α est l-primaire si l'extension $KQ^{(l)}(\sqrt[l]{\alpha})/KQ^{(l)}$ est non ramifiée ou de degré 1. On sait que α est l-primaire si et seulement si il vérifie les deux conditions suivantes :

i) Dans K l'idéal engendré par α est la puissance l^e d'un idéal,

ii) α vérifie les "congruences de Kummer".

Donnons ces congruences dans le cas où $\alpha \in K_\chi$, $\chi \in \mathfrak{X}$ (on sait que dans ce cas $K_\chi Q^{(l)}/Q^{(l)}$ est non ramifiée en l (cf. Prop. I.3)) :

PROPOSITION I.10. – *Pour* $\alpha \in K_\chi$, *α premier à l, les congruences de Kummer sont : Pour tout $\mathfrak{p}$ premier divisant l dans* $K_\chi Q^{(l)}$, *il existe* $\xi_{\mathfrak{p}} \in K_\chi Q^{(l)}$ *tel que* $\alpha \equiv \xi_{\mathfrak{p}}^l \bmod \mathfrak{p}^l$, *ou encore de façon équivalente : Soit $\mathfrak{p}_0$ un idéal premier de $K_\chi Q^{(l)}$ divisant l ; alors pour tout* $s \in \mathrm{Gal}(K_\chi Q^{(l)}/Q)$, *il existe* $\xi_s \in K_\chi Q^{(l)}$, *tel que* $\alpha^s \equiv \xi_s^l \bmod \mathfrak{p}_0^l$.

COROLLAIRE I.5. – *Soit* $\alpha \in K_\chi$, *α premier à l et soit* N *le degré résiduel de l dans* $K_\chi Q^{(l)}/Q$. *Alors α vérifie les congruences de Kummer si et seulement si* $\alpha^{s(1-l^N)} \equiv 1 \bmod \mathfrak{p}_0^l$ *pour tout* $s \in G_\chi$.

En effet, on a $\alpha^{s(1-l^N)} \equiv 1 \bmod \mathfrak{p}_0$, or $\xi_s^l \equiv 1 \bmod \mathfrak{p}_0$ entraîne $\xi_s \equiv 1 \bmod \mathfrak{p}_0$ et comme $(1 + \mathfrak{p}_0)^l \subset 1 + \mathfrak{p}_0^l$, le corollaire en résulte.

γ) *Définition des groupes* $\mathcal{L}$. Soit $\chi \in \mathfrak{X}$. Soient

$$\mathcal{L}_\chi = \{\overline{\alpha} \in K_\chi^*/K_\chi^{*l},\ (\alpha) = \mathfrak{U}^l \text{ dans } K_\chi\}$$

et
$$\mathcal{L}_\chi^0 = \{\overline{\alpha} \in \mathcal{L}_\chi,\ \alpha \text{ est } l\text{-primaire}\}\ ;$$

on pose $\mathcal{L}_\phi = \mathcal{L}_\chi^{e_\phi}$ et $\mathcal{L}_\phi^0 = \mathcal{L}_\chi^{0\,e_\phi}$ ($\mathcal{L}_\phi$ et $\mathcal{L}_\phi^0$ sont des $\mathbf{Z}_l^{(g_\chi)}$-modules). Le quotient $\mathcal{E}_\phi/\mathcal{E}_\phi^l$ s'identifie canoniquement à un sous-$\mathbf{Z}_l^{(g_\chi)}$-module de $\mathcal{L}_\phi$ (à savoir $(|E_\chi|/K_\chi^{*l} \cap |E_\chi|)^{e_\phi} \simeq (E_\chi/E_\chi^l)^{e_\phi}$) et est donc facteur direct dans $\mathcal{L}_\phi$; il existe un supplémentaire $\mathcal{L}_\phi(\mathcal{H})$ tel que

$$\mathcal{L}_\phi = \mathcal{E}_\phi/\mathcal{E}_\phi^l \oplus \mathcal{L}_\phi(\mathcal{H})\,.$$

DEFINITION I.8. – *Soit* $E_\chi^0 = \{\epsilon \in E_\chi,\ \epsilon$ *est l-primaire*$\}$ *et soit* $F_\chi^0 = F_\chi \cap E_\chi^0$. *On pose* $\mathcal{E}_\chi^0 = \mathbf{Z}_l \otimes |E_\chi^0|$, $\mathcal{F}_\chi^0 = \mathbf{Z}_l \otimes |F_\chi^0|$ *puis* $\mathcal{E}_\phi^0 = \mathcal{E}_\chi^{0e_\phi}$ *et* $\mathcal{F}_\phi^0 = \mathcal{F}^{0e_\phi}$.

Remarque I.8. – On rappelle que si $\phi \in \Phi^+$, $\phi \neq 1$, $\mathcal{E}_\phi \simeq \mathbf{Z}_l^{(g_\chi)}$ et $\mathcal{F}_\phi \simeq \hat{\mathcal{Q}}_\chi^{m_\phi(h)}$ (Déf. I.6) ; il en résulte que $\mathcal{E}_\phi^0 = \mathcal{E}_\phi$ ou $\mathcal{E}_\phi^l$, que $\mathcal{F}_\phi^0 = \mathcal{F}_\phi$ ou $\mathcal{F}_\phi^l$ et que si $m_\phi(h) > 0$ alors $\mathcal{F}_\phi^0 = \mathcal{F}_\phi$.

Compte tenu du fait que $\mathcal{L}_\phi^0$ est facteur direct dans $\mathcal{L}_\phi$ et que $\mathcal{E}_\phi^0/\mathcal{E}_\phi^l$ est facteur direct dans $\mathcal{L}_\phi^0$, on peut toujours supposer que $\mathcal{L}_\phi$ est décomposé de la manière suivante :

DEFINITION I.9. – *Nous poserons* $\mathcal{L}_\phi = \mathcal{E}_\phi^0/\mathcal{E}_\phi^l \oplus \mathcal{L}_\phi^0(\mathcal{H}) \oplus \mathcal{L}'_\phi(\mathcal{H})$, *avec* $\mathcal{L}_\phi^0 = \mathcal{E}_\phi^0/\mathcal{E}_\phi^l \oplus \mathcal{L}_\phi^0(\mathcal{H})$ et $\mathcal{L}_\phi(\mathcal{H}) = \mathcal{L}_\phi^0(\mathcal{H}) \oplus \mathcal{L}'_\phi(\mathcal{H})$.

δ) *Enoncés du "Spiegelungssatz".*

DEFINITION I.10. – (caractère "miroir"). *Soit* $\phi \in \Phi$, $\phi = \sum_{\chi' | \phi} \chi'$; *on définit* $\overline{\phi} = \theta \sum_{\chi' | \phi} \chi'^{-1}$. *On montre que* $\overline{\phi} \in \Phi$ *en vérifiant que* $\overline{\phi} = \sum_{\psi'} \psi'$ *où* ψ' *parcourt la* $\Gamma_{\mathbf{Q}_l}$*-classe de* $\overline{\chi}' = \theta \chi'^{-1}$. *On a aussi* $\overline{\overline{\phi}} = \phi$ *et* $\overline{\theta} = 1$.

Remarque I.9. – Nous n'utilisons pas le "miroir" d'un caractère rationnel χ car l'élément $\theta \sum_{\chi' | \chi} \chi'^{-1}$ n'est plus un élément de $\mathfrak{X}$ en général (en particulier, si ϕ_1 et ϕ_2 divisent χ, les caractères rationnels χ_1 et χ_2 respectivement au-dessus de $\overline{\phi}_1$ et $\overline{\phi}_2$ correspondent en général à des corps K_{χ_1} et K_{χ_2} distincts).

THEOREME I.3 [23]. – *Soit* $\phi \in \Phi$:

i) *On a la suite exacte* $1 \to \mathcal{E}^0_\phi / \mathcal{E}^l_\phi \to \mathcal{L}^0_\phi \to \mathcal{H}^0_\phi \to 1$, *où* $\mathcal{H}^0_\phi$ *est le sous-module de* $\mathcal{H}_\phi$ *formé des classes* $\mathrm{cl}(\mathfrak{U})$ *d'ordre* l^n, $n \geqslant 0$, *telles que* $\mathfrak{U}^{l^n}$ *est un idéal principal représentable par un élément* $\alpha \in \mathcal{L}^0_\phi(\mathcal{H})$,

ii) $\dim_\phi \mathcal{L}^0_\phi = \dim_{\overline{\phi}} \mathcal{H}_{\overline{\phi}}$,

iii) $\dim_\phi \mathcal{L}_\phi(\mathcal{H}) = \dim_\phi \mathcal{H}_\phi$,

iv) $\dim_\phi \mathcal{L}^0_\phi(\mathcal{H}) = \dim_\phi \mathcal{H}^0_\phi$.

DEFINITION I.11. – *On définit les invariants suivants :* $d_\phi = \dim_{\overline{\phi}} \mathcal{H}_{\overline{\phi}} \dim_\phi \mathcal{H}_\phi$ *(on a* $d_\phi + d_{\overline{\phi}} = 0$*),* $a_\phi = \dim_\phi(\mathcal{E}^0_\phi / \mathcal{E}^l_\phi)$ *et* $b_\phi = \dim_\phi(\mathcal{F}^0_\phi / \mathcal{F}'^l_\phi)$; *conformément à la terminologie du* § 2, e, *on peut dire que* d_ϕ *est un invariant "classe" et* a_ϕ *et* b_ϕ *des invariants "analytiques".*

COROLLAIRE I.6. – *On a :*

i) $\dim_{\overline{\phi}} \mathcal{H}_{\overline{\phi}}\text{-}\dim_\phi \mathcal{H}^0_\phi = a_\phi$ *et* $\dim_\phi \mathcal{H}_\phi\text{-}\dim_\phi \mathcal{H}^0_\phi = a_\phi - d_\phi$,

ii) $-a_{\overline{\phi}} \leqslant d_\phi \leqslant a_\phi$,

iii) $a_\phi + a_{\overline{\phi}} \leqslant 1$,

iv) *si* $\phi \in \Phi^+$, $\phi \neq 1$, *alors* $0 \leqslant a_\phi \leqslant b_\phi \leqslant 1$ *et* $0 \leqslant d_\phi \leqslant a_\phi$ *; si* $\phi \in \Phi^-$, $\phi \neq \theta$, *alors* $0 \leqslant a_{\bar\phi} \leqslant b_{\bar\phi} \leqslant 1$ *et* $-a_{\bar\phi} \leqslant d_\phi \leqslant 0$.

En effet, on a $\mathcal{L}^0_\phi = \mathcal{E}^0_\phi/\mathcal{E}^l_\phi \oplus \mathcal{L}^0_\phi(\mathcal{H})$; on utilise le Th. I.3 ii) et iv) pour démontrer i) ; ii) se déduit du fait que $\mathcal{H}^0_\phi \subset \mathcal{H}_\phi$ et du fait que $d_{\bar\phi} = -d_\phi$; enfin iii) et iv) se déduisent de la Prop. I.9.

Corollaire I.7. – i) *Soit* $\phi \in \Phi^+$, $\phi \neq 1$, $\phi \mid \chi$. *Supposons* $b_\phi = 1$. *Alors il existe* $\phi_1 \mid \chi$ *tel que* $m_{\bar\phi_1}(\mathcal{H}) \geqslant 1$.

ii) *Soit* $\phi \in \Phi^-$, $\phi \neq \theta$, $\phi \mid \chi$. *Supposons* $m_\phi(\mathcal{H}) \geqslant 1$. *Alors il existe* $\phi_2 \mid \chi_0$ *tel que* $b_{\phi_2} = 1$, *où* χ_0 *est le caractère rationnel au-dessus de* $\bar\phi$.

Démonstration. – i) On distingue deux cas :

– Si $\mathcal{F}_\phi = \mathcal{E}_\phi$, alors $\mathcal{E}_\phi = \mathcal{E}^0_\phi$ et $a_\phi = 1$; donc comme $\mathcal{E}^0_\phi/\mathcal{E}^l_\phi \subset \mathcal{L}^0_\phi$, on aura $\dim_{\bar\phi} \mathcal{H}_{\bar\phi} \geqslant 1$ (d'après le Th. I.3 ii)).

– Si $\mathcal{F}_\phi \subset \mathcal{E}^l_\phi$, alors $m_\phi(h) \geqslant 1$, donc $m_\chi(h) = m_\chi(\mathcal{H}) \geqslant 1$; il existe donc $\phi_1 \mid \chi$ tel que $\dim_{\phi_1} \mathcal{H}_{\phi_1} \geqslant 1$ mais alors comme $d_{\phi_1} \geqslant 0$, $\dim_{\bar\phi_1} \mathcal{H}_{\bar\phi_1} \geqslant 1$.

ii) On distingue deux cas :

– Si $d_\phi = 0$, alors $\dim_{\bar\phi} \mathcal{H}_{\bar\phi} = \dim_\phi \mathcal{H}_\phi \geqslant 1$; on a donc $m_{\chi_0}(\mathcal{H}) = m_{\chi_0}(h) \geqslant 1$ et il existe $\phi_2 \mid \chi_0$ tel que $m_{\phi_2}(h) \geqslant 1$, soit $\mathcal{F}_{\phi_2} \subset \mathcal{E}^l_{\phi_2}$ soit $\mathcal{F}^0_{\phi_2} = \mathcal{F}_{\phi_2}$.

– Si $d_\phi = -1$, la seule possibilité est $a_{\bar\phi} = 1$, soit $\mathcal{E}^0_{\bar\phi} = \mathcal{E}_{\bar\phi}$ et alors $\mathcal{F}^0_{\bar\phi} = \mathcal{F}_{\bar\phi}$.

3. Conclusion.

Il ne semble pas que dans le résultat ci-dessus (cor. I.7), la seule utilisation du "Spiegelungssatz" puisse apporter d'autres précisions sur la nature des caractères ϕ_1 et ϕ_2 (par exemple, a-t-on $\phi_1 = \phi$ dans le cas i) et $\phi_2 = \bar\phi$ dans le cas ii) ?) (cf. Th. IV. 1).

CHAPITRE II

NOMBRES DE BERNOULLI GENERALISES SOMMES DE GAUSS

1. Caractères de Dirichlet. (d'après [4], § 1).

Soit $\chi' \in \mathfrak{X}'_0$ et, pour m fixé, soit $\mathrm{Q}^{(m)}$ un corps cyclotomique contenant K_χ (on a alors $\chi' \in \mathfrak{X}'_{\mathrm{Q}^{(m)}}$) ; on n'impose pas que m soit le conducteur de χ'. On étend la définition de χ' en une application $\underline{\chi}'$ ainsi définie de $\mathbf{Z}$ dans Ω_l et qui dépend de m (cf. I.1, b, α, pour la définition de σ_a) :

$$\underline{\chi}'(a) = \chi'(\sigma_a) \quad \text{si} \quad (a\,, m) = 1\,,$$
$$\underline{\chi}'(a) = 0 \quad \text{si} \quad (a\,, m) \neq 1\,.$$

On a donc $\underline{\chi}'(b) = \underline{\chi}'(a)$ si $b \equiv a \bmod m$ et on a $\underline{\chi}'(a) = 0$ si et seulement si $(a\,, m) \neq 1$.

On notera $\mathrm{X}(m)$ l'ensemble des applications ainsi définies. On vérifie facilement que l'application de $\mathfrak{X}'_{\mathrm{Q}^{(m)}}$ dans $\mathrm{X}(m)$ définie par $\chi' \to \underline{\chi}'$ est bijective. Les éléments de $\mathrm{X}(m)$ sont caractérisés comme étant les applications c de $\mathbf{Z}$ dans Ω_l vérifiant les conditions :

$c(ab) = c(a)\,c(b)$ pour tout a, $b \in \mathbf{Z}$,

$c(a) = 0$ si et seulement si $(a\,, m) \neq 1$,

$c(b) = c(a)$ si $b \equiv a$ modulo m.

Les éléments de $\mathrm{X}(m)$ forment un groupe multiplicatif si l'on définit le produit cc' par $cc'(a) = c(a)\,c'(a)$; on a :

i) $cc' \in \mathrm{X}(m)$,

ii) l'élément neutre de $\mathrm{X}(m)$: c'est la fonction 1_m définie par $1_m(a) = 1$ (resp. 0) si $(a\,, m) = 1$ (resp. $(a\,, m) \neq 1$),

iii) l'inverse de $c \in \mathrm{X}(m)$: on pose $c^{-1}(a) = (c(a))^{-1}$ si $(a\,, m) = 1$, $c^{-1}(a) = 0$ sinon.

L'élément neutre de $\mathrm{X}(1)$ est le caractère trivial 1_1 défini par $1_1(a) = 1$ pour tout $a \in \mathbf{Z}$; il est distinct de 1_m, $m \neq 1$.

Nous posons $X = \bigcup_{m \geqslant 1} X(m)$; X est appelé l'ensemble des caractères de Dirichlet. Si $c \in X$, on pose $M(c) = \{m\ ,\ c \in X(m)\}$.

Soit $c \in X$ et soit $m \in M(c)$; la restriction de c à $\{a\ ,\ (a\ ,\ m) = 1\}$ permet de retrouver un caractère de $(\mathbf{Z}/m\mathbf{Z})^*$ qui est l'unique élément χ' de $\mathcal{X}'_0$ tel que $\underline{\chi}' = c$ (et qui est dit le caractère sous-jacent à c).

Nous adopterons la notation $\underline{\chi}'$ pour désigner les éléments de X: cette notation signifie que $\underline{\chi}'$ est un caractère de Dirichlet (pour un certain module supposé précisé dans le contexte) dont le caractère sous-jacent est $\chi' \in \mathcal{X}'_0$.

DEFINITION II.1. – *Si $\underline{\chi}' \in X(f_\chi)$, on dit que $\underline{\chi}'$ est un caractère de Dirichlet primitif.*

L'ensemble X est muni d'un produit qui redonne, par restriction, les lois de groupe dans les $X(m)$: si $\underline{\chi}'$, $\underline{\psi}' \in X$, on définit $\underline{\chi}'\ \underline{\psi}'$ par $\underline{\chi}'\ \underline{\psi}'(a) = \underline{\chi}'(a)\ \underline{\psi}'(a)$, pour tout $a \in \mathbf{Z}$. On vérifie facilement que si $\underline{\chi}' \in X(m_1)$, $\underline{\psi}' \in X(m_2)$, alors $\underline{\chi}'\ \underline{\psi}' \in X(m)$, où m est le p.p.c.m. de m_1 et m_2. Il en résulte en particulier que si $(m_1\ ,\ m_2) = 1$, alors $X(m_1 m_2) = X(m_1)\ X(m_2)$ (produit direct). Si $\underline{\chi}' \in X(m)$, alors pour tout $k \in \mathbf{Z}$, $\underline{\chi}'^k \in X(m)$; en particulier $\underline{\chi}'^0$ n'est autre que 1_m.

DEFINITION II.2. – *Par définition $\underline{\theta}$ sera un élément de $X(l)$ ainsi que ses puissances (en particulier $\underline{\theta}^0 = 1_l$).*

2. Nombres de Bernoulli généralisés ([20] et [4], § 2).

a) *Définitions.* Soit $\underline{\chi}' \in X(m)$; on pose :

$$\sum_{a=1}^{m} \underline{\chi}'(a) \frac{\mathrm{T}e^{a\mathrm{T}}}{e^{m\mathrm{T}} - 1} = \sum_{n \geqslant 0} \mathrm{B}_n(\underline{\chi}') \frac{\mathrm{T}^n}{n\,!}$$

(égalité de séries formelles). On montre que si $\underline{\chi}' \in X(m) \cap X(m')$, alors $\sum_{a=1}^{m'} \underline{\chi}'(a) \frac{\mathrm{T}e^{a\mathrm{T}}}{e^{m'\mathrm{T}} - 1} = \sum_{a=1}^{m} \underline{\chi}'(a) \frac{\mathrm{T}e^{a\mathrm{T}}}{e^{m\mathrm{T}} - 1}$, ce qui fait que les coefficients $\mathrm{B}_n(\underline{\chi}')$ ne dépendent que de $\underline{\chi}' \in X$ et non du choix de $m \in M(\underline{\chi}')$. Ce sont les nombres de Bernoulli généralisés. Pour $\underline{\chi}' = 1_1 \in X(1)$, on retrouve les nombres de Bernoulli ordinaires (au sens de [4] et [20]).

