PUBLICATIONS

MATHEMATIQUES

D'ORSAY

79.01

FONCTIONS L p-ADIQUES ET THÉORIE D'IWASAWA

Notes de Philippe SATGÉ d'après un cours de

Kenneth RIBET

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

PUBLICATIONS

MATHEMATIQUES

D'ORSAY

79.01

FONCTIONS L p-ADIQUES ET THÉORIE D'IWASAWA

Notes de Philippe SATGÉ d'après un cours de

Kenneth RIBET

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

Ces notes représentent la rédaction, faite par Philippe Satgé, de mon cours à Orsay au premier semestre 1977-78. Les sujets principaux que j'ai traités étaient les suivants :

- Mesures p-adiques (sur $\hat{\mathbb{Z}}$) attachées aux valeurs des fonctions L de Dirichlet.
- La théorie des fonctions L p-adiques à la Kubota-Leopoldt.
- Corps cyclotomiques, et en particulier : Unités cyclotomiques et groupes de classes.
- Relations (conjecturelles ou connues) entre fonctions L p-adiques et modules d'Iwasawa.

Pendant le cours, je consultais souvent mes notes d'un cours donné à Princeton par N. Katz [11] il y a deux ans (1976-77), ainsi que le manuscrit du nouveau livre de Lang sur les corps cyclotomiques [13]. On peut également signaler comme cours :

- Le livre de K. Iwasawa sur les fonctions L p-adiques [8], et ses articles [9] et [10].

- L'article de Coates à Durham [4], et surtout le dernier article de Coates-Wiles [5].

Je remercie vivement Philippe Satgé pour le travail important qu'il a fait en préparant ces notes, et en particulier pour la mise au point de plusieurs démonstrations. Sa contribution est partout évidente.

La rédaction finale de ce cours a profité de certaines remarques de Marie-France Vignéras, à qui j'adresse mes remerciements.

J'aimerais également remercier le département de mathématiques de l'Université de Paris-Sud pour l'accueil chaleureux que j'ai reçu pendant mon séjour à Orsay. Je pense en particulier à l'aide précieuse que m'a apportée Georges Poitou, et à la gentillesse de Mmes Bonnardel et Parvan, qui ont frappé ce manuscrit.

TABLE DES MATIÈRES

§ 0. RAPPEL.

Soit a un réel appartenant à $]0,1]$.

Pour tout complexe s de partie réelle plus grande que 1, la série $\sum_{n=o}^{\infty} (n+a)^{-s}$ converge et définit une fonction holomorphe sur le demi-plan $Re(s) > 1$; on note $\zeta(s,a)$ cette fonction et on l'appelle fonction zêta de Hurwitz associée à a. La fonction $\zeta(s,a)$ admet un prolongement méromorphe à tout le plan complexe avec un seul pôle en $s=1$; ce pôle est simple et son résidu est 1.

Soient X et Z deux indéterminées ; pour tout entier $n \geq 0$ on définit le polynôme $B_n(X)$ appelé $n^{\text{ième}}$ polynôme de Bernoulli par l'identité suivante :

$$\frac{Z e^{XZ}}{e^Z - 1} = \sum_{n \geq o} B_n(X) \frac{Z^n}{n!} .$$

Il est clair que les coefficients des $B_n(X)$ sont rationnels ; on montre que pour tout entier $k \geq 1$, on a $\zeta(1-k,a) = -\frac{1}{k} B_k(a)$.

Soit maintenant ε une application périodique de $\mathbf{Z}$ dans $\mathbb{C}$. Pour tout complexe s de partie réelle plus grande que 1, la série $\sum \varepsilon(n) n^{-s}$ converge ; nous notons $L(s,\varepsilon)$ sa somme. Si f est un multiple de la période de ε, on a

$L(s,\varepsilon) = f^{-s} \sum_{t=1}^{f} \varepsilon(t) \zeta(s, \frac{t}{f})$ pour tout s de partie réelle plus grande que 1 ; en conséquence $L(s,\varepsilon)$ se prolonge à $\mathbb{C}$ tout entier en une fonction méromorphe avec au plus un pôle en $s=1$ et, pour tout, entier $k \geq 1$, on a $L(1-k,\varepsilon) = -\frac{f^{k-1}}{k} \sum_{t=1}^{f} \varepsilon(t) B_k(\frac{t}{f})$.

Cette égalité montre que $-\frac{f^{k-1}}{k}\sum_{t=1}^{f}\varepsilon(t)\,B_k(\frac{t}{f})$ ne dépend pas du multiple f de la période de ε que l'on a choisie. Cette indépendance est le point dont nous aurons besoin dans la suite. On peut vérifier cette indépendance à l'aide d'identités simples sur les polynômes de Bernoulli sans interpréter la quantité qui nous intéresse comme la valeur en $1-k$ de $L(s,\varepsilon)$. Bien que plus rapide et suffisante pour la suite, cette dernière méthode ne serait pas dans l'"esprit".

Considérons maintenant une application périodique ε de $\mathbb{Z}$ dans un espace vectoriel V sur $\mathbb{Q}$ (nous serons essentiellement intéressés par le cas $V=\mathbb{Q}_p$). Soit f un multiple de la période de ε ; pour tout entier $k \geq 1$ et tout entier t les $B_k(\frac{t}{f})$ sont rationnels, donc $-\frac{f^{k-1}}{k}\sum_{t=1}^{f}\varepsilon(t)\,B_k(\frac{t}{f})$ est un élément de V. En choisissant une base de V sur $\mathbb{Q}$, en décomposant ε dans cette base et en raisonnant séparément sur chaque composante, on déduit de ce qui a été vu plus haut que $-\frac{f^{k-1}}{k}\sum_{t=1}^{f}\varepsilon(t)\,B_k(\frac{t}{f})$ ne dépend pas du multiple f de la période de ε choisie ; par analogie avec le cas $V=\mathbb{C}$, nous poserons $L(1-k,\varepsilon) = -\frac{f^{k-1}}{k}\sum_{t=1}^{f}\varepsilon(t)\,B_k(\frac{t}{f})$.

§ 1. LES CONGRUENCES DE KUMMER-MAZUR

Si ϵ est une fonction périodique de $\mathbb{Z}$ dans $\mathbb{Q}_p$ et si C est un entier rationnel, nous désignons par ϵ_C la fonction de $\mathbb{Z}$ dans $\mathbb{Q}_p$ définie par $\epsilon_C(x) = \epsilon(Cx)$; il est clair que ϵ_C est périodique et que sa période divise celle de ϵ. Pour tout entier strictement positif k, on pose $\Delta_C(1-k,\epsilon) = L(1-k,\epsilon) - C^k L(1-k,\epsilon_C)$ c'est-à-dire (voir § 0) $\Delta_C(1-k,\epsilon) = -\frac{f^{k-1}}{k}\left[\sum_{t=1}^{f} (\epsilon(t) - C^k\epsilon(Ct))B_k(\frac{t}{f})\right]$ où f est un multiple de la période de ϵ (donc aussi de celle de ϵ_C). Le but de ce paragraphe est la démonstration du théorème suivant :

THEOREME 1.1. (congruences de Kummer-Mazur). *Soient* $\epsilon_1,\dots,\epsilon_t$ *des applications périodiques de* $\mathbb{Z}$ *dans* $\mathbb{Q}_p$ *et* $k_1,\dots,k_t$ *des entiers strictement positifs. On suppose que, pour tout entier naturel* x, *la somme* $\sum_{i=1}^{t} \epsilon_i(x)x^{k_i-1}$ *est dans* $\mathbb{Z}_p$. *Alors, pour tout entier strictement positif* C *premier à* p *et aux périodes des* ϵ_i, *la somme* $\sum_{i=1}^{t} \Delta_C(1-k_i,\epsilon_i)$ *est dans* $\mathbb{Z}_p$.