DEFINITION II.3. – *Nous noterons* $B_n(\chi')$ *les nombres de Bernoulli associés aux caractères primitifs* $\underline{\chi}' \in X(f_\chi)$. *Nous les appellerons les nombres de Bernoulli primitifs.*

b) *Rappels de quelques propriétés des* $B_n(\underline{\chi}')$ ([20], [4]).

i) Calcul de $B_0(\underline{\chi}')$. On a $B_0(\underline{\chi}') = 0$ pour $\underline{\chi}' \neq 1_m$ et $B_0(1_m) = \dfrac{\varphi(m)}{m}$.

ii) Parité. On a $B_{2n+1}(\underline{\chi}') = 0$ si $\underline{\chi}'$ est pair et si $\underline{\chi}' \neq 1_1$, $B_{2n+1}(1_1) = 0$, pour $n \neq 0$ et $B_1(1_1) = \dfrac{1}{2}$; $B_{2n}(\underline{\chi}') = 0$ si $\underline{\chi}'$ est impair.

iii) Calcul des $B_n(\underline{\chi}')$. On dispose de deux formules permettant le calcul de $B_n(\underline{\chi}')$:

On a d'abord $B_n(\underline{\chi}') = \dfrac{1}{m} \sum\limits_{a=1}^{m} \underline{\chi}'(a)\,(a - m + mB)^n$ où, dans le développement de $(a - m + mB)^n$, on remplace B^i, $i \geqslant 0$, par B_i (nombre de Bernoulli ordinaire). Cette formule montre que $B_n(\underline{\chi}') \in Q^{(g_\chi)}$ pour tout n.

On a ensuite une formule de récurrence :

$$\sum_{i=0}^{m} C_{n+1}^{i}\, B_i(\underline{\chi}')\, m^{n+1-i} = (n+1) \sum_{a=1}^{m} \underline{\chi}'(a)\, a^n ,$$

pour tout $\underline{\chi}' \in X$, tout $m \in M(\underline{\chi}')$ et tout $n \in \mathbf{N}$.

iv) On a $B_n(\underline{\chi}'\underline{\theta}^0) = B_n(\underline{\chi}')\,(1 - \underline{\chi}'(l)\, l^{n-1})$, pour tout $n \geqslant 0$.

v) Soit $\underline{\chi}' \in X(m)$, $\underline{\chi}' \neq 1$, où $m = lm'$, $m' \not\equiv 0 \bmod l$; enfin on suppose $\chi'\theta \neq 1$. Alors, en posant, pour tout a premier à l, $a = \underline{\theta}(a)\,(1 + \gamma_a l)$, $\gamma_a \in \mathbf{Z}_l$, on a d'après iii) :

$$B_1(\underline{\chi}') = \frac{1}{m} \sum_{a=1}^{m} \underline{\chi}'(a)\, \underline{\theta}(a)\,(1 + \gamma_a l) = \frac{1}{m} \sum_{a=1}^{m}{}^{*}\ \underline{\chi}'\underline{\theta}(a) + $$
$$+ \frac{1}{m'} \sum_{a=1}^{m}{}^{*}\ \underline{\chi}'\underline{\theta}(a)\, \gamma_a ;$$

d'où ici :

$$B_1(\underline{\chi}') = \frac{1}{m'} \sum_{a=1}^{m}{}^{*}\ \underline{\chi}'\underline{\theta}(a)\, \gamma_a \quad (\underline{\chi}' \neq 1_m\,,\, \chi' \neq \theta^{-1}) .$$

3. Décomposition canonique des éléments de $\mathfrak{X}'$.

Soit $\chi' \in \mathfrak{X}'$ et soit m un multiple du conducteur de χ' ; on suppose $m \not\equiv 0$ modulo l^2 (on pose $m = m'l^n$, $m' \not\equiv 0$ mod l, $n = 0$ ou 1) :

Proposition II.1. – *Sous ces hypothèses :*

i) *Il existe* $\varphi' \in \mathfrak{X}'_{\mathrm{Q}(m')}$ *et* λ, $1 \leqslant \lambda \leqslant l-1$, *uniques, tels que* $\chi' = \varphi'\theta^\lambda$.

ii) *Soit* $\underline{\chi}'$ *l'élément de* $\mathrm{X}(m)$ *associé à* χ' *et soit* $\underline{\varphi}'$ *l'élément de* $\mathrm{X}(m')$ *associé à* φ'. *Alors :*

– *si* l *divise* m, *on a* $\underline{\chi}' = \underline{\varphi}'\underline{\theta}^\lambda$;

– *si* l *ne divise pas* m, *on a* $\underline{\chi}' = \underline{\varphi}'$.

Cette décomposition est alors l'unique décomposition de $\underline{\chi}' \in \mathrm{X}(m)$ *sur* $\mathrm{X}(m') \times \mathrm{X}(l^n)$.

Démonstration. – L'assertion i) résulte de la Rem. I.1 i), compte tenu du fait que $\mathrm{Q}^{(m)}$ est le composé des extensions linéairement disjointes $\mathrm{Q}^{(m')}/\mathrm{Q}$ et $\mathrm{Q}^{(l)}/\mathrm{Q}$ et qu'un élément de $\mathfrak{X}'_{\mathrm{Q}^{(l)}}$ se met de façon unique sous la forme θ^λ, $1 \leqslant \lambda \leqslant l-1$. L'assertion ii) est évidente.

Remarque II.1. – Supposons que $m = f_\chi = lf'_\chi$, $f'_\chi \not\equiv 0$ mod l. Alors, dans la décomposition $\chi' = \varphi'\theta^\lambda$, φ' est de conducteur f'_χ (se déduit aussi de la Rem. I.1), i)).

Remarque II.2. – Le nombre λ est constant sur la Γ_{Q_l}-classe de conjugaison de χ' : en effet, soit $\chi' = \varphi'\theta^\lambda$; le sous-groupe de décomposition de l dans $\mathrm{Q}^{(g_\chi)}/\mathrm{Q}$ est engendré par l'image de l dans $(\mathbf{Z}/g_\chi\mathbf{Z})^*$, d'où, tout Γ_{Q_l}-conjugué de χ' est de la forme $\chi'^{l^i} = \varphi'^{l^i}\theta^{\lambda l^i} = \varphi'^{l^i}\theta^\lambda$, car $\theta^l = \theta$. Ceci permettrait de définir la famille de nombres λ_ϕ, pour $\phi \in \Phi$.

Toujours sous les mêmes hypothèses, on a :

Proposition II.2. – *Soit* $r = (\lambda, l-1)$, *où* λ *est l'entier défini par la décomposition canonique* $\chi' = \varphi'\theta^\lambda$. *Alors l'indice de ramification* e *de* l *dans* K_χ *est égal à* $\dfrac{l-1}{r}$ ·

Démonstration. – Soit L le corps d'inertie de l dans l'extension $Q^{(m)}/K_\chi$; on sait que l'on a $Q^{(m')} \subset L \subset Q^{(m)}$; par définition, on aura $\mathrm{Gal}(Q^{(m)}/L) = \{\sigma \in \mathrm{Gal}(Q^{(m)}/Q^{(m')}),\ \chi'(\sigma) = 1\}$; or $\chi' = \varphi' \theta^\lambda$ et $\chi'(\sigma) = \varphi'(\sigma)\, \theta^\lambda(\sigma) = \theta^\lambda(\sigma)$ et $\mathrm{Gal}(Q^{(m)}/L) = \{\sigma \in \mathrm{Gal}(Q^{(m)}/Q^{(m')}),\ \theta^\lambda(\sigma) = 1\} \simeq \{\sigma \in \mathrm{Gal}(Q^{(l)}/Q),\ \theta^\lambda(\sigma) = 1\}$; la valeur de e en résulte immédiatement puisque θ est un générateur de $\mathfrak{X}'_{Q^{(l)}}$.

4. Sommes de Gauss [14].

a) *Définitions.* Soit $\underline{\chi}' \in X(m)$ et soit $\xi_m = \exp(2i\pi/m)$; on pose $\mathcal{G}_m(\underline{\chi}') = \sum_{a=1}^{m} \underline{\chi}'^{(a)}\, \xi_m^a$. De par le choix de ξ_m, on dit que cette somme de Gauss est la somme de Gauss normée associée à $\underline{\chi}'$ et au module m. C'est donc un élément de Ω_l qui dépend de $\underline{\chi}'$ et du choix de $m \in M(\underline{\chi}')$. Pour simplifier, nous écrirons $\mathcal{G}(\underline{\chi}')$ au lieu de $\mathcal{G}_m(\underline{\chi}')$.

DEFINITION II.4. – *Comme pour les nombres de Bernoulli, on notera $\mathcal{G}(\chi')$ la somme de Gauss $\mathcal{G}(\underline{\chi}')$ lorsque $\underline{\chi}'$ est primitif et que le module considéré est f_χ. Elle sera dite somme de Gauss primitive.*

b) *Décomposition des sommes de Gauss primitives pour $\chi' \in \mathfrak{X}'$.* On a le résultat suivant (cf. [14], § 20, 2) :

PROPOSITION II.3. – *Soit $\chi' \in \mathfrak{X}'$. On suppose que $f_\chi = l f'_\chi, f'_\chi \not\equiv 0$ mod l. Soit $\chi' = \varphi'\theta^\lambda$, $1 \leqslant \lambda \leqslant l-2$, la décomposition canonique de χ' ; alors on a (avec $\underline{\chi}' \in X(f_\chi)$, $\theta \in X(l)$ et $\varphi' \in X(f'_\chi)$) :*

$$\mathcal{G}(\chi') = \underline{\theta}^\lambda(f'_\chi)\, \underline{\varphi}'(l)\, \mathcal{G}(\varphi')\, \mathcal{G}(\theta^\lambda).$$

c) *Valuation des sommes de Gauss.* On désire, entre autre, déterminer la valuation l-adique de $\mathcal{G}(\chi')$, pour $\chi' \in \mathfrak{X}'$. Pour cela on va faire un choix particulier d'une uniformisante du corps $Q_l^{(g_\chi)}\, Q_l^{(f_\chi)}$ qui contient le nombre $\mathcal{G}(\chi')$: si $f_\chi \not\equiv 0$ mod l alors l'uniformisante sera l ; si $f_\chi \equiv 0$ mod l, l'extension $Q_l^{(g_\chi)}\, Q_l^{(f_\chi)}/Q_l^{(l)}$ est non ramifiée et on peut choisir une uniformisante dans $Q_l^{(l)}$. D'après [1] (chap. V, § 6) on peut poser la définition suivante :

DEFINITION II.5. – *On appelle π l'unique uniformisante de $Q_l^{(l)}$ telle que :*

i) $\pi^{l-1} + l = 0$,

ii) $\pi \equiv w - 1 \bmod \pi^2$ (*où* $w = \exp(2i\pi/l)$).

PROPOSITION II.4. — *L'uniformisante* π *est telle que pour tout* $s \in \mathrm{Gal}(\mathbf{Q}_l^{(l)}/\mathbf{Q}_l)$, *on a* $\pi^s = \theta(s)\pi$. *Il en résulte que pour tout* $i > 0$, $i \not\equiv 0 \bmod l-1$, *on a* $\mathrm{Tr}_{\mathbf{Q}_l^{(l)}/\mathbf{Q}_l}(\pi^i) = 0$. *Enfin, pour tout* d *divisant* $l-1$, $\pi^{(l-1)/d}$ *engendre l'unique sous-corps de* $\mathbf{Q}_l^{(l)}$ *de degré* d *sur* $\mathbf{Q}_l$.

Démonstration. — Soit $s \in \mathrm{Gal}(\mathbf{Q}_l^{(l)}/\mathbf{Q}_l)$; comme $\pi^{l-1} = -l$, il en résulte que $\pi^s = \gamma_s \pi$ où $\gamma_s^{l-1} = 1$; calculons γ_s : on a $\pi \equiv w - 1 \bmod \pi^2$, d'où $\pi^s = \gamma_s \pi \equiv w^s - 1 \bmod \pi^2$, soit $\gamma_s \equiv \dfrac{w^s - 1}{w - 1} \bmod \pi$; on sait que $\dfrac{w^s-1}{w-1} \equiv \theta(s) \bmod \pi$, d'où l'égalité $\gamma_s = \theta(s)$. La deuxième partie de la proposition est évidente.

PROPOSITION II.5. — *Soit* $\chi' \in \mathfrak{X}'$. *Si* $f_\chi \not\equiv 0 \bmod l$ *alors* $\mathscr{G}(\chi')$ *est une unité* l*-adique. Si* $f_\chi = l f'_\chi$ *et si* χ' *est décomposé sous la forme* $\chi' = \varphi'\theta^\lambda$; $1 \leqslant \lambda \leqslant l-2$, $\varphi' \in \mathfrak{X}'_{\mathbf{Q}(f'_\chi)}$, *on a* $\mathscr{G}(\chi') = u_{\chi'}\pi^{l-1-\lambda}$, *où* $u_{\chi'} \equiv \theta^\lambda(f'_\chi)\,\underline{\varphi}'(l)\,\mathscr{G}(\varphi')\,(-1)^\lambda\,\lambda! \bmod l$.

Démonstration. — On rappelle que dans $\mathbf{C}$ on a la relation $\mathscr{G}(\chi')\overline{\mathscr{G}(\chi')} = f_\chi$ [18], [14] d'où la première partie de la proposition et, dans le deuxième cas, le fait que $\mathscr{G}(\varphi')$ est une unité l-adique. On est donc ramené à calculer $\mathscr{G}(\theta^\lambda)$ pour $1 \leqslant \lambda \leqslant l-2$.

On a $\mathscr{G}(\theta^\lambda) = \sum_{a=1}^{l-1} \underline{\theta}^\lambda(a)\,w^a$; c'est un élément de $\mathbf{Q}_l^{(l)}$ car $\underline{\theta}^\lambda(a) \in \mathbf{Q}_l$. On peut donc écrire $\mathscr{G}(\theta^\lambda) = u_\lambda \pi^{x\lambda}$, u_λ unité de $\mathbf{Q}_l^{(l)}$. Soit $s \in \mathrm{Gal}(\mathbf{Q}_l^{(l)}/\mathbf{Q}_l)$, alors

$$\mathscr{G}(\theta^\lambda)^s = \sum_{a=1}^{l-1} \underline{\theta}^\lambda(a)\,w^{as} = \theta^{-\lambda}(s)\,\mathscr{G}(\theta^\lambda) = u_\lambda^s\,\pi^{sx\lambda} = u_\lambda^s\,\theta^{x\lambda}(s)\,\pi^{x\lambda} =$$
$$= \theta^{-\lambda}(s)\,u_\lambda\,\pi^{x\lambda},$$

ce qui conduit à $\theta^{x\lambda}(s)\,u_\lambda^s = \theta^{-\lambda}(s)\,u_\lambda$ pour tout s ; on aura donc $u_\lambda^{(l-1)(s-1)} = 1$, soit $u_\lambda^{l-1} \in \mathbf{Q}_l$; si u_λ n'appartient pas à $\mathbf{Q}_l$, $\mathbf{Q}_l(u_\lambda)$ est une extension de Kummer de degré $d > 1$, pour un d tel que

$u_\lambda^d \in \mathbf{Q}_l$; on a de même $\mathbf{Q}_l(u_\lambda) = \mathbf{Q}_l(\pi^{(l-1)/d})$ (Prop. II.4). La théorie de Kummer montre qu'il existe α premier à $(l-1)/d$ tel que $u_\lambda^\alpha = \pi^{(l-1)/d} y$, avec $y \in \mathbf{Q}_l$; u_λ étant une unité, ceci est impossible pour $d \neq 1$, en considérant les valuations des deux membres. Donc $u_\lambda \in \mathbf{Q}_l$ et $\theta^{x_\lambda}(s) = \theta^{-\lambda}(s)$ pour tout s, d'où $x_\lambda \equiv -\lambda \bmod l-1$ et la seule valeur possible (compte tenu du fait que la valuation de $\mathscr{G}(\theta^\lambda)$ est comprise entre 1 et $l-1$) est $x_\lambda = l-1-\lambda$. Pour $\lambda > 1$, calculons

$$(w-1)\,\mathscr{G}(\theta^\lambda) = \sum_{a=1}^{l} \theta^\lambda(a)\,(w^{a+1} - w^a) =$$

$$= \sum_{a=1}^{l} (\theta^\lambda(a-1) - \theta^\lambda(a))\,w^a \ ;$$

on a, pour tout b, $\theta^\lambda(b) \equiv b^\lambda \bmod l$ car $\lambda \neq 0$, d'où

$$(w-1)\,\mathscr{G}(\theta^\lambda) \equiv \sum_{a=1}^{l} w^a((a-1)^\lambda - a^\lambda) \equiv$$

$$\equiv \sum_{a=1}^{l} w^a \sum_{i=1}^{\lambda} C_\lambda^i(-1)^i a^{\lambda-i} \equiv \sum_{i=1}^{\lambda} C_\lambda^i(-1)^i \sum_{a=1}^{l} a^{\lambda-i} w^a \equiv$$

$$\equiv \sum_{i=1}^{\lambda-1} C_\lambda^i(-1)^i \mathscr{G}(\theta^{\lambda-i}) \bmod l \ ,$$

car $\sum_{a=1}^{l} a^{\lambda-i} w^a = 0$ pour $i = \lambda$;

$$(w-1)\,\mathscr{G}(\theta^\lambda) \equiv \sum_{i=1}^{\lambda-1} C_\lambda^i(-1)^i u_{\lambda-i}\,\pi^{l-1-\lambda+i} \bmod l\,,$$

d'où $(w-1)\,u_\lambda\,\pi^{l-1-\lambda} \equiv \sum_{i=1}^{\lambda-1} C_\lambda^i(-1)^i u_{\lambda-i}\,\pi^{l-1-\lambda+i} \bmod \pi^{l-1}$,

d'où $$u_\lambda \equiv -C_\lambda^1 u_{\lambda-1} \bmod \pi^{\lambda-1} \ ;$$

on a donc, pour $\lambda > 1$, $u_\lambda \equiv -\lambda u_{\lambda-1} \bmod l$ puisque u_λ et $u_{\lambda-1} \in \mathbf{Q}_l$. La relation $\mathscr{G}(\theta^\lambda)\,\overline{\mathscr{G}(\theta^\lambda)} = l$ conduit à $u_\lambda u_{l-1-\lambda} = (-1)^{\lambda+1}$ pour $1 \leqslant \lambda \leqslant l-2$. Pour $\lambda = l-2$ on a

$$\mathscr{C}(\theta^{l-2}) = \sum_{a=1}^{l-1} \theta(a)^{l-2}(w^a - 1) \equiv (w-1) \sum_{a=1}^{l-1} a^{l-2} \frac{w^a - 1}{w-1} \equiv$$

$$\equiv (w-1) \sum_{a=1}^{l-1} a^{l-1} \bmod \pi^2 \ ;$$

on a donc $\mathscr{C}(\theta^{l-2}) \equiv -(w-1) \bmod \pi^2$ soit $\mathscr{C}(\theta^{l-2}) \equiv -\pi \bmod \pi^2$. Ceci conduit à $u_{l-2} \equiv -1 \bmod l$, soit $u_1 \equiv -1 \bmod l$; il en résulte immédiatement $u_\lambda \equiv (-1)^\lambda \lambda! \bmod l$, pour $1 \leqslant \lambda \leqslant l-2$. La somme de Gauss $\mathscr{C}(\chi')$ s'écrit

$$\mathscr{C}(\chi') = \underline{\theta}^\lambda(f'_\chi)\, \underline{\varphi}'(l)\, \mathscr{C}(\varphi')\, \mathscr{C}(\theta^\lambda) = \underline{\theta}^\lambda(f'_\chi)\, \underline{\varphi}'(l)\, \mathscr{C}(\varphi')\, u_\lambda \pi^{l-1-\lambda}$$

et on aura bien $u_{\chi'} \equiv \underline{\theta}^\lambda(f'_\chi)\, \underline{\varphi}'(l)\, \mathscr{C}(\varphi')\, (-1)^\lambda \lambda!$ modulo l.

CHAPITRE III

UNITES CYCLOTOMIQUES l-PRIMAIRES DES CORPS K_χ, $\chi \in \mathfrak{X}$

1. Logarithme l-adique des unités ϕ-relatives ($\phi \in \Phi^+$).

a) *Choix d'une uniformisante.* Dans toute la suite, on sera amené à calculer dans les complétés $K_l \subset \hat{\Omega}_l$ des corps K contenus dans Q^a. D'après la Prop. I.3 et le Corol. I.1, lorsque l est ramifié dans K, K est de conducteur lf', $f' \not\equiv 0 \bmod l$. Comme l'extension $Q_l^{(f)}/Q_l^{(l)}$ est non ramifiée, quitte à se placer dans $Q_l^{(f)}$, on peut toujours écrire le développement l-adique d'un élément de K_l selon les puissances de l'uniformisante π (cf. Déf. II.5) avec des coefficients dans le corps $Q_l^{(f')}$. Sur la réunion, Q_l^a, de ces extensions K_l, on a, par restriction de la valuation définie sur Ω_l, une valuation, notée v, que nous normons par l'égalité $v(l) = l - 1$.

b) *Logarithme l-adique.* Nous utilisons dans Q_l^a le prolongement fonctionnel du logarithme l-adique défini normalement sur les nombres congrus à 1 modulo π : Pour toute unité l-adique de Q_l^a, on pose $\operatorname{Log} u = \dfrac{1}{1 - l^N} \operatorname{Log}(u^{1-l^N})$ où N est le degré résiduel de l dans l'extension qui contient u. L'application Log ainsi définie a pour noyau un groupe de racines de l'unité d'ordre premier à l.