Avant de démontrer ce théorème, nous allons en donner deux corollaires :

COROLLAIRE 1.2. *Avec les notations du théorème, si* $\sum_{i=1}^{t} \epsilon_i(x)x^{k_i-1}$ *est dans* $p^n\mathbb{Z}_p$ *pour un* $n>0$, *alors* $\sum_{i=1}^{t} \Delta_C(1-k_i,\epsilon_i)$ *est dans* $p^n\mathbb{Z}_p$.

Démonstration. On applique le théorème en remplaçant les ϵ_i par $\frac{\epsilon_i}{p^n}$ et on conclut en remarquant que $\Delta_C(1-k_i,\frac{\epsilon_i}{p^n}) = \frac{1}{p^n}\Delta_C(1-k_i,\epsilon_i)$.

COROLLAIRE 1.3. Soit V un espace vectoriel de dimension finie sur $\mathbb{Q}_p$ et L un sous-$\mathbb{Z}_p$-module libre de V tel que $\mathbb{Q}_p.L = V$. Soient $\epsilon_1, \dots, \epsilon_t$ des applications périodiques de $\mathbb{Z}$ dans V et $k_1, \dots, k_t$ des entiers strictement positifs. On suppose que, pour tout entier naturel x, la somme $\sum_{i=1}^{t} \epsilon_i(x) x^{k_i - 1}$ est dans $p^n L$ pour un $n \geq 0$. Alors, pour tout entier C premier à p et aux périodes des ϵ_i, la somme $\sum_{i=1}^{t} \Delta_C(1-k_i, \epsilon_i)$ est dans $p^n L$.

Démonstration. On décompose les ϵ_i suivant une $\mathbb{Z}_p$-base de L qui est aussi une $\mathbb{Q}_p$-base de V et on applique le corollaire précédent.

Ce corollaire 1.3 est la forme générale du théorème 1.1. Nous l'appliquerons essentiellement dans le cas où V est une extension finie de $\mathbb{Q}_p$ et où L est l'anneau des entiers de V.

Venons en à la démonstration du théorème ; deux lemmes seront nécessaires :

LEMME 1.4. Le théorème 1.1 est vrai dans le cas $t=1$ et $k=1$.

Démonstration. Dans ce cas on a une application ϵ_1 périodique de $\mathbb{Z}$ dans $\mathbb{Z}_p$; soit f sa période, il faut montrer que, pour tout entier $C \geq 1$ tel que $(C, fp) = 1$, la quantité $\Delta_C(0, \epsilon_1)$ est dans $\mathbb{Z}_p$. Pour tout entier a tel que $1 \leq a \leq f$, notons $\chi_{a,f}$ l'application de $\mathbb{Z}$ dans $\mathbb{Z}_p$ définie par $\chi_{a,f}(x) = 0$ si $x \not\equiv a \bmod f$ et $\chi_{a,f}(x) = 1$ si $x \equiv a \bmod f$. On a $\epsilon_1 = \sum_{a=1}^{f} \epsilon(a) \chi_{a,f}$ et $\Delta_C(0, \epsilon_1) = \sum_{a=1}^{f} \epsilon(a) \Delta_C(0, \chi_{a,f})$; pour démontrer notre lemme, il suffit donc de montrer que $\Delta_C(0, \chi_{a,f})$ est dans $\mathbb{Z}_p$ pour tout entier a tel que $1 \leq a \leq f$ et tout entier $C \geq 1$ tel que $(C, fp) = 1$. Pour un tel a et un tel C, notons d l'entier compris entre 1 et f tel que $Cd \equiv a \bmod f$. Le polynôme $B_1(X)$ étant $X - \frac{1}{2}$, on a $\Delta_C(0, \chi_{a,f}) = -(\frac{a}{f} - \frac{1}{2}) + C(\frac{d}{f} - \frac{1}{2})$ soit $\Delta_C(0, \chi_{a,f}) = \frac{dC - a}{f} + \frac{1-C}{2}$. Mais $\frac{dC-a}{f}$ est dans $\mathbb{Z}$ par définition de d et $\frac{1-C}{2}$ est dans $\mathbb{Z}_p$, puisque, par hypothèse, C est impair si $p=2$; en conséquence $\Delta_C(0, \chi_{a,f})$ est dans $\mathbb{Z}_p$ d'où le lemme.