Remarque III.1. – Le logarithme des unités de Q_l^a est un entier et on a $v(\operatorname{Log} u - \operatorname{Log} u^{1-l^N}) \geqslant l$.

Definition III.1. – *Soit* $\epsilon = 1 - \alpha\pi^n$, $\alpha \not\equiv 0 \bmod \pi$ *et* $n \geqslant 1$; *on pose* $L(\epsilon) = -\sum_{i=1}^{l-1} \dfrac{(\alpha\pi^n)^i}{i}$.

Remarque III.2. – On a $v(L(\epsilon)) = v(\epsilon - 1)$.

Proposition III.1. – *On a* $\operatorname{Log} \epsilon \equiv L(\epsilon) \bmod \pi^l$ *sauf si* $n = 1$ *auquel cas on a* $\operatorname{Log} \epsilon \equiv L(\epsilon) + \alpha^l \pi \bmod \pi^l$.

c) *Unités ϕ-relatives.*

DEFINITION III.2. – *Soit $\phi \in \Phi^+$ et soit χ le caractère rationnel au-dessus de ϕ. Nous appellerons unité ϕ-relative toute unité $\epsilon \in E_{K_\chi}$ telle que l'image de ϵ dans $E_{K_\chi}/E^l_{K_\chi}$ soit invariante par e_ϕ. Nous désignons par e'_ϕ un résidu modulo l dans $\mathbf{Z}[G_\chi]$ de e_ϕ ; il est clair que ϵ est ϕ-relative si et seulement si $\epsilon^{e'_\phi} = \epsilon u^l$, $u \in E_{K_\chi}$.*

PROPOSITION III.2. – *Soit $\phi \in \Phi^+$ et soit ϵ une unité ϕ-relative. Alors* $\operatorname{Log} \epsilon \equiv a_\lambda \pi^\lambda \bmod \pi^l$, *avec* $a_\lambda \in \mathbf{Z}_l^{(f'_\chi)}$, *où* λ, $1 \leqslant \lambda \leqslant l-1$ *est défini par la décomposition canonique de* χ' : $\chi' = \varphi' \theta^\lambda$.

Démonstration. – Montrons le résultat suivant :

LEMME III.1. – *Si ϵ est ϕ-relative alors l'élément*

$$e^\chi_{\theta^\lambda} = \frac{1}{l-1} \sum_{s \in H_1} \theta^{-\lambda}(s)\, \overline{s},$$

où $H_1 \simeq \operatorname{Gal}(\mathbf{Q}_l^{(l)}/\mathbf{Q}_l)$ *est le groupe d'inertie de* $\mathbf{Q}_l^a/\mathbf{Q}_l$ *et où* $\overline{s}$ *désigne la restriction de* s *à* K_χ, *est tel que* $e^\chi_{\theta^\lambda} \operatorname{Log} \epsilon \equiv \operatorname{Log} \epsilon \bmod \pi^l$ *(cette écriture a un sens car $\overline{s}$ est un élément du groupe de décomposition de l dans K_χ).*

Dans $E_{K_\chi}/E^l_{K_\chi}$, on a $\overline{\epsilon}^{\,e_\phi} = \overline{\epsilon}$ et $\overline{\epsilon}^{\,e^\chi_{\theta^\lambda}} = \overline{\epsilon}^{\,e_\phi e^\chi_{\theta^\lambda}}$. Calculons $e_\phi e^\chi_{\theta^\lambda}$; pour cela on calcule $e_{\chi'} e^\chi_{\theta^\lambda}$ pour $\chi' \mid \phi$. On a

$$e_{\chi'} e^\chi_{\theta^\lambda} = \frac{1}{g_\chi} \sum_{\sigma \in G_\chi} \chi'(\sigma^{-1})\, \sigma \frac{1}{l-1} \sum_{s \in H_1} \theta^{-\lambda}(s)\, \overline{s} =$$

$$= \frac{1}{g_\chi} \frac{1}{l-1} \sum_{s \in H_1} \chi'(\sigma^{-1})\, \theta^{-\lambda}(s)\, \sigma \overline{s} =$$

$$= \frac{1}{g_\chi (l-1)} \sum_{\tau \in G_\chi} \sum_{s \in H_1} \chi'(\overline{s} \tau^{-1})\, \theta^{-\lambda}(s)\, \tau =$$

$$= \frac{1}{g_\chi} \sum_{\tau \in G_\chi} \chi'^{-1}(\tau)\, \tau \frac{1}{l-1} \sum_{s \in H_1} \chi'(\overline{s})\, \theta^{-\lambda}(s) \;;$$

or $\chi' = \varphi'\theta^\lambda$, d'où $\sum_{s \in H_1} \chi'(\bar{s})\,\theta^{-\lambda}(s) = \sum_{s \in H_1} 1 = l - 1$ et

et $e_{\chi'}\, e^{\chi}_{\theta^\lambda} = e_{\chi'}$;

comme λ est constant sur la Γ_{Q_l}-classe de χ' (cf. Rem. II.2), on aura $e_\phi\, e^{\chi}_{\theta^\lambda} = e_\phi$, d'où $\bar{\epsilon}^{\,e^{\chi}_{\theta^\lambda}} = \bar{\epsilon}^{\,e_\phi} = \bar{\epsilon}$. Il en résulte immédiatement la relation $\operatorname{Log} \epsilon \equiv e^{\chi}_{\theta^\lambda} \operatorname{Log} \epsilon \equiv \dfrac{1}{l-1} \sum_{s \in H_1} \theta^{-\lambda}(s) \operatorname{Log} \epsilon^s \bmod \pi^l$.

Fin de la démonstration de la proposition. – On peut toujours écrire $\operatorname{Log} \epsilon \equiv \sum_{i=1}^{l-1} a_i \pi^i \bmod \pi^l$, $a_i \in \mathbf{Z}_l^{(f'_\chi)}$, en tenant compte de la relation $\pi^{l-1} = -l$. On aura

$$\operatorname{Log} \epsilon \equiv e^{\chi}_{\theta^\lambda} \operatorname{Log} \epsilon \equiv \frac{1}{l-1} \sum_{s \in H_1} \theta^{-\lambda}(s) \sum_{i=1}^{l-1} a_i^s \pi^{is} (\bmod \pi^l) \equiv$$

$$\equiv \frac{1}{l-1} \sum_{s \in H_1} \theta^{-\lambda}(s) \sum_{i=1}^{l-1} a_i\, \theta^i(s)\, \pi^i \equiv$$

$$\equiv \frac{1}{l-1} \sum_{i=1}^{l-1} a_i \pi^i \sum_{s \in H_1} \theta^{-\lambda}(s)\, \theta^i(s) \bmod \pi^l \ ;$$

or $\sum_{s \in H_1} \theta^{-\lambda}(s)\, \theta^i(s) = 0$ sauf si $i \equiv \lambda \bmod l-1$, auquel cas cette somme vaut $l - 1$, ce qui se produit une fois et une seule puisque $\lambda \in \{1, 2, \ldots, l-1\}$, d'où $\operatorname{Log} \epsilon \equiv a_\lambda \pi^\lambda \bmod \pi^l$.

COROLLAIRE III.1. – *Si $\epsilon \equiv 1 \bmod \pi$, ϵ ϕ-relative, alors* $\mathrm{L}(\epsilon) \equiv b_\lambda \pi^\lambda \bmod \pi^l$, $b_\lambda \in \mathbf{Z}_l^{(f'_\chi)}$. *Ceci résulte du fait que la fonction* L *est, modulo π^l, multiplicative* (cf. [1], chap. V, § 6) ; *on obtient alors* $\mathrm{L}(\epsilon) \equiv e^{\chi}_{\theta^\lambda} \mathrm{L}(\epsilon) \bmod \pi^l$ *et la suite des calculs est la même que ci-dessus à partir de l'expression* $\mathrm{L}(\epsilon) = \sum_{i=1}^{l-1} b_i \pi^i$, $b_i \in \mathbf{Z}_l^{(f'_\chi)}$.

2. Logarithme des unités cyclotomiques ϕ-relatives ($\phi \in \Phi^+$).

Nous supposons $f_\chi \neq l$, le cas $f_\chi = l$ étant connu [1], [6] et devant être traité à part. On sait que F_χ est engendré par η_χ qui a été définie dans le chap. I, § 2, d). Posons $\xi_\chi = \exp(2i\pi/f_\chi)$, $N_{Q^{(f_\chi)}/K_\chi}(1 - \xi_\chi) = \Theta_\chi$ et $\Theta_\phi = \Theta_\chi^{e'_\phi}$ pour tout $\phi \mid \chi$.

Proposition III.3. – *Soit $\phi \in \Phi^+$, $\phi \neq 1$. On suppose $f_\chi \neq l$. Le nombre Θ_ϕ est un l-entier de K_χ et il existe une unité ϕ-relative η_ϕ telle que $\Theta_\phi = \eta_\phi u^l$, u l-entier de K_χ, et telle que l'image de η_ϕ dans $\mathfrak{F}_\phi$ soit génératrice.*

Démonstration. – D'après la définition de η_χ, on aura $\eta_\chi^2 = \Theta_\chi^{D_\chi}$ où $D_\chi = \frac{1}{|V_\chi|}\left(\sum_{\tau \in V_\chi} \tau\right) \prod_{p \mid g_\chi} (1 - \sigma_\chi^{g_\chi/p})$ (p premier) (cf. [19] et chap. I, § 2, d) ; mais comme $\Theta_\chi \in K_\chi$, on a $\eta_\chi^2 = \Theta_\chi^{D'_\chi}$ avec $D'_\chi = \prod_{p \mid g_\chi} (1 - \sigma_\chi^{g_\chi/p}) \in \mathbf{Z}_l[G_\chi]$. Plaçons nous dans le $\mathbf{Z}_l[G_\chi]$ e_ϕ-module $(K_\chi^*/K_\chi^{*l})^{e_\phi}$ et désignons par $q_\phi(\alpha)$ l'image de $\alpha \in K_\chi^*$ dans ce module (i.e. $q_\phi(\alpha) = \alpha^{e'_\phi} K_\chi^{*l}$, par exemple). Considérons $(K_\chi^*/K_\chi^{*l})^{e_\phi}$ comme $\mathbf{Z}_l^{(g_\chi)}$-module (Prop. I.4 Rem. I.2) et calculons l'image de D'_χ par l'isomorphisme i_ϕ : $i_\phi(D'_\chi) = \prod_{p \mid g_\chi} (1 - \gamma_\phi^{g_\chi/p})$, où γ_ϕ est une racine primitive g_χ^e de l'unité convenable ; il en résulte que pour tout $p \mid g_\chi$, $1 - \gamma_\phi^{g_\chi/p}$ est un entier de $\mathbf{Z}_l^{(g_\chi)}$ premier à l et que $\omega = i_\phi(D'_\chi)$ est inversible dans $\mathbf{Z}_l^{(g_\chi)}$. On a donc $q_\phi(\Theta_\chi) = q_\phi(\eta_\chi)^{\omega'}$, ω' inversible dans $\mathbf{Z}_l^{(g_\chi)}$. En relevant cette égalité dans K_χ, on obtient une égalité de la forme $\Theta_\phi = \eta_\chi^{e'_\phi \Omega} u^l$, $\Omega \in \mathbf{Z}[G_\chi]$, avec $i_\phi(\Omega) = \omega'$ et $u \in K_\chi^*$; il suffit de poser $\eta_\phi = \eta_\chi^{e'_\phi \Omega}$, on constate alors que $\mathfrak{F}_\phi$ est engendré par l'image de η_ϕ. Le fait que Θ_χ soit (pour $f_\chi \neq l$) l-entier résulte de [19], § 8, 2 ; d'où, Θ_ϕ et u sont l-entiers et la proposition est démontrée.

Definition III.3. – *On pose $\overline{\Theta}_\phi = \Theta_\phi^{1-l^N}$ (N étant le degré résiduel de l dans $\mathbf{Q}^{(f_\chi)}$).*

PROPOSITION III.4. — *Soit* $s \in G_\chi$.

i) *On a* $\mathrm{Log}(\overline{\Theta}{}_\phi^s) \equiv a_\lambda \pi^\lambda \bmod \pi^l$, $a_\lambda \in \mathbf{Z}_l^{(f'_\chi)}$,

ii) *On a* $\mathrm{L}(\overline{\Theta}{}_\phi^s) \equiv b_\lambda \pi^\lambda \bmod \pi^l$, $b_\lambda \in \mathbf{Z}_l^{(f'_\chi)}$,

iii) *Si* $\lambda \neq 1$, *alors* $a_\lambda \equiv b_\lambda \bmod l$.

Démonstration. — On a (Prop. III.3) : $\Theta_\phi = \eta_\phi u^l$, η_ϕ unité ϕ-relative, u l-entier. Il en résulte que pour s fixé, $\mathrm{Log}(\overline{\Theta}{}_\phi^s) \equiv \mathrm{Log}(\eta_\phi^{s(1-l^{\mathrm{N}})})$ mod π^l ; d'après la Prop. III.2, $\mathrm{Log}\,\eta_\phi^{s(1-l^{\mathrm{N}})} \equiv a_\lambda \pi^\lambda \bmod \pi^l$, $a_\lambda \in \mathbf{Z}_l^{(f'_\chi)}$, d'où i). On aura de même, d'après le Corol. III.1, $\mathrm{L}(\overline{\Theta}{}_\phi^s) \equiv \mathrm{L}(\eta_\phi^{s(1-l^{\mathrm{N}})})$ mod π^l, soit $\mathrm{L}(\overline{\Theta}{}_\phi^s) \equiv b_\lambda \pi^\lambda \bmod \pi^l$, d'où ii). Posons $\overline{\Theta}{}_\phi^s = 1 - \alpha\pi$, α entier l-adique ; d'après la Prop. III.1, on a $\mathrm{L}(\overline{\Theta}{}_\phi^s) \equiv \mathrm{Log}(\overline{\Theta}{}_\phi^s) - \alpha^l \pi$ mod π^l, soit $\mathrm{L}(\overline{\Theta}{}_\phi^s) \equiv a_\lambda \pi^\lambda - \alpha^l \pi \bmod \pi^l$, soit $b_\lambda \pi^\lambda \equiv a_\lambda \pi^\lambda - \alpha^l \pi$ modulo π^l. Si $\lambda \neq 1$, alors on a nécessairement $\alpha \equiv 0 \bmod \pi$ d'où $b_\lambda \equiv a_\lambda \bmod \pi^{l-\lambda}$ ce qui entraîne $b_\lambda \equiv a_\lambda \bmod l$ puisque $a_\lambda, b_\lambda \in \mathbf{Z}_l^{(f'_\chi)}$.

COROLLAIRE III.2. — α) *Les conditions suivantes sont équivalentes :*

i) $\mathfrak{F}_\phi^0 = \mathfrak{F}_\phi$ (i.e. $b_\phi = 1$, cf. Déf. I.11),

ii) $\mathrm{L}(\overline{\Theta}{}_\phi^s) \equiv 0 \bmod \pi^l$, *pour tout* $s \in G_\chi$.

β) Si $\lambda \neq 1$, *les conditions suivantes sont équivalentes :*

i) $\mathfrak{F}_\phi^0 = \mathfrak{F}_\phi$ (i.e. $b_\phi = 1$),

ii) $\mathrm{Log}(\overline{\Theta}{}_\phi^s) \equiv 0 \bmod \pi^l$, *pour tout* $s \in G_\chi$.

Ceci résulte de la Prop. III.3 et du Corol. I.5 sur la l-primarité.

On est conduit à poser la définition suivante :

DEFINITION III.4. — *Soit* $\phi \in \Phi^+$. *On dira qu'on est dans le cas "spécial" si le nombre* λ *(qui ne dépend que de* ϕ*) dans la décomposition canonique de* $\chi' \mid \phi$, $\chi' = \varphi' \theta^\lambda$, *est égal à* 1.

Remarque III.3. — Dans le cas "spécial", on a donc $\chi' = \varphi'\theta$, $\varphi' \in \mathfrak{X}'_{\mathbf{Q}^{(f'_\chi)}}$. On constate que le cas "spécial" est caractérisé par le fait que le caractère miroir $\overline{\phi}$ (impair) de ϕ est de conducteur premier à l (ici $\overline{\phi}$ est le caractère l-adique au-dessus de φ'^{-1}). L'exemple le plus simple de cette situation est donné, pour $l = 3$, par $\mathrm{K}_\chi = \mathbf{Q}(\sqrt{3d})$, $d > 0$, $d \not\equiv 0 \bmod 3$ (on a ici $\phi = \chi$ et $\overline{\phi}$ est le caractère quadratique associé à $\mathbf{Q}(\sqrt{-d})$) (voir aussi les chap. IV, § 4 et V, § 4) ;

3. Caractérisation de la condition $b_\phi = 1$ dans le cas non "spécial".

Les propriétés des fonctions L_l l-adiques de Leopoldt-Fresnel vont nous permettre d'établir un critère simple pour la condition $b_\phi = 1$, dans tous les cas envisagés (à savoir $\phi \in \Phi^+$, $\phi \neq 1$, $f_\chi \neq l$) sauf dans le cas "spécial".

a) *Fonctions* $L_l(\chi')$. Soit $\underline{\chi}'$ un caractère primitif pair. On suppose $f_\chi \neq l$. D'après Leopoldt et Fresnel [16], [4], les nombres $L_l(\chi') = -\dfrac{\mathscr{C}(\chi')}{f_\chi} \sum\limits_{a=1}^{f_\chi} \underline{\chi}'^{-1}(a) \operatorname{Log}(1 - \xi_\chi^a)$ sont reliés aux valeurs en 1 des fonctions L_l l-adiques par l'expression $L_l(1, \chi') = \left(1 - \dfrac{\underline{\chi}'(l)}{l}\right) L_l(\chi')$.

On a alors le résultat suivant :

PROPOSITION III.5 (Fresnel, [4]). – *Soit $\underline{\chi}'$ un caractère primitif pair ; on suppose $f_\chi \neq l$. On a la congruence :* $L_l(1, \chi') \equiv B_1(\underline{\chi}'\underline{\theta}^{-1})$ mod l *dans* $Q_l^{(g_\chi)}$.

L'expression de $L_l(\chi')$ conduit au résultat suivant :

LEMME III.2. – *Soit $\phi \in \Phi^+$, $\phi \neq 1$; on suppose $f_\chi \neq l$. Pour tout $s \in G_\chi$, on a* $\operatorname{Log} \Theta_\phi^s \equiv -\dfrac{1}{g_\chi} \sum\limits_{\chi' | \phi} \chi'(s) \mathscr{C}(\chi'^{-1}) \dfrac{l}{l - \underline{\chi}'(l)} L_l(1, \chi')$ mod π^l.