Pour le second lemme on fixe un entier $k \geq 1$ et un entier $N \geq 0$. On désigne par δ une fonction périodique de $\mathbb{Z}$ dans $\mathbb{Z}_p$ dont la période est une puissance de p et qui vérifie pour tout x de $\mathbb{Z}$ la congruence $\delta(x) \equiv x^{k-1} \bmod p^N\mathbb{Z}_p$ (on peut par exemple prendre $\delta(x) = i^{k-1}$ où i est l'entier congru à x modulo p^N et compris entre 1 et p^N). On a alors :

LEMME 1.5. <u>Soit ϵ une fonction périodique de $\mathbb{Z}$ dans $\mathbb{Z}_p$ et C un entier positif premier à p et à la période de ϵ. La fonction δ étant celle définie ci-dessus, on a la congruence</u>

$$\Delta_C(0, \epsilon\delta) \equiv \Delta_C(1-k, \epsilon) \text{ modulo } p^N\mathbb{Z}_p.$$

<u>Démonstration</u>. Notons $f(\epsilon)$ la période de ϵ. Soit n un entier tel que $n > N$, que $p^n \frac{B_k(X)}{k} \in p^N\mathbb{Z}_p[X]$ et que p^n soit multiple de la période de δ ; on pose $f = f(\epsilon)p^n$. On a $\epsilon = \sum_{a=1}^{f} \epsilon(a)\chi_{a,f}$ où les $\chi_{a,f}$ sont définies dans la démonstration du lemme précédent. On a donc $\Delta_C(0, \epsilon\,\delta) = \sum_{a=1}^{f} \epsilon(a)\, \Delta_C(0, \chi_{a,f}\delta)$ et $\Delta_C(1-k, \epsilon) = \sum_{a=1}^{f} \epsilon(a)\Delta_C(1-k, \chi_{a,f})$; en conséquence il suffit de démontrer notre lemme pour $\epsilon = \chi_{a,f}$ ce que nous allons faire en trois étapes.

1) Soit d l'entier compris entre 1 et f tel que $Cd \equiv a \bmod f$ (d existe puisque, par hypothèse, C est premier à $f(\epsilon)$ et à p donc à f) ; montrons la congruence $\Delta_C(0, \chi_{a,f}\delta) \equiv a^{k-1}(\frac{Cd-a}{f} - \frac{C-1}{2}) \bmod p^N\mathbb{Z}_p$. On a $\Delta_C(0, \chi_{a,f}\,\delta) = -\delta(a)\,(\frac{a}{f} - \frac{1}{2}) + C\;\delta(Cd)\,(\frac{d}{f} - \frac{1}{2}) = \delta(a)(\frac{Cd-a}{f} - \frac{C-1}{2})$ puisque $Cd \equiv a \bmod f$ implique $\delta(Cd) = \delta(a)$. On a remarqué dans la démonstration du lemme précédent que $\frac{Cd-a}{f}$ et $\frac{C-1}{2}$ sont dans $\mathbb{Z}_p$ (même pour $p=2$) ; comme $\delta(a) \equiv a^{k-1} \bmod p^N\mathbb{Z}_p$, on a bien $\Delta_C(0, \chi_{a,f}.\delta) \equiv a^{k-1}(\frac{Cd-a}{f} - \frac{C-1}{2}) \bmod p^N\mathbb{Z}_p$.