Démonstration. – Posons $\Gamma_\chi = \operatorname{Gal}(Q^{(f_\chi)}/Q)$; on a

$$\sum_{a=1}^{f_\chi} \underline{\chi}'^{-1}(a) \operatorname{Log}(1 - \xi_\chi^a) = \sum_{\sigma \in \Gamma_\chi} \chi'^{-1}(\sigma) \operatorname{Log}(1 - \xi_\chi^\sigma) ;$$

posons $\sigma = \bar{s}\tau$ (en notant par $\bar{s} \in \Gamma_\chi$ un prolongement quelconque dans Γ_χ de $s \in G_\chi$) ; il vient :

$$\sum_{\tau \in \Gamma_\chi} \chi'^{-1}(\bar{s}\tau) \operatorname{Log}(1 - \xi_\chi^{\tau\bar{s}}) = \chi'^{-1}(s) \sum_{\tau \in \Gamma_\chi} \chi'^{-1}(\tau) \operatorname{Log}(1 - \xi_\chi^{\tau\bar{s}}) =$$

$$= \chi'^{-1}(s) \sum_{\tau \in V_\chi} \sum_{\sigma_i} \chi'^{-1}(\sigma_i) \operatorname{Log}(1 - \xi_\chi^{\tau\sigma_i\bar{s}}) =$$

$$= \chi'^{-1}(s) \sum_{\sigma_i} \chi'^{-1}(\sigma_i) \operatorname{Log}(N(1 - \xi_\chi^{\sigma_i\bar{s}}))$$

(N désigne la norme dans l'extension $Q^{(f_\chi)}/K_\chi$; les σ_i représentent G_χ) $= \chi'^{-1}(s) \sum_{\sigma_i} \chi'^{-1}(\sigma_i) \operatorname{Log} \Theta_\chi^{\sigma_i s}$, d'où

$$\sum_{\sigma \in G_\chi} \chi'^{-1}(\sigma) \operatorname{Log} \Theta_\chi^{\sigma s} = -\chi'(s) \frac{f_\chi}{\mathscr{C}(\chi')} L_l(\chi') = -\chi'(s) \overline{\mathscr{C}(\chi')} L_l(\chi') \ ;$$

mais $\overline{\mathscr{C}(\chi')} = \sum_{a=1}^{f_\chi} \underline{\chi}'^{-1}(a)\, \xi_\chi^{-a} = \sum_{a=1}^{f_\chi} \underline{\chi}'^{-1}(-a)\, \xi_\chi^{a}$;

or $\underline{\chi}'$ étant pair, on aura $\overline{\mathscr{C}(\chi')} = \mathscr{C}(\chi'^{-1})$. Il en résulte par sommation sur $\chi' \mid \phi$:

$$\sum_{\sigma \in G_\chi} \phi(\sigma^{-1}) \operatorname{Log}(\Theta_\chi^{\sigma s}) = -\sum_{\chi' \mid \phi} \chi'(s)\, \mathscr{C}(\chi'^{-1})\, L_l(\chi') = -$$

$$= -\sum_{\chi' \mid \phi} \chi'(s)\, \mathscr{C}(\chi'^{-1}) \frac{l}{l - \underline{\chi}'(l)} L_l(1\,,\chi')\,.$$

Comme $e'_\phi \equiv e_\phi \bmod l$ et $\operatorname{Log}(\Theta_\chi^{\sigma s}) \equiv 0 \bmod \pi$, on en déduit que $\operatorname{Log} \Theta_\phi^s \equiv -\dfrac{1}{g_\chi} \sum_{\chi' \mid \phi} \chi'(s)\, \mathscr{C}(\chi'^{-1}) \dfrac{l}{l - \underline{\chi}'(l)} L_l(1\,,\chi') \bmod \pi^l$. Le résultat essentiel est alors le suivant, dans le cas non spécial :

PROPOSITION III.6. – *Soit $\phi \in \Phi^+$, $\phi \neq 1$; on suppose $f_\chi \neq l$ et $\lambda \neq 1$. Alors les conditions suivantes sont équivalentes :*

i) $b_\phi = 1$,

ii) *le nombre de Bernoulli primitif* $B_1(\chi'\theta^{-1})$ *est congru à* 0 *modulo* $\mathscr{L}_\chi$ *dans* $Q^{(g_\chi)}$ *(condition indépendante du choix de* $\chi' \mid \phi$*),*

iii) $m_{\overline{\phi}}(h) > 0$, *où* $\overline{\phi}$ *est le caractère miroir de* ϕ.

Démonstration. – La condition i) équivaut à $\operatorname{Log}(\overline{\Theta}_\phi^s) \equiv 0 \bmod \pi^l$, pour tout $s \in G_\chi$ (Corol. III.2, β) ce qui équivaut à (Lemme III.2) : $\sum_{\chi' \mid \phi} \chi'^{-1}(s)\, \mathscr{C}(\chi'^{-1}) \dfrac{l}{l - \underline{\chi}'(l)} L_l(1\,,\chi') \equiv 0 \bmod \pi^l$, pour tout $s \in G_\chi$.

Considérons la matrice $(\chi'(\sigma_\chi^k))_{\substack{k=1,\dots g_\chi \\ \chi' \mid \phi}} = \left(\chi_0'^{l^i}(\sigma_\chi^k)\right)_{\substack{k=1,\dots,g_\chi \\ i=1,\dots,\phi(1)}}$, où

$\chi_0' \mid \phi$ est fixé et où $\phi(1)$ est le degré résiduel de l dans $\mathrm{Q}^{(g_\chi)}/\mathrm{Q}$; cette matrice est de rang $\phi(1)$: en effet, elle est du type Vandermonde et il suffit de prouver que $\chi_0'^{l^i}(\sigma_\chi) = \chi_0'^{l^j}(\sigma_\chi)$ entraîne $i \equiv j \bmod \phi(1)$; or une telle égalité entraîne $\chi_0'^{l^i} = \chi_0'^{l^j}$ (puisque σ_χ est un générateur de G_χ), ce qui conduit au résultat par définition du degré résiduel. La condition nécessaire et suffisante devient donc

$$\mathscr{C}(\chi'^{-1}) \frac{l}{l - \underline{\chi}'(l)} \mathrm{L}_l(1\,, \chi') \equiv 0 \bmod \pi^l ,$$

pour tout $\chi' \mid \phi$. Distinguons deux cas :

α) $f_\chi \not\equiv 0 \bmod l$. Dans ce cas, la condition devient :

$$\frac{\mathscr{C}(\chi'^{-1})}{l - \underline{\chi}'(l)} \mathrm{L}_l(1\,, \chi') \equiv 0 \bmod \pi$$

(car $\underline{\chi}'(l) \neq 0$) soit, puisque $\mathscr{C}(\chi'^{-1})$ est une unité l-adique (Prop. II.5) , $\mathrm{L}_l(1\,, \chi') \equiv 0 \bmod \pi$, soit $\mathrm{B}_1(\underline{\chi}'\underline{\theta}^{-1}) \equiv 0 \bmod \pi$ (Prop. III.5), ce qui se traduit encore par $\mathrm{B}_1(\underline{\chi}'\underline{\theta}^{-1}) \equiv 0 \bmod \mathscr{L}_\chi$ puisque $\mathrm{B}_1(\underline{\chi}'\underline{\theta}^{-1})$ appartient à $\mathrm{Q}^{(g_\chi)}$. On a enfin $\mathrm{B}_1(\underline{\chi}'\underline{\theta}^{-1}) = \mathrm{B}_1(\chi'\theta^{-1})$ car $\underline{\chi}'\underline{\theta}^{-1}$ est primitif.

β) $f_\chi \equiv 0 \bmod l$. Dans ce cas $\underline{\chi}'(l) = 0$ et la condition devient $\mathscr{C}(\chi'^{-1})\, \mathrm{L}_l(1\,, \chi') \equiv 0 \bmod \pi^l$. On utilise alors l'expression de la somme de Gauss donnée par la Prop. II.5, ce qui conduit immédiatement à la condition $\mathrm{L}_l(1\,, \chi') \equiv 0 \bmod \pi^{\lambda+1}$, soit $\mathrm{B}_1(\underline{\chi}'\underline{\theta}^{-1}) \equiv 0 \bmod \pi^{\lambda+1}$, mais $\mathrm{B}_1(\underline{\chi}'\underline{\theta}^{-1})$ est un élément de $\mathrm{Q}^{(g_\chi)}$ extension non ramifiée de Q pour l, donc, puisque $\lambda + 1$ est au plus égal à $l - 1$, cette congruence est équivalente à $\mathrm{B}_1(\underline{\chi}'\underline{\theta}^{-1}) \equiv 0 \bmod \mathscr{L}_\chi$. On a $\underline{\chi}'\underline{\theta}^{-1} \in \mathrm{X}(f_\chi)$; or $\chi'\theta^{-1} = \varphi'\theta^{\lambda-1}$ est de conducteur $lf_\chi' = f_\chi$ pour $\lambda \neq 1$, mais la circonstance $\lambda = 1$ est justement écartée. D'où la condition ii) dans ce cas.

L'assertion iii) va résulter du lemme suivant :

LEMME III.3. – *Soit* $\psi' \in \mathfrak{X}'^-$, $\psi' \neq \theta$. *Alors* $\mathrm{B}_{\psi'} = \mathrm{B}_1(\psi'^{-1})$.

On utilise la formule de récurrence (chap. II, § 2, b) définissant les nombres de Bernoulli pour le caractère primitif $\underline{\psi}'^{-1}$, $m = f_\psi$, et $n = 1$; on obtient : $\mathrm{B}_0(\psi'^{-1})\, f_\psi^2 + 2\mathrm{B}_1(\psi'^{-1})\, f_\psi = 2 \sum_{a=1}^{f_\chi} \underline{\psi}'^{-1}(a) a$;

mais $B_0(\underline{\psi}'^{-1}) = 0$ car ψ' n'est pas le caractère unité, d'où le résultat compte tenu de la définition de $B_{\psi'}$ (Déf. I.7).

Démonstration de iii). – On a $B_1(\chi'\theta^{-1}) = B_{\chi'^{-1}\theta}$, d'après le lemme III.3, car $\chi'^{-1}\theta \in \mathfrak{X}'^{-}$ et $\chi'^{-1}\theta \neq \theta$ puisque $\chi' \neq 1$. La condition $m_{\bar{\phi}}(h) > 1$ résulte de la définition de $m_{\bar{\phi}}(h)$ compte tenu du fait que l'élément de Φ au-dessus de $\chi'^{-1}\theta$ est $\bar{\phi}$.

4. Conclusion.

L'utilisation des fonctions L_l l-adiques permet d'obtenir une caractérisation simple de la condition $b_\phi = 1$, à partir des invariants analytiques définis au chap. I, dans le cas non "spécial" (i.e. $\lambda \neq 1$). Le résultat général que nous avons obtenu dans le chap. IV montre clairement que le cas "spécial" est lié à un problème de caractères primitifs : en effet, si $\chi' = \varphi'\theta$, on a aussi (Prop. II.1, ii))

$$\underline{\chi}' = \underline{\varphi}'\underline{\theta} \quad (\underline{\chi}' \in X(f_\chi),\ \underline{\varphi}' \in X(f'_\chi)) \ ;$$

or la fonction L_l, dans ce cas, s'approche au moyen du nombre de Bernoulli $B_1(\underline{\theta}\,\underline{\chi}'^{-1}) = B_1(\underline{\theta}\,\underline{\varphi}'^{-1}\underline{\theta}^{-1}) = B_1(\underline{\varphi}'^{-1}\underline{\theta}^0)$ distinct du nombre de Bernoulli primitif $B_1(\varphi'^{-1})$ qui, d'après nos résultats (th. IV.1), doit seul intervenir. De plus comme

$$B_1(\underline{\varphi}'^{-1}\underline{\theta}^0) = B_1(\varphi'^{-1})\,(1 - \underline{\varphi}'^{-1}(l))\,,$$

il n'est pas étonnant de ne pas pouvoir atteindre l'énoncé général puisque le cas $\underline{\varphi}'(l) = 1$ peut parfaitement se produire (cf. Rem. III.4, ci-dessus).

Nous pensons que ce phénomène est à la base de la présence dans certains énoncés de [3] de la condition supplémentaire $\varphi(l) \neq 1$, condition qui devrait donc pouvoir être éliminée à notre avis ; même remarque en ce qui concerne certains énoncés de [12] et ce qui est dit à la fin du § 4 de [12]. Nous proposons dans le chapitre suivant une résolution partielle du problème qui semble confirmer l'inadaptation de la fonction Log l-adique dans les définitions classiques.

Remarque III.4. – Les caractères $\chi' \in \mathfrak{X}'$ pour lesquels $\lambda = 1$ et $\varphi'(l) = 1$ sont exactement ceux pour lesquels $\overline{\chi}'$ est trivial sur le groupe de décomposition de l dans $\mathbf{Q}^a/\mathbf{Q}$. On peut appeller ces caractères les caractères singuliers relativement à l ; cette propriété est stable par $\Gamma_{\mathbf{Q}_l}$-conjugaison uniquement, ainsi nous pouvons parler des caractères l-adiques singuliers (ensemble noté Φ^*). On peut aussi dire que les miroirs des caractères singuliers sont exactement les éléments de $\mathfrak{X}'_{\mathbf{Q}_D}$ si $\mathbf{Q}_D$ est le corps de décomposition de l dans $\mathbf{Q}^a$. La propriété d'être miroir d'un caractère singulier est, elle, stable par $\Gamma_{\mathbf{Q}}$-conjugaison.

CHAPITRE IV

CARACTERISATION DE LA CONDITION $b_\phi = 1$ PAR LA METHODE DES SERIES FORMELLES

Dans tout le chapitre, $\phi \mid \chi$ désigne un élément de Φ^+ différent de 1. De plus, le cas $e = 1$ (i.e. $\lambda = l - 1$) ayant été résolu dans le chap. III et le cas $f_\chi = l$ étant connu, nous supposerons $f_\chi = l f'_\chi$, $f'_\chi \neq 1$, $f'_\chi \not\equiv 0 \bmod l$. On rappelle que tout $\chi' \mid \phi$ est décomposé sous la forme $\chi' = \varphi' \theta^\lambda$, $1 \leqslant \lambda \leqslant l - 2$, $\varphi' \in \mathcal{X}'_{\mathbf{Q}^{(f'_\chi)}}$ et λ ne dépendant que de ϕ. Dans ces conditions, $b_\phi = 1$ (i.e. $\mathcal{F}'^{\,0}_\phi = \mathcal{F}'_\phi$) équivaut à $\mathrm{L}(\overline{\Theta}^s_\phi) \equiv 0 \bmod \pi^l$ pour tout $s \in \mathrm{G}_\chi$ (corol. III.2, α). Nous allons étudier $\mathrm{L}(\overline{\Theta}^s_\phi)$ modulo π^l.

1. Etude de $\mathrm{L}(\overline{\Theta}^s_\phi)$.

a) *Rappels.* On rappelle que dans $\mathbf{Q}_l^a$ si $\epsilon = 1 - \alpha\,\pi^n$, α l-entier, $n \geqslant 1$, alors $\mathrm{L}(\epsilon) = -\sum_{i=1}^{l-1} \frac{(\alpha\pi^n)^i}{i}$.

Définissons aussi sur $\mathbf{Q}_l^a$ la fonction E : pour $\omega \equiv 0 \bmod \pi$, $\mathrm{E}(\omega) = \sum_{i=0}^{l-1} \frac{\omega^i}{i\,!}$.

Les fonctions L et E ainsi définies ont les propriétés suivantes ([1], chap. V, § 6 et [15]) :

LEMME IV.1. — i) *Soient* ϵ_1 *et* ϵ_2 *des unités l-adiques congrues à* 1 *modulo* π ; *alors* $\mathrm{L}(\epsilon_1\epsilon_2) \equiv \mathrm{L}(\epsilon_1) + \mathrm{L}(\epsilon_2) \bmod \pi^l$.

ii) *On a* $\mathrm{E}(k\pi) \equiv w^k \bmod \pi^l$, *pour tout* $k \in \mathbf{Z}$.

b) *Calcul modulo l de* $\mathrm{L}(\overline{\Theta}^s_\phi)$. Commençons par faire une remarque qui simplifiera de beaucoup le calcul de $\mathrm{L}(\overline{\Theta}^s_\phi) \bmod \pi^l$:

Remarque IV.1. — D'après le corol. III.1, on a $\mathrm{L}(\overline{\Theta}^s_\phi) \equiv b_\lambda \pi^\lambda \bmod \pi^l$, $b_\lambda \in \mathbf{Z}_l^{(f'_\chi)}$. Comme on a supposé l ramifié dans K_χ, on a donc $1 \leqslant \lambda \leqslant l - 2$; on peut alors effectuer les calculs de la manière suivante : on calcule $L(\overline{\Theta}^s_\phi)$ modulo π^{l-1} au lieu de π^l. Soit R_s le résidu obtenu. Alors la condition $b_\phi = 1$ est équivalente à $R_s \equiv 0 \mod \pi^{l-1}$, pour tout $s \in G_\chi$ (en effet, on aura

$$L(\overline{\Theta}^s_\phi) = R_s + \beta_s \pi^{l-1} \equiv b_\lambda \pi^\lambda \mod \pi^l \ ;$$

donc $b_\phi = 1$ équivaut à $b_\lambda \equiv 0 \mod l$. Si $b_\lambda \equiv 0 \mod l$ alors $R_s \equiv 0 \mod \pi^{l-1}$ et, inversement, si $R_s \equiv 0 \mod \pi^{l-1}$, on aura $R_s + \beta_s \pi^{l-1} = \gamma_s \pi^{l-1} \equiv b_\lambda \pi^\lambda \mod \pi^l$; comme $\lambda \neq l-1$, on obtient bien $b_\lambda \equiv 0 \mod l$).

On a $\overline{\Theta}_\phi = \overline{\Theta}_\chi^{e'_\phi}$, où $\overline{\Theta}_\chi = \prod_{u \in V_\chi} (\xi_\chi^u - 1)^{l^N - 1}$; on a

$$(\xi_\chi - 1)^{l^N} \equiv \xi_\chi^{l^N} - 1 \mod l,$$

soit, en posant $l^N = 1 + tf'_\chi$, $t \not\equiv 0 \mod l$, puisque N est aussi le degré résiduel de l dans $Q^{(f'_\chi)}$, $\xi_\chi^{l^N} = \xi_\chi \xi_\chi^{tf'_\chi}$; or $\xi_\chi^{f'_\chi} = w$, ce qui fait que $\xi_\chi^{l^N} = \xi_\chi w^t$ et $\overline{\Theta}^s_\chi = \prod_{u \in V_\chi} (\xi_\chi^{us} - 1)^{l^N - 1} \equiv \prod_{u \in V_\chi} \dfrac{\xi_\chi^{us} w^{tus} - 1}{\xi_\chi^{us} - 1}$ mod l (en effet, $\xi_\chi^{us} - 1$ est, dans le cas $f_\chi \neq l$, une unité l-adique). On a donc à calculer

$$L(\overline{\Theta}_\chi^{se'_\phi}) \equiv \frac{1}{g_\chi} \sum_{\sigma \in G_\chi} \phi(\sigma^{-1}) L(\overline{\Theta}_\chi^{s\sigma}) \equiv$$

$$\equiv \frac{1}{g_\chi} \sum_{\sigma \in G_\chi} \phi(\sigma^{-1}) L\Big(\prod_{u \in V_\chi} \frac{\xi_\chi^{us\bar\sigma} w^{tus\bar\sigma} - 1}{\xi_\chi^{us\bar\sigma} - 1} \Big)$$

qui est (en utilisant le lemme IV 1, i)) congru à

$$\frac{1}{g_\chi} \sum_{\sigma \in G_\chi} \sum_{u \in V_\chi} \phi(\sigma^{-1}) L\Big(\frac{\xi_\chi^{su\bar\sigma} w^{tus\bar\sigma} - 1}{\xi_\chi^{us\bar\sigma} - 1} \Big) \mod l\,,$$

en désignant par $\bar\sigma$ un prolongement de σ dans Γ_χ. Cette somme peut s'écrire

$$\frac{1}{g_\chi} \sum_{\sigma \in G_\chi} \sum_{u \in V_\chi} \phi(\sigma^{-1} u^{-1}) L\Big(\frac{\xi_\chi^{\bar\sigma us} w^{\bar\sigma ust} - 1}{\xi_\chi^{\bar\sigma us} - 1} \Big) =$$

$$= \frac{1}{g_\chi} \sum_{\sigma \in \Gamma_\chi} \phi(\sigma^{-1}) L\Big(\frac{\xi_\chi^{\sigma s} w^{t\sigma s} - 1}{\xi_\chi^{\sigma s} - 1} \Big) =$$

$$\frac{1}{g_\chi}\sum_{\sigma\in\Gamma_\chi}\sum_{\chi'|\phi}\chi'(\sigma^{-1})\,L\Big(\frac{\xi_\chi^{\sigma s}w^{\sigma st}-1}{\xi_\chi^{\sigma s}-1}\Big)=$$

$$=\frac{1}{g_\chi}\sum_{\chi'|\phi}\sum_{a=1}^{f_\chi}\underline{\chi}'^{-1}(a)\,L\Big(\frac{\xi_\chi^{sa}w^{tsa}-1}{\xi_\chi^{sa}-1}\Big)$$

(avec $\underline{\chi}'\in X(f_\chi)$) ; elle est donc en vertu du lemme IV.1, ii), congrue modulo l à $\frac{1}{g_\chi}\sum_{\chi'|\phi}\sum_{a=1}^{f_\chi}\underline{\chi}'^{-1}(a)\,L\Big(\frac{\xi_\chi^{sa}\,E(tsa\pi)-1}{\xi_\chi^{sa}-1}\Big)$. Posons $sa=b$ (s est premier à f_χ, par conséquent b parcourt tous les résidus modulo f_χ) ; on obtient :

$$\frac{1}{g_\chi}\sum_{\chi'|\phi}\sum_{b=1}^{f_\chi}\underline{\chi}'^{-1}(s^*b)\,L\Big(\frac{\xi_\chi^{b}\,E(tb\pi)-1}{\xi_\chi^{b}-1}\Big)=$$

$$=\frac{1}{g_\chi}\sum_{\chi'|\phi}\underline{\chi}'(s)\sum_{b=1}^{f_\chi}\underline{\chi}'^{-1}(b)\,L\Big(\frac{\xi_\chi^{b}\,E(tb\pi)-1}{\xi_\chi^{b}-1}\Big).$$

Compte tenu du fait que la matrice $(\underline{\chi}'(s))_{\substack{s\in G_\chi\\ \chi'|\phi}}$ est de rang égal au nombre de χ' divisant ϕ (cf. démonstration de la Prop. III.6) il en résulte le critère suivant :

Proposition IV.1. – *Dans le cas $f_\chi\equiv 0$ mod l, $f_\chi\neq l$, une condition nécessaire et suffisante pour que $b_\phi=1$ est que pour tout $\chi'\mid\phi$, un résidu quelconque modulo π^{l-1} de l'expression*

$$\frac{1}{g_\chi}\sum_{a=1}^{f_\chi}\underline{\chi}'^{-1}(a)\,L\Big(\frac{\xi_\chi^{a}\,E(ta\pi)-1}{\xi_\chi^{a}-1}\Big),$$

soit congru à 0 *modulo l.*

Nous allons effectuer ce calcul en établissant d'abord des identités de séries formelles. Nous généralisons en cela le calcul qui se trouve dans [1], chap. V, § 6, pour le cas particulier $f_\chi=l$.