2) Montrons $\Delta_C(1-k, \chi_{a,f}) \equiv a^{k-1}(\frac{Cd-a}{f} - \frac{C-1}{2})$ modulo $p^N\mathbb{Z}_p$ où d est toujours l'entier compris entre 1 et f tel que $Cd \equiv a \bmod f$. On vérifie sur la définition de $B_k(X)$ que $B_k(X) = X^k - \frac{k}{2}X^{k-1} + \sum_{j=o}^{k-2} \frac{\alpha_j}{\beta_j} X^j$ avec α_j et β_j dans $\mathbb{Z}$. On a donc $-\frac{f^{k-1}}{k} B_k(\frac{a}{f}) = -\frac{f^{k-1}}{k}\left[(\frac{a}{f})^k - \frac{k}{2}(\frac{a}{f})^{k-1}\right] - \frac{f}{k}\left[\sum_{j=o}^{k-2} \frac{\alpha_j}{\beta_j} a^j f^{k-2-j}\right]$; mais on a choisi f de sorte que $\frac{f}{k}\frac{\alpha_j}{\beta_j} \in p^N\mathbb{Z}_p$ pour tout j, donc on a $-\frac{f^{k-1}}{k} B_k(\frac{a}{f}) \equiv -\frac{f^{k-1}}{k}\left[(\frac{a}{f})^k - \frac{k}{2}(\frac{a}{f})^{k-1}\right] \bmod p^N\mathbb{Z}_p$. On a la même congruence en

remplaçant a par d. De ces deux congruences résultent la congruence

$$\Delta_C(1-k,\chi_{a,f}) \equiv -\frac{f^{k-1}}{k}\left[\left(\frac{a}{f}\right)^k - \frac{k}{2}\left(\frac{a}{f}\right)^{k-1}\right] + C^k\,\frac{f^{k-1}}{k}\left[\left(\frac{d}{f}\right)^k - \frac{k}{2}\left(\frac{d}{f}\right)^{k-1}\right] \bmod p^N\mathbb{Z}_p \quad \text{soit}$$

$$\Delta_C(1-k,\chi_{a,f}) \equiv \left(\frac{a^{k-1}}{2} - C^k\,\frac{d^{k-1}}{2}\right) - \left(\frac{a^k}{fk} - C^k\,\frac{d^k}{fk}\right) \bmod p^N\mathbb{Z}_p .$$

D'autre part on a $Cd \equiv a \bmod f$ donc $(Cd)^{k-1} \equiv a^{k-1} \bmod f$; comme, par hypothèse, p^{N+1} divise f, on en déduit $\frac{a^{k-1}}{2} - C^k\frac{d^{k-1}}{2} \equiv a^{k-1}\left(\frac{1-C}{2}\right) \bmod p^N\mathbb{Z}_p$. Enfin l'hypothèse $p^n\,\frac{B_k(X)}{k} \in p^N\mathbb{Z}_p[X]$ implique $\frac{f}{k} \in p^N\mathbb{Z}_p$ puisque le coefficient de X^k dans $B_k(X)$ est 1. Posons $Cd = a+r$; l'entier r est dans $f\mathbb{Z}$ et l'on a $\frac{(Cd)^k - a^k}{fk} = \frac{ka^{k-1}r}{fk} + \frac{r^2}{fk}z$ pour un z dans $\mathbb{Z}$. De $\frac{f}{k} \in p^N\mathbb{Z}_p$ on tire $\frac{r^2}{fk} \in p^N\mathbb{Z}_p$ et donc $\frac{(Cd)^k - a^k}{fk} \equiv \frac{a^{k-1}r}{f} \bmod p^N\mathbb{Z}_p$ soit $\frac{(Cd)^k - a^k}{fk} \equiv a^{k-1}\,\frac{Cd-a}{f} \bmod p^N\mathbb{Z}_p$. En regroupant ces congruences, on obtient $\Delta_C(1-k,\chi_{a,f}) \equiv a^{k-1}\left(\frac{Cd-a}{f} - \frac{C-1}{2}\right) \bmod p^N\mathbb{Z}_p$ qui est ce qu'on cherchait.

3) En juxtaposant les congruences obtenues en 1) et 2) on obtient

$$\Delta_C(1-k,\chi_{a,f}) \equiv \Delta_C(0,\chi_{a,f}\,\delta) \bmod p^N\,\mathbb{Z}_p$$

ce qui achève la démonstration de notre lemme.