2. Calcul de séries formelles.

Pour plus de commodité nous revenons aux notations du chap. II sur les caractères de Dirichlet et les nombres de Bernoulli.

DEFINITION IV.1. — *On pose* $E(T) = \sum_{i=0}^{l-1} \frac{T^i}{i\,!}$; *on a donc* $E(T) \equiv e^T$ mod T^l (*congruences dans* $\mathbf{Z}_l[[T]]$). *On pose* $L(1 + T) = - \sum_{i=1}^{l-1} \frac{(-T)^i}{i}$; *on a donc* $L(1 + T) \equiv \mathrm{Log}(1 + T)$ mod T^l.

Les séries L et Log sont définies sur l'ensemble des séries formelles congrues à 1 mod T et les séries E et exp sur l'ensemble des séries formelles congrues à 0 mod T.

Nous considérons les séries formelles dans $\Omega_l[[T]]$ et, éventuellement, celles qui sont à coefficients l-entiers.

DEFINITION IV.2. — *Pour* $\underline{\chi}' \in X(m)$, $m \equiv 0$ mod l, $m \neq l$, *posons*

$$\overline{\mathcal{L}}_{\underline{\chi}'}(T) = \frac{1}{g_\chi} \sum_{a=1}^{m} \underline{\chi}'^{-1}(a)\, L\left(\frac{\xi_m^a\, E(taT) - 1}{\xi_m^a - 1}\right) .$$

Remarque IV.2. — Admettons pour l'instant que $\overline{\mathcal{L}}_{\underline{\chi}'}(T)$ soit une série à coefficients l-entiers. Il en résulte que l'expression que l'on désire calculer (Prop. IV.1) est égale (pour $m = f_\chi$) à $\overline{\mathcal{L}}_{\underline{\chi}'}(\pi)$. On peut même ne calculer $\overline{\mathcal{L}}_{\underline{\chi}'}(T)$ que modulo T^{l-1} (Rem. IV.1).

a) *Calcul de la série auxilliaire* $\mathcal{L}_{\underline{\chi}'}(T)$. On commence par calculer la série analogue à $\overline{\mathcal{L}}_{\underline{\chi}'}(T)$ avec Log et exp à la place de L et E et sans aucune hypothèse sur $m > 0$:

DEFINITION IV.3. — *Pour* $\underline{\chi}' \in X(m)$, *on définit la série formelle*

$$\mathcal{L}_{\underline{\chi}'}(T) = \frac{1}{g_\chi} \sum_{a=1}^{m} \underline{\chi}'^{-1}(a)\, \mathrm{Log}\left(\frac{\xi_m^a\, e^{taT} - 1}{\xi_m^a - 1}\right) .$$

On considère la fraction rationnelle $\frac{P(x)}{x^m - 1} \in \Omega_l(x)$, P polynôme non nul de degré strictement inférieur à m. On la décompose en éléments simples : $\frac{P(x)}{x^m - 1} = \sum_{k=1}^{m} \frac{A_k}{x - \xi_m^k}$ ce qui donne

$$A_i = \frac{P(\xi_m^i)}{\prod_{k \neq i} (\xi_m^i - \xi_m^k)} .$$

On a $(x^m - 1)' = mx^{m-1}$ soit $\left(\prod_{k=1}^{m} (x - \xi_m^k)\right)' = \sum_{i=1}^{m} \prod_{k \neq i} (x - \xi_m^k)$

soit $m\xi_m^{-i} = \prod_{k \neq i} (\xi_m^i - \xi_m^k)$, d'où $A_i = \dfrac{\xi_m^i \, P(\xi_m^i)}{m}$; par substitution de e^T à x on obtient l'identité

$$\frac{e^{aT}}{e^{mT} - 1} = \sum_{i=1}^{m} \frac{\xi_m^i \xi_m^{ai}}{m(e^T - \xi_m^i)} = \frac{1}{m} \sum_{i=1}^{m} \frac{\xi_m^{ai}}{\xi_m^{-i} e^T - 1}$$

qui s'écrit $\dfrac{1}{m} \sum_{i=1}^{m} \dfrac{\xi_m^{-ai}}{\xi_m^i e^T - 1}$ (on a ici $P(x) = x^a$), pour $a < m$. Si $a = m$, $\dfrac{e^{mT}}{e^{mT} - 1} = 1 + \dfrac{1}{e^{mT} - 1}$, d'où $\dfrac{e^{mT}}{e^{mT} - 1} = 1 + \dfrac{1}{m} \sum_{i=1}^{m} \dfrac{1}{\xi_m^i e^T - 1}$.

Définissons $\lambda_m^a = 0$ si $a \neq m$, $\lambda_m^m = 1$; on a

$$\frac{e^{aT}}{e^{mT} - 1} = \lambda_m^a + \frac{1}{m} \sum_{i=1}^{m} \frac{\xi_m^{-ai}}{\xi_m^i e^T - 1}, \qquad \text{pour } 1 \leqslant a \leqslant m.$$

Soit $n_m^a(T) = \dfrac{e^{aT}}{e^{mT} - 1} - \dfrac{1}{mT}$; c'est une série formelle entière car le terme $\dfrac{1}{mT}$ s'élimine. On posera

$$N_m^a(T) = \int n_m^a(T) \, dT \qquad \text{pour} \qquad 1 \leqslant a \leqslant m,$$

le signe $\int$ ayant le sens suivant :

Soit $S(T)$ une série formelle $\sum_{i \geqslant 0} s_i T^i$. On posera

$$\int S(T) \, dT = \sum_{i \geqslant 0} \frac{s_i}{i + 1} T^{i+1}$$

(primitive sans terme constant de la série).

Par définition des nombres de Bernoulli généralisés, on a

$$\sum_{a=1}^{m} \underline{\chi}'(a) \, n_m^a(T) = \sum_{a=1}^{m} \underline{\chi}'(a) \frac{e^{aT}}{e^{mT} - 1} - \frac{1}{m} \sum_{a=1}^{m} \underline{\chi}'(a) \frac{1}{T} =$$

$$= \sum_{n \geq 0} B_n(\underline{\chi}') \frac{T^{n-1}}{n!} - \frac{1}{mT} \sum_{a=1}^{m} \underline{\chi}'(a) .$$

Si $\underline{\chi}' \neq 1_m$, $\sum_{a=1}^{m} \underline{\chi}'(a) = 0$ mais $B_0(\underline{\chi}') = 0$ et le terme en $\frac{1}{T}$ s'élimine.

Si $\underline{\chi}' = 1_m$ alors $\sum_{a=1}^{m} \underline{\chi}'(a) = \varphi(m)$ mais $B_0(1_m) = \frac{\varphi(m)}{m}$ et le terme en $\frac{1}{T}$ s'élimine encore. On a $\sum_{a=1}^{m} \underline{\chi}'(a)\, n_m^a(T) = \sum_{n \geq 1} B_n(\underline{\chi}') \frac{T^{n-1}}{n!}$, pour tout $\underline{\chi}' \in X(m)$, cette relation ayant lieu identiquement pour tout élément de $M(\underline{\chi}')$. Appliquons la pour les caractères $\underline{\psi}' \in X(m)$: Pour b premier à m multiplions la relation précédente par $\underline{\psi}'^{-1}(b)$, $\underline{\psi}' \in X(m)$ et sommons sur $\underline{\psi}'$:

$$\sum_{\underline{\psi}' \in X(m)} \underline{\psi}'^{-1}(b) \sum_{a=1}^{m} \underline{\psi}'(a)\, n_m^a(T) = \sum_{\underline{\psi}'} \sum_{n \geq 1} B_n(\underline{\psi}') \frac{T^{n-1}}{n!} \underline{\psi}'^{-1}(b) =$$

$$= \sum_{a=1}^{m} n_m^a(T) \sum_{\underline{\psi}' \in X(m)} \underline{\psi}'(b^* a)$$

(où b^* désigne l'inverse de b mod m) ; on pose $[b^* a]_m = c$ (où $[\ ]_m$ est la fonction résidu mod m) ; on obtient :

$$\sum_{c=1}^{m} n_m^{[bc]_m}(T) \sum_{\underline{\psi}' \in X(m)} \underline{\psi}'(c)$$

or $\sum_{\underline{\psi}' \in X(m)} \underline{\psi}'(c) = 0$ (resp. $\varphi(m)$) si $c \neq 1$ (resp. $c = 1$), d'où, il reste $\varphi(m)\, n_m^b(T)$, ce qui donne par l'opération $\int$:

$$N_m^b(T) = \frac{1}{\varphi(m)} \sum_{\underline{\psi}' \in X(m)} \underline{\psi}'^{-1}(b) \sum_{n \geq 1} B_n(\underline{\psi}') \frac{T^n}{n\, n!},$$

pour tout b, $1 \leqslant b \leqslant m$, et $(b, m) = 1$.

On a pour tout a : $N_m^a(T) = \int \left(\frac{e^{aT}}{e^{mT} - 1} - \frac{1}{mT} \right) dT$; posons $a = dx, m = d\delta, (x, \delta) = 1 \cdot N_{d\delta}^{dx}(T) = \int \left(\frac{e^{dxT}}{e^{d\delta T} - 1} - \frac{1}{d\delta T} \right) dT$, en faisant le changement de variable $X = dT$, on obtient

$$\int \left(\frac{e^{xX}}{e^{\delta X}-1} - \frac{1}{\delta X}\right)\frac{dX}{d} = \frac{1}{d}\,N_\delta^x(X)\,,$$

d'où $N_m^a = N_{d\delta}^{dx}(T) = \dfrac{1}{d}\,N_\delta^x(dT)$, où $(a\,,m) = d$, $1 \leqslant a \leqslant m$. On a

$$n_m^a(T) = \frac{e^{aT}}{e^{mT}-1} - \frac{1}{mT} = \frac{1}{m}\left(m\lambda_m^a + \sum_{i=1}^{m} \frac{\xi_m^{-ai}}{\xi_m^i\,e^T - 1} - \frac{1}{T}\right).$$

Posons $L_k^m(T) = \mathrm{Log}\left(\dfrac{\xi_m^k\,e^T - 1}{\xi_m^k - 1}\right)$ pour $1 \leqslant k < m$ (en fait k est défini mod m) et $L_m^m(T) = \mathrm{Log}\left(\dfrac{e^T-1}{T}\right)$; ce sont des séries formelles en T. Le terme constant de $\dfrac{1}{m}\sum\limits_{k=1}^{m} \xi_m^{-ak}\,L_k^m(T)$ est nul car $L_k^m(T) \equiv 0$ mod (T) pour tout k. Dérivons cette série ; on obtient :

$$\frac{1}{m}\sum_{k=1}^{m-1} \xi_m^{-ak}\,\frac{\xi_m^k\,e^T}{\xi_m^k\,e^T-1} + \frac{1}{m}\left(\frac{e^T}{e^T-1} - \frac{1}{T}\right) =$$

$$= \frac{1}{m}\sum_{k=1}^{m} \xi_m^{-ak}\,\frac{\xi_m^k\,e^T}{\xi_m^k\,e^T-1} - \frac{1}{mT}$$

mais

$$\frac{\xi_m^k\,e^T}{\xi_m^k\,e^T-1} = 1 + \frac{1}{\xi_m^k\,e^T-1}$$

d'où

$$\frac{1}{m}\left(\sum_{k=1}^{m} \xi_m^{-ak}\left(1 + \frac{1}{\xi_m^k\,e^T-1}\right) - \frac{1}{T}\right) = \frac{1}{m}\left(\sum_{k=1}^{m} \frac{\xi_m^{-ak}}{\xi_m^k\,e^T-1} - \frac{1}{T} + \sum_{k=1}^{m} \xi_m^{-ak}\right);$$

or $\dfrac{1}{m}\sum\limits_{k=1}^{m} \xi_m^{-ak} = \lambda_m^a$; on retrouve ainsi l'expression de $n_m^a(T)$, d'où

$N_m^a(T) = \dfrac{1}{m}\sum\limits_{k=1}^{m} \xi_m^{-ak}\,L_k^m(T)$ pour tout a, $1 \leqslant a \leqslant m$. On multiplie cette identité par ξ_m^{ra}, $1 \leqslant r \leqslant m$, et on somme sur a :

$$\sum_{a=1}^{m} \xi_m^{ra} \mathrm{N}_m^a(\mathrm{T}) = \frac{1}{m}\sum_{a=1}^{m}\ \sum_{k=1}^{m} \xi_m^{(r-k)a}\, \mathrm{L}_k^m(\mathrm{T}) =$$

$$= \frac{1}{m}\sum_{k=1}^{m} \mathrm{L}_k^m(\mathrm{T}) \sum_{a=1}^{m} \xi_m^{(r-k)a} = \mathrm{L}_r^m(\mathrm{T}) \sum_{a=1}^{m} \xi_m^{ra}\, \mathrm{N}_m^a(\mathrm{T});$$

comme N_m^a n'est calculable qu'en fonction des N_σ^x, on remplace la sommation $\sum\limits_{a=1}^{m}$ par la suivante : On pose $a = dx$, $d = (a, m)$; si $m = d\delta$, alors $(x, \delta) = 1$ et $1 \leqslant x \leqslant \delta$; cette décomposition est unique et lorsque d parcourt l'ensemble des diviseurs de m et, pour chaque d, x parcourt $\{x, (x, \delta) = 1,\ 1 \leqslant x \leqslant \delta\}$ alors on retrouve tout élément a, $1 \leqslant a \leqslant m$ une fois et une seule ; on a :

$$\mathrm{L}_r^m(\mathrm{T}) = \sum_{d\mid m} \frac{1}{d} \sideset{}{^*}\sum_{x=1}^{\delta} \xi_m^{rdx}\, \mathrm{N}_\delta^x(d\mathrm{T})$$

pour tout r, $1 \leqslant r \leqslant m$.

On aura alors $\mathscr{L}_{\underline{\chi}'}(\mathrm{T}) = \dfrac{1}{g_\chi}\sum\limits_{a=1}^{m} \underline{\chi}'^{-1}(a)\ \mathrm{L}_a^m(ta\mathrm{T})$, pour $\underline{\chi}' \in \mathrm{X}(m)$

$$\mathscr{L}_{\underline{\chi}'}(\mathrm{T}) = \frac{1}{g_\chi}\sum_{a=1}^{m} \underline{\chi}'^{-1}(a) \sum_{d\mid m}\ \sideset{}{^*}\sum_{x=1}^{\delta} \frac{1}{d}\ \xi_m^{adx}\, \mathrm{N}_\delta^x(dta\mathrm{T}) \text{ ; en utilisant}$$

$$\mathrm{N}_\delta^x(\mathrm{T}) = \frac{1}{\varphi(\delta)} \sum_{\underline{\psi}' \in \mathrm{X}(\delta)} \underline{\psi}'^{-1}(x) \sum_{n \geqslant 1} \mathrm{B}_n(\underline{\psi}') \frac{\mathrm{T}^n}{n\,n!},$$

on aura

$$\mathscr{L}_{\underline{\chi}'}(\mathrm{T}) = \frac{1}{g_\chi}\sum_{a=1}^{m} \underline{\chi}'^{-1}(a) \sum_{d\mid m}\ \sum_{x=1}^{\delta}\ \sum_{\underline{\psi}' \in \mathrm{X}(\delta)}\ \sum_{n \geqslant 1}$$

$$\frac{1}{d}\, \xi_m^{adx} \frac{\underline{\psi}'^{-1}(x)}{\varphi(\delta)} \mathrm{B}_n(\underline{\psi}') \frac{(dta\mathrm{T})^n}{n\,n!}$$

on introduit les sommes de Gauss (chap. II, § 4), $\mathscr{T}(\underline{\psi}') = \sum\limits_{x=1}^{\delta} \underline{\psi}'(x)\, \xi_\delta^x$, pour $\psi' \in \mathrm{X}(\delta)$ et $\xi_\delta = \exp(2i\pi/\delta)$; on a alors

$$\sum_{x=1}^{\delta} \underline{\psi}'^{-1}(x)\, \xi_m^{adx} = \sum_{x=1}^{\delta} \underline{\psi}'^{-1}(x)\, \xi_\delta^{ax}.$$

Si $(a, \delta) = 1$, alors en posant $ax = y$, si x parcourt $\{1, \ldots, \delta\}$ alors $[ax]_\delta$ parcourt le même ensemble, et comme $\underline{\psi}'(y) = \underline{\psi}'(y')$ si $y - y' \equiv 0 \bmod \delta$ alors on aura $\sum_{y=1}^{\delta} \underline{\psi}'^{-1}(y a^*)\, \xi_\delta^y$, a^* inverse de $a \bmod \delta$, soit $\sum_{y=1}^{\delta} \underline{\psi}'^{-1}(a^*)\, \underline{\psi}'^{-1}(y)\, \xi_\delta^y = \underline{\psi}'(a)\mathscr{C}(\underline{\psi}'^{-1})$. Supposons maintenant $(a, \delta) \neq 1$, alors c'est que $(a, m) \neq 1$, mais pour un tel a, $\underline{\chi}'^{-1}(a) = 0$. On peut donc toujours supposer que $(a, m) = 1$, auquel cas on est ramené au cas précédent. On a alors :

$$\mathscr{L}_{\underline{\chi}'}(\mathrm{T}) = \frac{1}{g_\chi} \sum_{a=1}^{m} \sum_{d \mid m} \sum_{\underline{\psi}' \in \mathrm{X}(\delta)} \sum_{n \geqslant 1} \underline{\chi}'^{-1}(a)\, \frac{\underline{\psi}'(a)}{\varphi(\delta)} \mathscr{C}(\underline{\psi}'^{-1})\, \mathrm{B}_n(\underline{\psi}')\, \frac{a^n d^{n-1} t^n \mathrm{T}^n}{n\, n!}$$

La sommation $\sum_{a=1}^{m} \underline{\chi}'^{-1}(a)\, \underline{\psi}'(a)\, a^n$ s'écrit $\sum_{a=1}^{m} (\underline{\chi}'^{-1} \underline{\psi}')(a)\, a^n$, le caractère $\underline{\chi}'^{-1} \underline{\psi}'$ est un élément de $\mathrm{X}(m)$ car $\underline{\chi}'^{-1} \in \mathrm{X}(m)$ et $\underline{\psi}' \in \mathrm{X}(\delta)$, $\delta \mid m$. Cette somme sera notée $\mathrm{S}^n_{\underline{\chi}'^{-1}\underline{\psi}'}(m)$. On a donc obtenu :

LEMME IV.2. – *On a l'égalité de séries formelles :*

$$\mathscr{L}_{\chi'}(\mathrm{T}) = \frac{1}{g_\chi} \sum_{d \mid m} \sum_{\underline{\psi}' \in \mathrm{X}(\delta)} \sum_{n \geqslant 1} \mathrm{S}^n_{\underline{\chi}'^{-1}\underline{\psi}'}(m)\, \mathrm{B}_n(\underline{\psi}')\, \mathscr{C}(\underline{\psi}'^{-1}) \frac{d^{n-1}}{\varphi(\delta)} \frac{t^n \mathrm{T}^n}{n\, n!}$$

pour tout $m \in \mathrm{N}^*$ et tout $\underline{x}' \in \mathrm{X}(m)$.