Revenons maintenant à la démonstration du théorème 1.1. On reprend les notations de ce théorème. Les ϵ_i étant périodiques, il existe un entier $K \geq 0$ tel que, pour tout x de $\mathbb{Z}$ et tout $i=1,\ldots,t$, on ait $p^K\epsilon_i(x) \in \mathbb{Z}_p$. Pour chaque i, notons δ_i l'application de $\mathbb{Z}$ dans $\mathbb{Z}_p$ définie pour tout x de $\mathbb{Z}$ par $\delta_i(x) = y^{k_i-1}$ où y est l'entier congru à x modulo p^K et compris entre 1 et p^K ; les δ_i sont donc périodiques de périodes p^K et vérifient $\delta_i(x) \equiv x^{k_i-1} \bmod p^K\mathbb{Z}_p$.

Soit C un entier positif premier aux périodes des ϵ_i et à p. Le lemme 1.5 montre que $\Delta_C(0,p^K\epsilon_i\delta_i) \equiv \Delta_C(1-k_i,p^K\epsilon_i) \bmod p^K\mathbb{Z}_p$ donc que $\Delta_C(0,\epsilon_i\delta_i) \equiv \Delta_C(1-k_i,\epsilon_i) \bmod \mathbb{Z}_p$. Posons $\epsilon = \sum_{i=1}^{t} \epsilon_i\delta_i$; il est clair que ϵ est une application périodique de $\mathbb{Z}$ dans $\mathbb{Q}_p$ et que C est premier à la période de ϵ. On a $\Delta_C(0,\epsilon) = \sum_{i=1}^{t} \Delta_C(0,\epsilon_i\delta_i)$ donc $\Delta_C(0,\epsilon) \equiv \sum_{i=1}^{t} \Delta_C(1-k_i,\epsilon_i) \bmod \mathbb{Z}_p$. Enfin l'hypothèse $\sum_{i=1}^{t} \epsilon_i(x)\,x^{k_i-1} \in \mathbb{Z}_p$ montre que les valeurs de ϵ sont dans $\mathbb{Z}_p$ donc le lemme

1.4 montre que $\Delta_C(0,\epsilon)$ est dans $\mathbb{Z}_p$. On en déduit que $\sum_{i=1}^{t} \Delta_C(1-k_i, \epsilon_i)$ est dans $\mathbb{Z}_p$ ce qui est l'assertion du théorème.

Montrons comment ce théorème 1.1 permet de retrouver deux résultats classiques de Kummer. On note ζ la fonction zêta de Riemann, c'est-à-dire avec le vocabulaire du § 0, la fonction zêta de Hurwitz associée à 1 ; on a :

PROPOSITION 1.6. 1) <u>Si</u> $p-1$ <u>ne divise pas</u> $k \geq 1$, <u>alors</u> $\zeta(1-k)$ <u>est</u> p-<u>entier</u>.

2) <u>Si</u> $p-1$ <u>ne divise pas</u> $k > 1$, <u>si</u> $k' > 1$ <u>et si</u> $k \equiv k' \bmod (p-1)$, <u>alors</u> $\zeta(1-k) \equiv \zeta(1-k') \bmod p\mathbb{Z}_p$.

<u>Démonstration</u>. 1) On prend $t=1$, $\epsilon_1=1$ et $k_1=k$ dans le théorème 1.1 ; pour tout entier C positif et premier à p, on a $\Delta_C(1-k,\epsilon_1) = (1-C^k)\,\zeta(1-k)$. Comme pour tout x de $\mathbb{Z}$ on a $\epsilon_1(x)x^{k-1} = x^{k-1} \in \mathbb{Z}_p$, le théorème permet d'affirmer que $(1-C^k)\,\zeta(1-k)$ est p-entier. Choisissons pour C un entier dont la classe modulo p engendre le groupe multiplicatif du corps à p éléments ; pour ce C la quantité $1-C^k$ est une p-unité donc $\zeta(1-k)$ est p entier.