b) *Etude du reste modulo* T^ℓ *de la série* $\overline{\mathscr{L}}_{\underline{\chi}'}(\mathrm{T})$. On rappelle (Déf. III.2) qu'on a posé

$$\overline{\mathscr{L}}_{\underline{\chi}'}(\mathrm{T}) = \frac{1}{g_\chi} \sum_{a=1}^{m} \underline{\chi}'^{-1}(a)\, \mathrm{L}\left(\frac{\xi_m^a\, \mathrm{E}(ta\mathrm{T}) - 1}{\xi_m^a - 1}\right)$$

et que (Rem. IV. 2) on désire calculer $\overline{\mathscr{L}}_{\underline{\chi}'}(\mathrm{T})$ modulo T^ℓ. La série $\mathrm{E}(at\mathrm{T})$ est à coefficients ℓ-entiers ; de même $\mathrm{L}(\mathrm{X})$ est à coefficients l-entiers. La série $\dfrac{\xi_m^a\, \mathrm{E}(at\mathrm{T}) - 1}{\xi_m^a - 1}$ est de la forme $1 + \mathrm{S}(\mathrm{T})$ avec $\mathrm{S}(\mathrm{T})$ à coefficients ℓ-entiers, lorsque m est de la forme $\ell\, \mathrm{m}'$, m'

distinct d'une puissance de ℓ, car dans ce cas $\xi_m^a - 1$ est une unité ([19], § 8). D'où comme ℓ ne divise pas $g_\chi, \bar{\mathcal{L}}_{\underline{\chi}'}$ (T) est à coefficients ℓ-entiers. Considérons maintenant les séries $\bar{\mathcal{L}}_{\underline{\chi}'}(T)$ et $\mathcal{L}_{\underline{\chi}'}(T)$ modulo T^ℓ. On a

$$\mathcal{L}_{\underline{\chi}'}(T) = \frac{1}{g_\chi} \sum_{a=1}^{m} \underline{\chi}'^{-1}(a) \operatorname{Log}\left(\frac{\xi_m^a e^{atT} - 1}{\xi_m^a - 1}\right)$$

et $e^{atT} \equiv E(atT) \bmod T^\ell$ dans $\Omega_\ell[[T]]$. On a

$$\frac{\xi_m^a e^{atT} - 1}{\xi_m^a - 1} \equiv \frac{\xi_m^a E(atT) - 1}{\xi_m^a - 1}$$

mod T^ℓ. Soient U et V deux séries en T telles que $U \equiv V \equiv 1$ mod T et telles que $V \equiv U \bmod T^\ell$. Alors $L(U) \equiv \operatorname{Log}(V) \bmod T^\ell$; en effet : on peut écrire $V = U(1 + ST^\ell)$ dans $\Omega_\ell[[T]]$, soit $\operatorname{Log} V = \operatorname{Log} U + \operatorname{Log}(1 + ST^\ell)$; donc ici $\operatorname{Log}(1 + ST^\ell) \equiv 0 \bmod T^\ell$. On obtient donc finalement

$$\operatorname{Log}(U) \equiv \operatorname{Log}(V) \bmod T^\ell \qquad \text{mais} \qquad \operatorname{Log}(U) \equiv L(U) \bmod T^\ell ;$$

on a donc $\operatorname{Log}\left(\frac{\xi_m^a e^{atT} - 1}{\xi_m^a - 1}\right) \equiv L\left(\frac{\xi_m^a E(atT) - 1}{\xi_m^a - 1}\right) \bmod T^\ell$, soit

$$\tilde{\mathcal{L}}_{\underline{\chi}'}(T) \equiv \mathcal{L}_{\underline{\chi}'}(T) \bmod T^\ell \qquad \text{et} \qquad \bar{\mathcal{L}}_{\underline{\chi}'}(T)$$

est à coefficients ℓ-entiers. Ecrivons

$$\mathcal{L}_{\underline{\chi}'}(T) = \sum_{i=0}^{\ell-1} a_i T^i + T^\ell S(T), \; S(T) \in \Omega_\ell[[T]] ;$$

alors $\overline{\mathcal{L}_{\underline{\chi}'}}(T) \equiv \mathcal{L}_{\underline{\chi}'}(T) \bmod T^\ell$ entraîne $\overline{\mathcal{L}_{\underline{\chi}'}}(T) = \sum_{i=0}^{\ell-1} a_i T^i + T^\ell \bar{S}(T)$, $\bar{S}(T) \in \Omega_\ell[[T]]$; comme $\overline{\mathcal{L}_{\underline{\chi}'}}(T)$ est à coefficient ℓ-entiers, les a_i, pour $i = 0, \ldots, \ell - 1$ sont ℓ-entiers ; ce sont les ℓ premiers coefficients de la série $\mathcal{L}_{\underline{\chi}'}(T)$ à savoir (Lemme IV.2) :

$$\frac{1}{g_\chi} \sum_{d \mid m} \sum_{\underline{\psi}' \in X(\delta)} \sum_{n=1}^{\ell-1} S^n_{\underline{\chi}'^{-1}\underline{\psi}'}(m)\, B_n(\underline{\psi}')\, \mathcal{C}(\underline{\psi}'^{-1}) \frac{d^{n-1}}{\varphi(\delta)} \frac{t^n T^n}{n\, n!}$$

et on a :

LEMME IV. 3. — *On a dans le sous-anneau des séries formelles à coefficients ℓ-entiers la congruence :*

$$\overline{\mathcal{L}}_{\chi'}(\mathrm{T}) \equiv \frac{1}{g_\chi} \sum_{d \mid m} \sum_{\underline{\psi}' \in \mathrm{X}(\delta)} \sum_{n=1}^{\ell-1} \mathrm{S}^n_{\underline{\chi}'^{-1}\underline{\psi}'}(m)\, \mathrm{B}_n(\underline{\psi}')\, \mathscr{C}(\underline{\psi}'^{-1}) \frac{d^{n-1}}{\varphi(\delta)} \frac{t^n\, \mathrm{T}^n}{n\, n!} \bmod \mathrm{T}^\ell .$$

c) *Applications du calcul de séries formelles.* En vertu de la Prop. IV.1 et de la Rem. IV.2 on a obtenu :

PROPOSITION IV.2. — *Une condition nécessaire et suffisante pour que $b_\phi = 1$, dans le cas $f_\chi \equiv 0 \bmod \ell$, $f_\chi \neq \ell$, est que :*

$$\sum_{d \mid f_\chi} \sum_{\underline{\psi}' \in \mathrm{X}(\delta)} \sum_{n=1}^{\ell-2} \mathrm{S}^n_{\underline{\chi}'^{-1}\underline{\psi}'}(f_\chi)\, \mathrm{B}_n(\underline{\psi}')\, \mathscr{C}(\underline{\psi}'^{-1}) \frac{d^{n-1}}{\varphi(\delta)} \frac{n^n}{n\, n!}\, t^n \equiv 0 \bmod \ell,$$

pour tout $\chi' \mid \phi$.

Remarque IV. 3. — Nous avons limité la sommation sur n à l'intervalle $1 \leqslant n \leqslant \ell - 2$, compte tenu de la Rem. IV.1 et du fait que le coefficient de $\pi^{\ell-1}$ est ℓ-entier.

3. Fin des calculs.

a) *Etude du coefficient de π^n.*

DEFINITION IV.4. — *On pose*

$$\Lambda_n = \sum_{d \mid f_\chi} \sum_{\underline{\psi}' \in \mathrm{X}(\delta)} \mathrm{S}^n_{\underline{\chi}'^{-1}\underline{\psi}'}(f_\chi)\, \mathrm{B}_n(\underline{\psi}')\, \mathscr{C}(\underline{\psi}'^{-1}) \frac{d^{n-1}}{\varphi(\delta)} ;$$

Λ_n est le coefficient de $\dfrac{\pi^n\, t^n}{n\, n!}$ pour $1 \leqslant n \leqslant \ell - 2$ (*mais n'est pas à priori un élément de* $\mathbf{Z}_\ell^{(f_\chi)}$). *On peut donc calculer* $\Lambda_n \bmod \pi^{\ell-1-n}$.

On sait que $\mathrm{B}_n(\underline{\psi}')$ est de la forme $\dfrac{1}{\delta} \displaystyle\sum_{c=1}^{\delta} \mathrm{D}_n(c)\, \underline{\psi}'(c)$ où $\mathrm{D}_n(c)$ est défini par le développement symbolique $\mathrm{D}_n(c) = (c - \delta + \delta\, \mathrm{B})^n$, où $B^i, i \geqslant 0$, est remplacé par $B_i = B_i(1_1)$, nombre de Bernoulli ordinaire (chap. II, § 2) ; comme $i \leqslant n \leqslant \ell - 2$, les B_i sont ℓ-entiers (théorème de von Staudt), donc $D_n(c)$ est aussi ℓ-entier). On aura

$$\Lambda_n = \sum_{d \mid f_\chi} \sum_{a=1}^{f_\chi} \sum_{b=1}^{\delta} \sum_{c=1}^{\delta} \underline{\chi}'^{-1}(a)\, a^n\, \xi_\delta^b\, D_n(c)\, \frac{d^{n-1}}{\delta\varphi(\delta)} \sum_{\underline{\psi}' \in X(\delta)} \underline{\psi}'(ab^* c),$$

où b^* est inverse de b mod δ lorsque $(b, \delta) = 1$ (sinon $b^* = 0$ par exemple). On a $\sum_{\underline{\psi}' \in X(\delta)} \underline{\psi}'(ab^* c) = 0$ sauf si $ab^* c \equiv 1 \bmod \delta$ auquel cas la somme vaut $\varphi(\delta)$. La sommation sur b peut donc être limitée au seul terme $b \equiv ac \bmod \delta$ pour chaque couple (a, c) fixé, $(a, \delta) = 1$, $(c, \delta) = 1$; on peut en fait faire $b = ac$ avec a quelconque et $(c, \delta) = 1$ car pour $(a, \delta) \neq 1$, on a $\underline{\chi}'^{-1}(a) = 0$ et enfin ξ_δ^b ne dépend que de b modulo δ, d'où

$$\Lambda_n = \sum_{d \mid f_\chi} \frac{d^{n-1}}{\delta} \sum_{a=1}^{f_\chi} \sideset{}{^*}\sum_{c=1}^{\delta} \underline{\chi}'^{-1}(a)\, a^n\, D_n(c)\, \xi_\delta^{ac}.$$

On a $D_n(c) \equiv (c-\delta)^n B_0 + n(c-\delta)^{n-1}\delta B_1 \bmod \delta^2$, soit puisque $B_0 = 1$ et $B_1 = \frac{1}{2}$, $D_n(c) \equiv c^n - \frac{n}{2}\delta c^{n-1} \bmod \delta^2$; de plus $D_1(c) = c - \frac{1}{2}\delta$; il en résulte que dans le calcul de Λ_n mod ℓ, on peut, lorsque $\delta \not\equiv 0 \bmod \ell$, remplacer $D_n(c)$ par $c^n - \frac{n}{2}\delta c^{n-1}$ pour tout n $\left(\text{en effet, pour } n \geqslant 2 \text{ ceci ne change rien car } d^{n-1} \equiv 0 \bmod \ell \text{ et pour } n = 1,\ D_1(c) = c - \frac{1}{2}\delta\right)$ et lorsque $\delta \equiv 0 \bmod \ell$, il suffit alors de faire le calcul modulo δ^2 :

$$\Lambda_n \equiv \sum_{d \mid f_\chi} \frac{d^{n-1}}{\delta} \sum_{a=1}^{f_\chi} \sideset{}{^*}\sum_{c=1}^{\delta} \underline{\chi}'^{-1}(a)\, a^n \left(c^n - \frac{n}{2}\delta c^{n-1}\right) \xi_\delta^{ac} \bmod l.$$

On est amené à poser la définition suivante :

DEFINITION IV. 5. – *On pose* $\Lambda_n^d = \frac{d^{n-1}}{\delta} \sum_{a=1}^{f_\chi} \sideset{}{^*}\sum_{c=1}^{\delta} \underline{\chi}'^{-1}(a)\, a^n c^n \xi_\delta^{ac}$

et $\Lambda'^{d}_{n} = \dfrac{n d^{n-1}}{2} \sum_{a=1}^{f_\chi} \sum_{c=1}^{\delta}{}^{*} \underline{\chi}'^{-1}(a)\, a^n\, c^{n-1}\, \xi_\delta^{ac}$. *On a donc*

$$\Lambda_n = \sum_{d \mid f_\chi}' (\Lambda^d_n - \Lambda'^d_n).$$

b) *Etude du terme* Λ'^d_n *modulo* ℓ. On a :

$$\sum_{c=1}^{\delta}{}^{*} c^{n-1} \sum_{a=1}^{f_\chi}{}' \underline{\chi}'^{-1}(a)\, a^n\, \xi_\delta^{ac} \equiv \sum_{c=1}^{\delta}{}^{*} c^{n-1} \sum_{a=1}^{f_\chi} \underline{\chi}'^{-1}(a)\, \theta^n(a)\, \xi_\delta^{ac} \equiv$$

$$\equiv \sum_{c=1}^{\delta}{}^{*} c^{n-1} \sum_{a=1}^{f_\chi}{}^{*} \underline{\chi}'^{-1}(a)\, \underline{\theta}^n(a)\, \xi_\delta^{ac_0}$$

(où c_0 est premier à f_χ et $c_0 \equiv c \bmod \delta$)

$$\equiv \sum_{c=1}^{\delta}{}^{*} c^{n-1}\, \underline{\chi}'(c_0)\, \underline{\theta}^{-n}(c_0) \sum_{a=1}^{f_\chi}{}^{*} \underline{\chi}'^{-1}\, \underline{\theta}^n(a)\, \xi_\delta^a \bmod \ell\ ;$$

posons $H = \mathrm{Gal}(Q^{(f_\chi)}/Q^{(\delta)})$, on a

$$\sum_{\sigma \in \Gamma_\chi} \chi'^{-1}(\sigma)\, \theta^n(\sigma)\, \xi_\delta^\sigma = \sum_{\tau \in H} \chi'^{-1}\, \theta^n(\tau) \sum_{\sigma_i} \chi'^{-1}\, \theta^n(\sigma_i)\, \xi_\delta^{\sigma_i}$$

($\sigma_i \in \Gamma_\chi$ représentant Γ_χ/H) ; la somme $\sum_{\tau \in H} \chi'^{-1}\, \theta^n(\tau)$ est nulle sauf si $\chi'^{-1}\,\theta^n$ est trivial sur H. Si $\delta \equiv 0 \bmod \ell$ cette somme est, pour $H \neq (1)$, nulle (car alors pour $\tau \in H$, $\theta(\tau) = 1$ et χ' étant de conducteur f_χ n'est pas trivial sur $H \neq (1)$). Si $\delta \not\equiv 0 \bmod \ell$, la seule valeur à étudier est $n = 1$, car $d^{n-1} \equiv 0 \bmod \ell$ pour $n > 1$; pour $n = 1$, $\chi'^{-1}\,\theta$ est trivial sur H si déjà $\chi'^{-1}\,\theta$ est trivial sur $\mathrm{Gal}(Q^{(f_\chi)}/Q^{(f'_\chi)})$ et il est nécessaire que dans la décomposition canonique de χ',

$$\chi' = \varphi'\, \theta^\lambda,$$

on ait $\lambda = 1$ auquel cas, on a $\chi'^{-1}\,\theta = \varphi'^{-1}$; la seule possibilité étant alors $\delta = f'_\chi$ (Rem. II .1). On est donc ramené aux deux cas $\delta = f_\chi$ et $\delta = f'_\chi$ avec $n = \lambda = 1$:

α) $\delta = f_\chi$, n quelconque. Le terme calculé devient

$$\sum_{c=1}^{f_\chi}{}^{*} c^{n-1} \underline{\chi}'(c)\, \underline{\theta}^{-n}(c) \sum_{a=1}^{f_\chi}{}^{*} \underline{\chi}'^{-1} \underline{\theta}^{n}(a)\, \xi_{f_\chi}^{a} \equiv$$

$$\equiv \sum_{c=1}^{f_\chi}{}^{*} \underline{\chi}'\, \underline{\theta}^{-1}(c) \mathcal{G}(\underline{\chi}'^{-1} \underline{\theta}^{n}) \bmod \ell \ ;$$

or $\sum_{c=1}^{f_\chi}{}^{*} \underline{\chi}'\, \underline{\theta}^{-1}(c) \equiv 0 \bmod \ell$, car $\chi' \neq \theta$.

β) $\delta = f'_\chi$, $n = 1$, $\lambda = 1$. Le terme calculé est alors

$$\sum_{c=1}^{f'_\chi}{}^{*} \underline{\chi}'(c_0)\, \underline{\theta}^{-1}(c_0) \sum_{a=1}^{f_\chi}{}^{*} \underline{\chi}'^{-1} \underline{\theta}(a)\, \xi_{f'_\chi}^{a} \ ;$$

or le coefficient $\sum_{c=1}^{f'_\chi}{}^{*} \underline{\chi}'(c_0)\, \underline{\theta}^{-1}(c_0)$ est égal à

$$\sum_{c=1}^{f'_\chi}{}^{*} \underline{\varphi}'(c_0) = \sum_{c=1}^{f'_\chi}{}^{*} \underline{\varphi}'(c) = 0,$$

car $\varphi' \neq 1$:

LEMME IV. 4. – *On a* $\Lambda'^{d}_{n} \equiv 0 \bmod \ell$, *pour tout* $d \mid f_\chi$ *et tout* n, $1 \leqslant n \leqslant \ell - 2$.

c) *Etude du terme* Λ^{d}_{n}. On a $\Lambda^{d}_{n} = \dfrac{d^{n-1}}{\delta} \sum_{c=1}^{\delta}{}^{*} c^{n} \sum_{a=1}^{f_\chi} \underline{\chi}'^{-1}(a)\, a^{n}\, \xi_{\delta}^{ac}$;

on peut se restreindre aux deux cas suivants : $\delta \not\equiv 0 \bmod \ell$ et $n = 1$ puis $\delta \equiv 0 \bmod \ell$, n quelconque.

α) $\delta \not\equiv 0 \bmod \ell$ et $n = 1$. On aura alors

$$\Lambda_{1}^{d} = \frac{1}{\delta} \sum_{c=1}^{\delta}{}^{*} c \sum_{a=1}^{f_\chi} \underline{\chi}'^{-1}(a)\, a\, \xi_{\delta}^{ac} \equiv$$

$$\equiv \frac{1}{\delta} \sum_{c=1}^{\delta}{}^{*} c\, \underline{\chi}'(c_0)\, \underline{\theta}^{-1}(c_0) \sum_{a=1}^{f_\chi} \underline{\chi}'^{-1} \underline{\theta}\ (a)\ \xi_{\delta}^{a} \ \bmod \ell,$$

et, d'après ce que l'on a vu en b), $\sum_{a=1}^{f_\chi} \underline{\chi}'^{-1}\, \underline{\theta}\,(a)\, \xi_\delta^a = 0$ sauf dans le cas β) ($\delta = f'_\chi$, $\lambda = 1$), auquel cas on aura

$$\Lambda_1^\ell = \frac{1}{f'_\chi} \sum_{c=1}^{\delta}{}^{*} c\, \underline{\chi}'\,(c_0)\, \underline{\theta}^{-1}\,(c_0)\,(\ell - 1) \sum_{b=1}^{f'_\chi}{}^{*} \underline{\varphi}'^{-1}\,(b)\, \xi_{f'_\chi}^b \equiv$$

$$\equiv - \frac{\mathcal{G}\,(\varphi'^{-1})}{f'_\chi} \sum_{c=1}^{f'_\chi}{}^{*} c\, \underline{\varphi}'\,(c_0) \equiv - \frac{1}{f'_\chi} \mathcal{G}(\varphi'^{-1}) \sum_{c=1}^{f'_\chi} c\underline{\varphi}'\,(c) \bmod \ell.$$

On reconnaît que $\frac{1}{f'_\chi} \sum_{c=1}^{f'_\chi} c\, \underline{\varphi}'\,(c) = \mathrm{B}_1\,(\varphi')$, car $\underline{\varphi}' \neq 1_{f'_\chi}$ dans $\mathrm{X}\,(f'_\chi)$ et $\underline{\varphi}'$ est primitif, d'ou $\Lambda_1^\ell \equiv - \mathcal{G}\,(\varphi'^{-1})\, \mathrm{B}_1\,(\varphi') \bmod \ell$.