2) On prend $t=2$, $\epsilon_1=1$, $\epsilon_2=-1$, $k_1=k$ et $k_2=k'$ dans le théorème 1.1 ; de plus on suppose $k \leq k'$. Pour tout entier C positif et premier à p on a

$$\Delta_C(1-k,\epsilon_1) + \Delta_C(1-k',\epsilon_2) = (1-C^k)\,\zeta(1-k) - (1-C^{k'})\,\zeta(1-k').$$

Les hypothèses $k \neq 1$ et $k \equiv k' \bmod (p-1)$ impliquent que $\epsilon_1(x)x^{k-1} + \epsilon_2(x)x^{k'-1} = x^{k-1}(1-x^{k'-k})$ est dans $p\mathbb{Z}_p$ pour tout x de $\mathbb{Z}$. Le théorème permet donc d'affirmer que $(1-C^k)\,\zeta(1-k) - (1-C^{k'})\,\zeta(1-k')$ est dans $p\mathbb{Z}_p$; comme $p-1$ divise $k-k'$ on a $1-C^{k'} \equiv 1-C^k \bmod p$, donc $(1-C^k)[\zeta(1-k)-\zeta(1-k')]$ est dans $p\mathbb{Z}_p$.

On achève la démonstration comme au point 1).

REMARQUE 1.7. On connaît en fait des résultats plus précis que ceux de la proposition 1.6 ; par exemple on sait que $\zeta(1-k)$ est p entier si et seulement si $p-1$ ne divise pas $k \geq 1$; on sait aussi que si $p-1$ ne divise pas $k > 1$, si $k' > 1$ et si $k \equiv k' \bmod (p-1)p^N$, alors $(1-p^{k-1})\zeta(1-k) \equiv (1-p^{k'-1})\,\zeta(1-k') \bmod p^{N+1}\mathbb{Z}_p$.
Nous reviendrons sur ce type de résultat à la fin du § 7 (remarque 7.16).

§ 2. GENERALITES SUR LES MESURES p-ADIQUES.

Soit X un espace topologique compact et totalement discontinu et soit R l'anneau des entiers d'une extension finie de $\mathbb{Q}_p$. On note respectivement $\mathrm{loc}(X,R)$ et $\mathrm{Cont}(X,R)$ l'espace des applications localement constantes et l'espace des applications continues de X dans R. Dans les paragraphes suivants X sera $\hat{\mathbb{Z}}$ ou $\mathbb{Z}_p$.

DEFINITION 2.1. <u>On appelle mesure sur</u> X <u>à valeur dans</u> R <u>toute application</u> R-<u>linéaire de</u> $\mathrm{Cont}(X,R)$ <u>dans</u> R.

REMARQUE 2.2. Si l'on munit $\mathrm{Cont}(X,R)$ de la topologie de la convergence uniforme (i.e. pour un $f\in\mathrm{Cont}(X,R)$, les $V_\epsilon(f)=\{g\in\mathrm{Cont}(X,R),\ \sup_{x\in X}|f(x)-g(x)|<\epsilon\}$ où $|\ |$ est la valeur absolue dans R décrivent un système fondamental de voisinages de f lorsque ϵ décrit les réels positifs), alors toute mesure au sens précédent est une application continue de $\mathrm{Cont}(X,R)$ dans R : en effet, il suffit clairement de montrer la continuité en 0 ; soit p^nR un voisinage de 0 dans R, il existe un $\epsilon>0$ tel que $f\in V_\epsilon(0)$ implique $f(x)\in p^nR$ pour tout x de R ; pour un tel f on a $f=p^ng$ avec $g\in\mathrm{Cont}(X,R)$; par linéarité, l'image de f par une mesure est donc le produit de p^n par l'image de g donc est dans p^nR ce qui montre la continuité de la mesure.

Si μ est une mesure sur X à valeurs dans R et si f est dans $\mathrm{Cont}(X,R)$ on notera souvent $\int_X f(x)\,d\mu(x)$ l'image $\mu(f)$ de f par μ. Nous aurons besoin de la proposition suivante :

PROPOSITION 2.3. <u>Si</u> μ <u>est une application</u> R-<u>linéaire de</u> $\mathrm{loc}(X,R)$ <u>dans</u> R, <u>il existe une mesure sur</u> X <u>à valeurs dans</u> R <u>et une seule qui prolonge</u> μ ; <u>nous la noterons encore</u> μ.