β) $\delta \equiv 0 \bmod \ell$, n quelconque. On étudie mod ℓ l'expression

$\Lambda_n^d = \frac{d^{n-1}}{\delta} \sum_{a=1}^{f_\chi} \sum_{c=1}^{\delta}{}^{*} \underline{\chi}'^{-1}\,(a)\, a^n\, c^n\, \xi_\delta^{ac}$; on peut poser

$$a = \theta\,(a)\,(1 + \gamma_a\,\ell) \qquad \text{et} \qquad c = \theta\,(c)\,(1 + \gamma_c\,\ell),\ \gamma_a, \gamma_c \in \mathbf{Z}_\ell,$$

pour $(a\,,\,\ell) = (c\,,\,\ell) = 1$. D'où

$$\Lambda_n^d \equiv \frac{d^{n-1}}{\delta} \sum_{a=1}^{f_\chi}{}^{*} \sum_{c=1}^{\delta}{}^{*} \underline{\chi}'^{-1}\,(a)\, \underline{\theta}^n\,(ac)\,(1 + n\,\gamma_a\,\ell + n\,\gamma_c\,\ell)\, \xi_\delta^{ac} \equiv$$

$$\equiv \frac{d^{n-1}}{\delta} \sum_{a=1}^{f_\chi}{}^{*} \sum_{c=1}^{\delta}{}^{*} \underline{\chi}'^{-1}\,(a)\, \underline{\theta}^n\,(ac)\, \xi_\delta^{ac} +$$

$$+ \frac{n\,\ell\, d^{n-1}}{\delta} \sum_{a=1}^{f_\chi}{}^{*} \sum_{c=1}^{\delta}{}^{*} \underline{\chi}'^{-1}\,(a)\, \underline{\theta}^n\,(ac)\, \gamma_c\, \xi_\delta^{ac} +$$

$$+ \frac{n\,\ell\, d^{n-1}}{\delta} \sum_{a=1}^{f_\chi}{}^{*} \sum_{c=1}^{\delta}{}^{*} \underline{\chi}'^{-1}(a)\, \underline{\theta}^n\,(ac)\, \gamma_a\, \xi_\delta^{ac}.$$

i) Calcul de $\frac{d^{n-1}}{\delta} \sum_{a=1}^{f_\chi}{}^{*} \sum_{c=1}^{\delta}{}^{*} \underline{\chi}'^{-1}\,(a)\, \underline{\theta}^n\,(ac)\, \xi_\delta^{ac}$. La somme

$$\sum_{a=1}^{f_\chi}{}^{*} \underline{\chi}'^{-1}(a)\, \underline{\theta}^n(a)\, \xi_\delta^{ac}$$

est nulle sauf si $\delta = f_\chi$ (cf. *b*) cas α) d'où, pour $\delta = f_\chi$, on obtient $\frac{1}{f_\chi} \sum_{c=1}^{f_\chi}{}^{*} \underline{\theta}^n(c)\, \underline{\chi}'(c)\, \underline{\theta}^{-n}(c)\, \mathscr{G}(\underline{\chi}'^{-1}\underline{\theta}^n) = \frac{1}{f_\chi}\sum_{c=1}^{f_\chi}{}^{*} \underline{\chi}'(c)\, \mathscr{G}(\underline{\chi}'^{-1}\underline{\theta}^n) = 0.$

ii) Calcul de $\frac{n\,\ell\, d^{n-1}}{\delta} \sum_{a=1}^{f_\chi}{}^{*} \sum_{c=1}^{\delta}{}^{*} \underline{\chi}'^{-1}(a)\, \underline{\theta}^n(ac)\, \gamma_c\, \xi_\delta^{ac}$. Il suffit de calculer la double sommation modulo ℓ : on a

$$\sum_{a=1}^{f_\chi}{}^{*} \sum_{c=1}^{\delta}{}^{*} \underline{\chi}'^{-1}(a)\, \underline{\theta}^n(ac)\, \gamma_c\, \xi_\delta^{ac} = \sum_{c=1}^{\delta}{}^{*} \underline{\theta}^n(c)\, \gamma_c \sum_{a=1}^{f_\chi}{}^{*} \underline{\chi}'^{-1}\, \underline{\theta}^n(a)\, \xi_\delta^{ac}\ ;$$

on est encore ramené au seul cas $\delta = f_\chi$ et alors on obtient

$$\frac{n}{f'_\chi} \sum_{c=1}^{f_\chi}{}^{*} \underline{\theta}^n(c)\, \gamma_c\, \underline{\chi}'(c)\, \underline{\theta}^{-n}(c)\, \mathscr{G}(\underline{\chi}'^{-1}\underline{\theta}^n) = \frac{n}{f'_\chi}\mathscr{G}(\underline{\chi}'^{-1}\underline{\theta}^n) \sum_{c=1}^{f_\chi}{}^{*} \underline{\chi}'(c)\, \gamma_c\ ;$$

On reconnaît (chap. II, § 2, *b*) : $\frac{1}{f'_\chi}\sum_{c=1}^{f_\chi}{}^{*} \underline{\chi}'(c)\, \gamma_c = B_1(\underline{\chi}'\, \underline{\theta}^{-1})$, d'où la valeur finale de ce terme : $n\, \mathscr{G}(\underline{\chi}'^{-1}\underline{\theta}^n)\, B_1(\underline{\chi}'\,\underline{\theta}^{-1})$.

iii) Etude de $\frac{n\,\ell\, d^{n-1}}{\delta} \sum_{a=1}^{f_\chi}{}^{*} \sum_{c=1}^{\delta}{}^{*} \underline{\chi}'^{-1}(a)\, \underline{\theta}^n(ac)\, \gamma_{\dot{a}}\, \xi_\delta^{ac}$. Il y a en facteur le nombre $\sum_{c=1}^{\delta}{}^{*} \underline{\theta}^n(c)\, \xi_\delta^{ac}$; comme $\delta \equiv 0 \bmod \ell$, cette expression est une combinaison linéaire à coefficients entiers de sommes de Gauss de la forme $\sum_{c=1}^{\ell-1} \underline{\theta}^n(c)\, w^{ic}$, $i \geqslant 0$, elles-mêmes multiples de $\mathscr{G}(\theta^n)$; or d'après la Prop. II.5, $\mathscr{G}(\theta^n)$ a pour valuation $\ell - 1 - n$; comme Λ_n est coefficient de π^n, le terme correspondant est multiple de $\pi^{\ell-1}$ et est donc négligeable. On a donc finalement obtenu :

LEMME IV.5. – *On a* $\Lambda_n^d \equiv 0 \bmod \pi^{\ell-1-n}$ *sauf dans les deux cas suivants :*

i) $n = 1, \lambda = 1, d = \ell$, *où* $\Lambda_1^{\ell} \equiv - \mathcal{G}(\underline{\varphi}'^{-1})\, B_1(\varphi') \bmod \pi^{\ell-1-n}$,

ii) $1 \leqslant n \leqslant \ell - 2$, $d = 1$, *où*

$$\Lambda_n^1 \equiv n\, \mathcal{G}(\underline{\chi}'^{-1}\, \underline{\theta}^n)\, B_1(\underline{\chi}'\, \underline{\theta}^{-1}) \bmod \pi^{\ell-1-n}$$

En conclusion, nous avons obtenu pour Λ_n (d'après les lemmes IV. 4 et IV. 5) :

PROPOSITION IV. 3. — *On a* :

i) *Pour* $\lambda > 1$ *et* $1 \leqslant n \leqslant \ell - 2$,

$$\Lambda_n \equiv n\, \mathcal{G}(\underline{\chi}'^{-1}\, \underline{\theta}^n)\, B_1(\underline{\chi}'\, \underline{\theta}^{-1}) \bmod \pi^{\ell-1-n},$$

ii) *Pour* $\lambda = 1$ *et* $2 \leqslant n \leqslant \ell - 2$,

$$\Lambda_n \equiv n\, \mathcal{G}(\underline{\chi}'^{-1}\, \underline{\theta}^n)\, B_1(\underline{\chi}'\, \underline{\theta}^{-1}) \bmod \pi^{\ell-1-n}$$

iii) *Pour* $\lambda = 1$ *et* $n = 1$,

$$\Lambda_1 \equiv - \mathcal{G}(\varphi'^{-1})\, B_1(\varphi') + \mathcal{G}(\underline{\chi}'^{-1}\, \underline{\theta})\, B_1(\underline{\chi}'\, \underline{\theta}^{-1}) \bmod \pi^{\ell-2}.$$

d) *Etude de* Λ_n *pour* $\lambda = 1$.

α) *Etude de* Λ_1.

On a $\mathcal{G}(\underline{\chi}'^{-1}\underline{\theta}) = \mathcal{G}(\underline{\varphi}'^{-1}\underline{\theta}^{\circ}) = \underline{\varphi}'^{-1}(\ell)\, \mathcal{G}(\varphi'^{-1})\, \mathcal{G}(\underline{\theta}^{\circ})$ ([14], § 20, 2) ; on a $\mathcal{G}(\underline{\theta}^{\circ}) = -1$, d'où

$$\Lambda_1 \equiv - \mathcal{G}(\varphi'^{-1})\, B_1(\varphi') - \varphi'^{-1}(\ell)\, \mathcal{G}(\varphi'^{-1})\, B_1(\underline{\chi}'\, \underline{\theta}^{-1}) \equiv - \\ - \mathcal{G}(\varphi'^{-1})\, (B_1(\varphi') + \underline{\varphi}'^{-1}(\ell)\, B_1(\underline{\chi}'\, \underline{\theta}^{-1}))$$

or $\underline{\chi}'\, \underline{\theta}^{-1} = \underline{\varphi}'\, \underline{\theta}^{\circ}$ et $B_1(\underline{\varphi}'\, \underline{\theta}^{\circ}) = (1 - \underline{\varphi}'(\ell))\, B_1(\varphi')$ (chap. II, § 2, *b*) ; d'où $\Lambda_1 = - \underline{\varphi}'^{-1}(\ell)\, B_1(\varphi')\, \mathcal{G}(\varphi'^{-1})$.

β) *Etude de* Λ_n, $2 \leqslant n \leqslant \ell - 2$. Toujours pour $\lambda = 1$,

$$\Lambda_n = n\, \mathcal{G}(\underline{\chi}'^{-1}\, \underline{\theta}^n)\, B_1(\underline{\chi}'\, \underline{\theta}^{-1}),$$

mais $\mathcal{G}(\underline{\chi}'^{-1}\, \underline{\theta}^n) = \mathcal{G}(\underline{\varphi}'^{-1}\, \underline{\theta}^{n-1})$ est pour $n > 1$ de valuation $\ell - 1 - n + 1$ (Prop. II.5), ce qu'on néglige puisqu'il y a π^n en facteur.

Ainsi dans les cas non résolus au chap. III, on a $b_\phi = 1$ si et seulement si le nombre de Bernoulli primitif $B_1(\varphi')$ est congru à 0 mod $\mathfrak{L}_\chi$ soit $B_{\varphi'^{-1}} \equiv 0 \bmod \mathfrak{L}_\chi$, soit encore $m_{\bar{\phi}}(h) > 0$.

e) *Etude de* Λ_n *pour* $\lambda > 1$. Etudions à titre de vérification le cas $\lambda > 1$. On a alors à calculer

$$\sum_{n=1}^{\ell-2} \Lambda_n \frac{\pi^n t^n}{n\, n!} \equiv \sum_{n=1}^{\ell-2} \mathcal{G}\,(\underline{\chi}'^{-1}\,\underline{\theta}^n)\; B_1\,(\underline{\chi}'\,\underline{\theta}^{-1})\frac{\pi^n t^n}{n!} =$$

$$= B_1\,(\underline{\chi}'\,\underline{\theta}^{-1}) \sum_{n=1}^{\ell-2} \underline{\theta}^{n-\lambda}\,(f'_\chi)\,\underline{\varphi}'^{-1}\,(\ell)\;\mathcal{G}\,(\varphi'^{-1})\;\mathcal{G}\,(\underline{\theta}^{n-\lambda})\frac{t^n\,\pi^n}{n!}\,;$$

on rappelle que t est défini par $\ell^N = 1 + t\,f'_\chi$; on a $t^n \equiv \underline{\theta}^n\,(t) \bmod \ell$, et $\underline{\theta}^n\,(t\,f'_\chi) = \underline{\theta}^n\,(-1) = (-1)^n$ soit $\underline{\theta}^n\,(t) = (-1)^n\,\underline{\theta}^{-n}\,(f'_\chi)$. On utilise le fait que (cf. démonstration de la Prop. II.5)

$$\mathcal{G}\,(\underline{\theta}^{n-\lambda}) \equiv (-1)^{\mu_n}\,\mu_n\,!\;\pi^{\ell-1-\mu_n} \bmod \ell,$$

pour $n \neq \lambda$, avec μ_n = résidu de $n-\lambda$ appartenant à l'ensemble $\{1, \ldots, \ell-1\}$; pour $n = \lambda$, $\mathcal{G}\,(\underline{\theta}^\circ) = -1$, ce qui est l'expression précédente pour $\mu_n = \ell - 1$. Si $n > \lambda$, $\pi^n\,\mathcal{G}(\underline{\theta}^{n-\lambda})$ est de valuation $\ell - 1 + \lambda$; il reste le cas $n \leqslant \lambda$, auquel cas $\mu_n = \ell - 1 + n - \lambda$, et la valuation de $\pi^n\,\mathcal{G}\,(\underline{\theta}^{n-\lambda})$ est $\ell - 1 - \mu_n + n = \lambda$ et on obtient l'expression

$$\sum_{n=1}^{\lambda-1} \underline{\theta}^{n-\lambda}\,(f'_\chi)\,\underline{\varphi}'^{-1}\,(\ell)\mathcal{G}\;(\varphi'^{-1})\quad(-1)^{\mu_n}\frac{\mu_n\,!}{n!}\;(-1)^n\,\underline{\theta}^{-n}\,(f'_\chi)\;\pi^\lambda +$$

$$+ (-1)^{\lambda-1}\,\underline{\theta}^{-\lambda}\,(f'_\chi)\,\underline{\varphi}'^{-1}\,(\ell)\;\mathcal{G}\,(\varphi'^{-1})\frac{\pi^\lambda}{\lambda!} =$$

$$= \underline{\theta}^{-\lambda}\,(f'_\chi)\,\underline{\varphi}'^{-1}\,(\ell)\;\mathcal{G}\,(\varphi'^{-1})\;(-1)^\lambda\,\pi^\lambda\Big(\sum_{n=1}^{\lambda-1}\frac{(\ell-1+n-\lambda)\,!}{n\,!} - \frac{1}{\lambda!}\Big).$$

Evaluons la somme $\dfrac{-1}{\lambda\,!} + \displaystyle\sum_{n=1}^{\lambda-1}\frac{(\ell-1+n-\lambda)\,!}{n\,!}$; on a

$$(\ell-1-\lambda)\,!\sum_{n=1}^{\lambda-1}\frac{(\ell-1+n-\lambda)\,!}{n\,!\;(\ell-1-\lambda)\,!} = (\ell-1-\lambda)!\sum_{n=1}^{\lambda-1} C^n_{\ell-1+n-\lambda} =$$

$$= (\ell-1-\lambda)\,!\sum_{n=1}^{\lambda-1}\frac{(\ell-\lambda)\,(\ell-\lambda+1)\ldots(\ell-\lambda+n-1)}{n\,!} \equiv$$

$$\equiv (\ell - 1 - \lambda)\,!\, \sum_{n=1}^{\lambda-1} (-1)^n \frac{\lambda(\lambda-1)\ldots(\lambda-n+1)}{n\,!} \equiv$$

$$\equiv (\ell - 1 - \lambda)\,!\, \sum_{n=1}^{\lambda-1} (-1)^n C_\lambda^n \equiv -(1+(-1)^\lambda)(\ell - 1 - \lambda)\,! \mod \ell\ ;$$

la somme cherchée est donc égale à $-\dfrac{1}{\lambda\,!} - (1+(-1)^\lambda)(\ell-1-\lambda)!$;

or

$$(\ell - 1 - \lambda)\,! \equiv (-1)^\lambda (\ell-1)(\ell-2)\ldots(\lambda+\,) =$$

$$= (-1)^\lambda \frac{(\ell-1)\,!}{\lambda\,!} \equiv \frac{(-1)^{\lambda-1}}{\lambda\,!}$$

et la somme a pour valeur $\dfrac{(-1)^\lambda}{\lambda\,!}$.

PROPOSITION IV.4. — *Soit* $\chi \in \mathfrak{X}^{\,+}\ \chi \neq 1$. *On suppose*

$$f_\chi = \ell f'_\chi, f'_\chi \neq 1, f'_\chi \not\equiv 0 \mod \ell.$$

Alors pour tout $\phi \mid \chi$ *on a :*

$$L(\overline{\Theta}{}^s_\phi) \equiv \frac{1}{g_\chi} \sum_{\chi' \mid \phi} \chi'(s)\, B_1(\chi'\theta^{-1})\, \underline{\theta}^{-\lambda}(f'_\chi)\, \underline{\varphi}'^{-1}(\ell)\, \mathscr{C}(\varphi'^{-1}) \frac{\pi^\lambda}{\lambda!} \mod \ell.$$

Remarque IV.4. — Pour $\lambda \neq 1$, on vérifie facilement que cette expression coïncide mod ℓ avec l'expression de $\mathrm{Log}(\Theta^s_\phi)$ donnée dans le lemme III.2. Ainsi nous retrouvons bien la condition voulue.

Nous résumons les résultats obtenus dans les Chap. III et IV ainsi que le cas $f_\chi = \ell$ dans le théorème suivant :

THÉORÈME IV.1. — *Soit* $\phi \in \Phi^+$, $\phi \neq 1$. *Alors une condition nécessaire et suffisante pour que* $b_\phi = 1$ (i.e. $\mathscr{F}^\circ_\phi = \mathscr{F}_\phi$) *est que* $m_{\overline{\phi}}(h) > 0$ ($\overline{\phi}$ *désignant le caractère miroir de* ϕ).

4. Exemple d'application des calculs précédents.

On suppose $\ell = 3$ et on suppose que χ est un caractère quadratique pair distinct de θ. On a $K_\chi = Q(\sqrt{f_\chi})$ et $K_{\theta\chi} = Q(\sqrt{-3f_\chi})$. On appelle ϵ_χ l'unité fondamentale de K_χ, choisie plus grande que 1 et on appelle η_χ l'unité cyclotomique définie dans le Chap. I, § 2, *d*. On vérifie facilement que (cf. Chap. III, § 2) $\Theta_\phi = \eta_\chi u^3$; enfin d'après [1] (chap. V, § 4, 1) on vérifie que $|\eta_\chi| = |\epsilon_\chi|^{-h}$, où h est le nombre de classes de K_χ. On en déduit alors la congruence : $L(\overline{\Theta}_\phi) \equiv -h\, L(\overline{\epsilon}_\chi) \mod \pi^3$, où $\overline{\epsilon}_\chi = \epsilon_\chi^2$ (resp. ϵ_χ^8) si 3 n'est pas inerte dans K_χ (resp. est inerte), et où $\pi = \sqrt{-3}$ par exemple.

Nous allons interpréter les deux membres de cette conguence.

LEMME IV.6. – *Posons* $\epsilon_\chi = t + u\sqrt{f_\chi}$ *si* 3 *n'est pas inerte dans* K_χ, *sinon posons* $\epsilon_\chi^4 = t + u\sqrt{f_\chi}$. *Alors*

$$L(\overline{\epsilon}_\chi) \equiv 2\,u\,t\sqrt{f_\chi} \mod \pi^3.$$

Posons $n = t^2 - f_\chi u^2$. On a

$$\overline{\epsilon}_\chi = t^2 + f_\chi u^2 + 2\,u\,t\sqrt{f_\chi} = n + 2\,f_\chi u^2 + 2\,u\,t\sqrt{f_\chi}$$

et

$$L(\overline{\epsilon}_\chi) = n - 1 + 2 f_\chi u^2 + 2\,u\,t\sqrt{f_\chi} - \frac{1}{2}(n - 1 + 2 f_\chi u^2 + 2\,u\,t\sqrt{f_\chi})^2.$$

i) Si $f_\chi \equiv 0 \mod 3$, $\overline{\epsilon}_\chi = \epsilon_\chi^2$, $n = 1$ et

$$L(\overline{\epsilon}_\chi) \equiv 2\,f_\chi u^2 + 2\,u\,t\sqrt{f_\chi} - 2\,u^2\,t^2\,f_\chi \mod \pi^3,$$

mais $t^2 \equiv 1 \mod 3$, d'où $L(\overline{\epsilon}_\chi) \equiv 2\,u\,t\sqrt{f_\chi} \mod \pi^3$.

ii) Si $f_\chi \not\equiv 0 \mod 3$, $ut \equiv 0 \mod 3$, $n - 1 + 2\,f_\chi u^2 \equiv 0 \mod 3$ et $L(\overline{\epsilon}_\chi) \equiv n - 1 + 2\,f_\chi u^2 + 2\,u\,t\sqrt{f_\chi} \mod 9$. Si $n = 1$ alors

$$u \equiv 0 \mod 3 \qquad \text{et} \qquad L(\overline{\epsilon}_\chi) \equiv 2\,u\,t\sqrt{f_\chi} \mod 9.$$

Si $n = -1$ alors $t \equiv 0 \mod 3$ et $n - 1 + 2\,f_\chi u^2 = 2\,t^2 \equiv 0 \mod 9$ d'où $L(\overline{\epsilon}_\chi) \equiv 2\,u\,t\sqrt{f_\chi} \mod 9$.

Posons comme d'habitude $\chi = \varphi\,\theta^\lambda$, φ de conducteur premier à 3 et $1 \leqslant \lambda \leqslant 2$.

Si h' est le nombre de classes de $Q(\sqrt{-3f_\chi})$, on a (Chap. I, § 2, *d*) : $h' = -\dfrac{1}{f_{\chi\theta}}\displaystyle\sum_{a=1}^{f_{\chi\theta}} \chi\theta(a)\,a = -B_1(\chi\theta)$ (nombre de Bernoulli primitif) et d'après la Prop. IV.4 on a

$$\mathrm{L}(\overline{\Theta}_\phi) \equiv -\mathrm{B}_1(\chi\theta)\,\underline{\theta}^\lambda(f'_\chi)\,\underline{\varphi}(3)\,\mathscr{C}(\varphi)\frac{\pi^\lambda}{\lambda!} \bmod \pi^3$$

d'où la relation $h\,u\,t\sqrt{f_\chi} \equiv h'\,\underline{\theta}^\lambda(f'_\chi)\,\underline{\varphi}(3)\;\mathscr{C}(\varphi)\frac{\pi^\lambda}{\lambda!} \bmod \pi^3$.

Distinguons deux cas :

i) $f_\chi \not\equiv 0 \bmod 3$; alors $\lambda = 2$, $\phi = \varphi$ est pair, d'ou $\mathscr{C}(\varphi) = \sqrt{f_\chi}$ ([1], chap. V, § 4, 3) et $h\,u\,t \equiv -3\,h'\,\varphi(3) \bmod \pi^3$, soit

$$h\frac{u\,t}{3} \equiv -\varphi(3)\,h' \bmod 3.$$

On retrouve bien les congruences de [17] puisque dans ce cas

$$\mathrm{L}(\overline{\epsilon}_\chi) \equiv \mathrm{Log}\,(\overline{\epsilon}_\chi) \bmod \pi^3.$$

ii) $f_\chi \equiv 0 \bmod 3$. Ceci correspond au cas "spécial". Nous renvoyons le lecteur à nos remarques (chap. III, § 4) rappelant que l'utilisation dans le cas "spécial" des fonctions L_ℓ ℓ-adiques de Leopoldt-Fresnel ne permet pas en général de conclure. Ce phénomène apparaît clairement ici car dans le cas $\varphi(3) = 1$, la congruence de [17] se réduit à $0 \equiv 0 \bmod 3$ et Ankeny, Artin et Chowla supposaient dans leur papier de 1952, $f_\chi = 3q$, $q \not\equiv 2 \bmod 3$. Ici nous allons obtenir une congruence non triviale :

Nous avons $\chi = \varphi\,\theta$, $\lambda = 1$ et φ est impair, donc

$$\mathscr{C}(\varphi) = \sqrt{-f_\chi/3}$$

([1], chap. V, § 4, 3) et

$$h\,u\,t\sqrt{f_\chi} \equiv h'\,\underline{\theta}\,(f'_\chi)\,\underline{\varphi}(3)\sqrt{-f_\chi/3}\sqrt{-3} \bmod \pi^3$$

soit $h\,u\,t \equiv h'\,\underline{\theta}\,(f'_\chi)\,\underline{\varphi}(3) \bmod 3$; on vérifie que $\underline{\theta}\,(f'_\chi)\,\underline{\varphi}(3) = -1$, d'où $h\,u\,t \equiv -h' \bmod 3$.

Remarque IV.5. – Il est facile, compte tenu de l'expression de $\mathrm{L}(\Theta_\phi)$ (Prop. IV.4) et de la Rem. IV.4 d'obtenir des congruences généralisant celles provenant de l'utilisation des fonctions L_ℓ ℓ-adiques dans tous les cas, y compris le cas "spécial", à condition de remplacer, comme pour le cas quadratique ci-dessus, le logarithme par la fonction L.

5. Conclusion.

Pour compléter les remarques (chap. III, § 4) déjà faites nous pensons que la définition classique du régulateur (par imitation du cas complexe) est inadaptée au cas ℓ-adique compte tenu du fait que le phénomène essentiel dans ces questions est la ℓ-primarité (et par extension la ℓ^n-primarité) et que la fonction Log ℓ-adique ne la traduit pas, au contraire de la fonction L (la ℓ^n-primarité nécessitant d'introduire les fonctions de Chafarevitch (cf. [15])).

CHAPITRE V

AUTRES CONSEQUENCES DES RESULTATS PRECEDENTS

1. Classes de caractères ℓ-adiques.

a) *Définitions.* Les résultats des chapitres précédents (notamment les Th. I.1, I.2, I.3 et IV. 1) montrent qu'il y a certaines relations possibles entre les groupes $\mathcal{H}_\phi$ $\phi \in \Phi$, relations qui font intervenir ϕ et $\bar{\phi}$ mais aussi leurs différents caractères ℓ-adiques conjugués (i.e. divisant le caractère rationnel qui est au-dessus). On est donc conduit à poser la définition suivante :

DEFINITION V.1. – *Nous dirons que deux caractères ϕ et ϕ' sont "équivalents" si ϕ' est obtenu à partir de ϕ au moyen d'une composition finie des opérations suivantes :*

i) *passage d'un élément de Φ au caractère miroir,*

ii) *passage d'un élément de Φ à l'un de ses conjugués.*

PROPOSITION V.1. – *La relation précédente est une relation d'équivalence dont les classes sont finies. Une classe* C *est une réunion disjointe de* $C^+ = C_\cap \Phi^+$ *et* $C^- = C_\cap \Phi^-$ *et on a* $|C^+| = |C^-|$.

Remarque V.1. – Cette notion de classe permet d'améliorer la connaissance de la structure des groupes $\mathcal{H}_\phi$: en effet, il apparaîtra clairement dans les exemples que la considération simultanée de tous les $\mathcal{H}_\phi$, pour les caractères ϕ d'une classe C, donne le maximum d'informations sur chacun d'eux, alors que l'examen du seul couple $\mathcal{H}_\phi$, $\mathcal{H}_{\bar{\phi}}$ (comme il est classique de le faire) est, à priori, moins précis.

b) *Exemples de classes.* Pour engendrer une classe, il suffit de prendre $\phi \in \Phi$ et de procéder de la façon suivante : on établit la liste des conjugués de ϕ puis celle de leurs miroirs respectifs ; à partir de chacun des caractères ainsi obtenus, on recommence le même processus.

Remarque V.2. – Comme $\bar{\phi}$ est dans la classe de ϕ, on peut toujours engendrer une classe à partir d'un caractère réel.

Nous représentons les classes de la façon suivante :

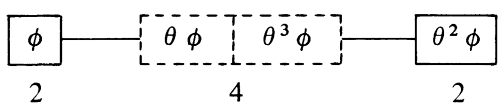
i) Dans un rectangle en trait plein (resp. pointillé) nous regroupons les ensembles de caractères conjugués réels (resp. imaginaires). De tels rectangles sont donc associés aux caractères rationnels (i.e. aux corps K_χ, $\chi \in \mathfrak{X}$) pairs (resp. impairs). On indique à côté le degré du corps K_χ concerné.

ii) Nous relions par un trait un caractère ℓ-adique et son miroir.

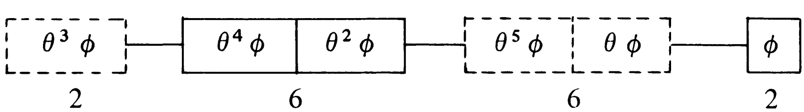
Dans les exemples suivants, on suppose que le caractère $\phi \mid \chi$ est tel que K_χ/Q est linéairement disjointe de $Q^{(\ell)}/Q$. Le graphe obtenu ne dépend donc en fait que du couple (g_χ, ℓ).

Exemple V.1. – $g_\chi = 2$, $\ell = 3$.

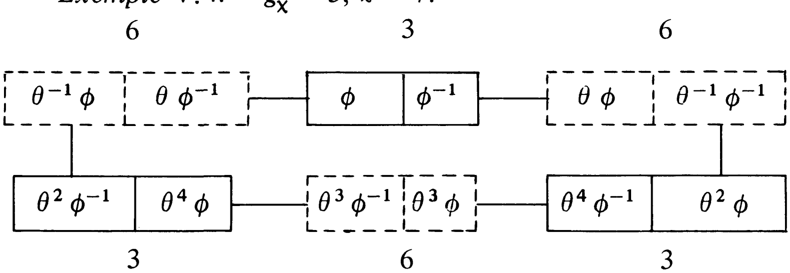
Exemple V.2. $g_\chi = 2$, $\ell = 5$.



Exemple V.3. $g_\chi = 2$, $\ell = 7$.



Exemple V.4. – $g_\chi = 3$, $\ell = 7$.



2. Problèmes.

Posons la définition suivante :

DEFINITION V. 2. – *On appelle propriété* A (resp. A^+, A^-) *la propriété* : "$m_\phi(\mathcal{H}) = m_\phi(h)$ *pour tout* $\phi \in \Phi$" (resp. $\phi \in \Phi^+$, $\phi \in \Phi^-$). *On appelle propriété* B (resp. B^+, resp. B^-) *la propriété* "$l^{m_\phi(h)}$ *annule le groupe* $\mathcal{H}_\phi$ *pour tout* $\phi \in \Phi$" (resp. $\phi \in \Phi^+$, $\phi \in \Phi^-$).

Il est clair que A implique B.

Seule à notre connaissance la propriété B^- est démontrée (théorème de Stickelberger). On peut alors poser les problèmes suivants :

i) Les propriétés A, B sont-elles vraies (même question avec A^-, A^+ et B^+) ?

ii) Quelles sont des conditions nécessaires à l'existence d'un contre-exemple ?

Remarque V.3. – En restreignant les propriétés A et B à une classe C, on peut envisager les deux questions précédentes ; on est ainsi ramené à une situation équivalente plus simple.

Nous allons, dans le § suivant, examiner les propriétés A et B relativement à une classe C dans un esprit "numérique" et nous allons préciser des conditions d'ordre numérique à satisfaire pour espérer trouver des contre-exemples. Il est important de noter que dans les cas numériques connus, il y a, dans une classe C "suffisamment peu" de $\mathcal{H}_\phi$ non triviaux pour que les résultats établis dans les chapitres précédents permettent de contredire A et B (les conditions nécessaires à un contre-exemple sont relativement difficiles à obtenir sur le plan numérique).

3. Etude des propriétés A et B.

DEFINITION V.3. – *Soit* C *une classe,* $C = C^+ \cup C^-$. *On appelle* C_0 *l'ensemble* $\{\phi \in C^-, m_\phi(h) > 0\}$ *et on appelle* $\bar{C}_0$ *l'ensemble* $\{\bar{\phi}, \phi \in C_0\}$. Dans la pratique, C_0 est connu à partir du calcul des nombres de Bernoulli.

Remarque V.4. – Il convient de remarquer que dans les tous premiers exemples numériques que l'on peut obtenir, la plupart des $m_\phi(h)$, pour $\phi \in C$, sont nuls et, la plupart des $m_\phi(h)$ non nuls, sont égaux à 1. On peut alors donner quelques énoncés tenant compte de ce fait.

PROPOSITION V.2. – *Soit* C *une classe.*

i) *Si dans* C_0 *il n'y a pas de couples de caractères conjugués alors* A^- *est vraie ;*

ii) *Si dans* $\overline{C}_0$ *il n'y a pas de couples de caractères conjugués alors* A^+ *est vraie pour* C.

Démonstration

i) résulte du Corol. I.3.

ii) Soit χ un caractère rationnel au-dessus d'un élément de C^+. Par hypothèse, pour au plus un $\phi_0 \mid \chi$, $m_{\bar{\phi}_0}(h) > 0$, soit $b_{\phi_0} = 1$ (Th. IV.1). Si on avait pour $\phi_1 \mid \chi$, $\phi_1 \neq \phi_0, \mathcal{H}_{\phi_1} \neq (1)$, on aurait (Th. I.3) $\mathcal{H}_{\bar{\phi}_1} \neq (1)$ soit $m_{\bar{\phi}_1}(h) > 0$ soit $b_{\phi_1} = 1$, ce qui est absurde.

PROPOSITION V.3. – *Soit* C *une classe. On fait les deux hypothèses suivantes :*

i) *Pour tout* $\phi \in C^-$, $m_\phi(h) \leqslant 1$,

ii) *Dans* $\overline{C}_0$, *il n'y a pas de couples de caractères conjugués. Alors* A *est vraie pour* C.

Démonstration. – D'après la Prop. V.2 A^+ est vraie. Supposons A^- fausse : cela signifie qu'il existe $\phi_1, \phi_2 \in C_0$ tels que $\mathcal{H}_{\phi_1} \simeq (\mathbf{Z}/\ell\,\mathbf{Z})^n$, $n \geqslant 2$ et $\mathcal{H}_{\phi_2} = (1)$. Comme $m_{\phi_1}(h) = m_{\phi_2}(h) = 1$, on a

$$b_{\bar{\phi}_1} = b_{\bar{\phi}_2} = 1 \ ;$$

$\mathcal{H}_{\bar{\phi}_2}$ est nécessairement trivial (Th. I.3) et $a_{\bar{\phi}_2} = 0$ (Corol. I.6, i)) mais $b_{\bar{\phi}_2} = 1$ et $a_{\bar{\phi}_2} = 0$ entraîne $m_{\bar{\phi}_2}(h) > 0$, ce qui contredit A^+.

COROLLAIRE V.1. – *Si* C *est la classe obtenue pour* $g_\chi = 2$, $\ell = 5$, *des conditions nécessaires à un contre-exemple à la propriété* A *sont les suivantes* (cf. Exemple V.2) :

i) $m_{\theta\phi}(h)$, $m_{\theta^3\phi}(h) > 0$ *et l'un de ces deux nombres au moins est supérieur ou égal à* 2.

ii) $a_\phi + \dim_\phi \mathcal{H}_\phi > 0$, $a_{\theta^2\phi} + \dim_{\theta^2\phi} \mathcal{H}_{\theta^2\phi} > 0$ *et l'un de ces deux nombres est supérieur ou égal à* 2.

En effet, si par exemple $m_{\theta\phi}(h) = 0$, alors A^- est vérifiée (donc A) ; on doit donc avoir $m_{\theta\phi}(h)$, $m_{\theta^3\phi}(h) > 0$. Si ces deux nombres sont égaux à 1, la Prop. V.3 montre que A est vraie. De plus l'un des groupes $\mathcal{H}_{\theta\phi}$, $\mathcal{H}_{\theta^2\phi}$ a un 5-rang plus grand que 1 strictement (sinon A^- est vraie (Corol. I .4)), d'où le corollaire en utilisant pour (ii) le th. I .3.

Remarque V.5. – En modifiant les hypothèses des énoncés précédents, on pourrait en donner d'autres ; en fait il est préférable d'examiner des situations numériques et d'essayer pour chacune d'elles de conclure en utilisant tous les renseignements dont on dispose. Si l'on rencontre un cas "non décidable" il faudra voir s'il constitue un contre-exemple ou non, par d'autres méthodes.

Signalons pour terminer quelques études numériques qui sont en cours de programmation :

a) Etude des types de classes suivantes :

i) classes obtenues pour $g_\chi = 2$ et $\ell = 5$;

ii) classes obtenues pour $g_\chi = 3$ et $\ell = 7, 13, 19, \ldots$ (situation destinée à exploiter les résultats des tables de [10]) ;

iii) classes engendrées par les caractères θ, pour tout ℓ. (situation du "Théorème de Fermat").

b) Etude de la table de [28]. En effet, cette table met en évidence un certain nombre de cas intéressants (une trentaine environ) pour lesquels il est nécessaire de recalculer les invariants $m_\phi(h)$ (la table de [28] ne permettant de retrouver que les invariants $m_\chi(h)$).

BIBLIOGRAPHIE

[1] Z.I. BOREVITCH et I.R. CHAFAREVITCH, Théorie des Nombres, Gauthier-Villars, Paris (1967).

[2] A. BRUMER, Travaux récents d'Iwasawa et de Leopoldt, Séminaire Bourbaki 325 (1967).

[3] J. COATES and S. LICHTENBAUM, On ℓ-adic Zeta functions, *Ann. of Math.*, 98 (1973), 498-550.

[4] J. FRESNEL, Nombres de Bernoulli et fonctions L p-adiques, *Ann. Inst. Fourier,* Grenoble 17, 2 (1967), 281-333.

[5] J. FRESNEL, Applications arithmétiques de la formule p-adique des résidus, Séminaire Delange-Pisot-Poitou, 18 (1966-67), 1-8.

[6] E. GALLOU, Sur le rang du p-groupe des classes relatives des corps $Q^{(p)}$, Séminaire de théorie des Nombres, Grenoble (1972).

[7] R. GILLARD, Relations de Stickelberger, Séminaire de théorie des Nombres, Grenoble (1974).

[8] G. GRAS et M.N. GRAS, Signature des unités cyclotomiques et parité du nombre de classes des extensions cycliques de Q de degré premier impair, *Ann. Inst. Fourier,* Grenoble 25, 1 (1975), 1-22.

[9] G. GRAS, Critère de parité du nombre de classes des extensions abéliennes réelles de Q de degré impair, *Bull. Soc. Math. de France*, 103 (1975), 177-190.

[10] M.N. GRAS, Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de Q, *Jour. für die reine und ang. Math.*, 277 (1975), 89-116.

[11] G. GRAS et M.N. GRAS, Calcul du nombre de classes et des unités des extensions abéliennes réelles de Q, *Publ. Math. de l'Univ. de Besançon* (Théorie des Nombres) 1974-1975.

[12] R. GREENBERG, On p-adic L-Functions and cyclotomic Fields, *Nagoya Math. J.*, 56 (1974), 61-77.

[13] H. HASSE, Über die Klassenzahl abelscher Zahlkörper, Berlin (1952).

[14] H. HASSE, Vorlesungen über Zahlentheorie, Berlin (1950).

[15] H. HASSE, Zur Arbeit von I.R. Šafarevič über das allgemeine Reziprozitätsgesetz, *Math. Nach.*, (1951), 301-327.

[16] T. KUBOTA und H.W. LEOPOLDT, Eine p-adische theorie der Zetawerte ; I Einführung der p-adischer Dirichletschen, L-Funktionen, *Jour. für die reine und ang. Math.*, 214/215 (1964), 328-339.

[17] A. KUDO, On a class number relation of imaginary abelian fields, *J. Math. Soc. Japan,* 27, 1 (1975).

[18] S. LANG, Algebraic Number Theory, New-York (1970).

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

[20] H.W. LEOPOLDT, Eine Verallgemeinerung der Bernoullishen Zahlen, *Abh. Math. Sem. Univ. Hamburg,* 22 (1958), 131-140.

[21] H.W. LEOPOLDT, Über Fermatquotienten von Kreisenheiten und Klassenzahlformeln modulo p, *Rend. Cir. mat. Palermo,* Serie 2, 9 (1960), 39-50.

[22] H.W. LEOPOLDT, Über Klassenzahlprimteiler reeller abelscher Zahlkörper als Primteiler verallgemeinerter Bernoullischen Zahlen, *Abh. Math. Sem. Univ. Hamburg,* 23 (1959), 36-47.

[23] H.W. LEOPOLDT, Zur Struktur der ℓ-Klassengruppe galoisscher Zahlkörper, *Jour. für die reine und ang. Math.*, 199 (1958), 165-174.

[24] H.W. LEOPOLDT, Zur Arithmetik in abelschen Zahlkörpern, *Jour. für die reine und ang. Math.*, 209 (1962), 54-71.

[25] B. ORIAT, Relation entre les 2-groupes des classes d'idéaux au sens ordinaire et restrient de certains corps de nombres, *Bull. Soc. Math. France,* 104 (1976), 301-307.

[26] B. ORIAT, Traduction française de "Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper" de Leopoldt, *Publ. Math. de l'Univ. de Besançon* (Théorie des Nombres) 1974-1975.

[27] B. ORIAT, Quelques caractères utiles à l'arithmétique, *Publ. Math. de l'Univ. de Besançon* (Théorie des Nombres) 1974-1975.

[28] G. SCHRUTKA V. RECHTENSTAMM, Tabelle der (relativ)-Klassenzahlen der Kreiskörper, *Abh. Deutschen Akad. Berlin,* Math. Klasse (1964), 1-64.

[29] J.P. SERRE, Représentations linéaires des groupes finis, Hermann (1971).

Manuscrit reçu le 2 octobre 1975
Proposé par J. Martinet.

Georges GRAS,
Mathématiques
Faculté des Sciences
25030 Besançon Cedex.