<u>Démonstration.</u> Nous aurons besoin du lemme suivant :

LEMME 2.4. <u>On suppose toujours que</u> $\mathrm{Cont}(X,R)$ <u>est muni de la topologie de la convergence uniforme définie dans la remarque 2.2. Tout</u> f <u>de</u> $\mathrm{Cont}(X,R)$ <u>est limite d'une suite d'éléments de</u> $\mathrm{loc}(X,R)$.

<u>Démonstration.</u> Soit $f \in \mathrm{Cont}(X,R)$; pour tout $n > 0$, on choisit un système $r(1;n), \ldots, r(t_n;n)$ d'éléments de R représentant les classes de R/p^nR. Pour chaque n on définit f_n en posant, pour tout x de X, $f_n(x) = r(i;n)$ si $f(x) \equiv r(i;n) \bmod p^nR$. Il est clair que les f_n appartiennent à $\mathrm{loc}(X,R)$ et convergent vers f lorsque n tend vers l'infini.

Revenons à notre démonstration. Soit f un élément de $\mathrm{Cont}(X,R)$ et $(f_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathrm{loc}(X,R)$ qui converge vers f. Un raisonnement analogue à celui fait dans la remarque 2.2 montre que la suite des $\mu(f_n)$ est une suite de Cauchy dans R. On vérifie que sa limite ne dépend que de f et pas du choix des f_n et on note $\mu(f)$ cette limite. Il est clair que l'application f donne $\mu(f)$ est une application R-linéaire de $\mathrm{Cont}(X,R)$ dans R, i.e. que μ est une mesure de X dans R. Il est clair que la restriction de cette mesure à $\mathrm{loc}(X,R)$ est μ. Enfin l'unicité de notre prolongement résulte de la remarque 2.2.

Soit α un élément de $\mathrm{Cont}(X,R)$; la multiplication par α est une application R-linéaire m_α de $\mathrm{Cont}(X,R)$ dans lui-même. En conséquence, si μ est une mesure sur X à valeurs dans R, la composée $\mu \circ m_\alpha$ est aussi une mesure sur X à valeurs dans R ; on la note $\alpha\mu$ et on dit que c'est la mesure de densité α par rapport à μ. Autrement dit, on pose la définition suivante :

DEFINITION 2.5. <u>Soit</u> μ <u>une mesure sur</u> X <u>à valeurs dans</u> R <u>et</u> α <u>un élément de</u> Cont(X,R). <u>La mesure</u> $\alpha\mu$ <u>de densité</u> α <u>par rapport à</u> μ <u>est définie par</u> $\int_X f(x)\,d(\alpha\mu)(x) = \int_X f(x)\,\alpha(x)\,d\mu(x)$ <u>pour tout</u> f <u>de</u> Cont(X,R).

REMARQUE 2.6. Soit μ une mesure sur X à valeurs dans R et soit S l'anneau des entiers d'une extension finie du corps des fractions de R. La mesure μ se prolonge uniquement en une mesure μ^S à valeurs dans S de la manière suivante : on choisit une base $s_1,\dots,s_n$ de S sur R, on décompose tout $\epsilon \in \mathrm{Cont}(X,S)$ en $\epsilon = \sum_{i=1}^{n} \epsilon_i s_i$ avec $\epsilon_i \in \mathrm{Cont}(X,R)$ et on pose $\mu^S(\epsilon) = \sum_{i=1}^{n} \mu(\epsilon_i) s_i$; il est clair que μ^S est une mesure à valeurs dans S indépendante du choix des s_i. Dans la suite nous écrirons par abus μ à la place de μ^S.

§ 3. LES MESURES μ_C, $\mu_{C,\alpha}$, ν_C ET $\nu_{C,\alpha}$.

Pour chaque C de $\hat{\mathbb{Z}}^*$, nous allons définir une mesure μ_C sur $\hat{\mathbb{Z}}$ et une mesure ν_C sur $\mathbb{Z}_p$ à valeurs dans l'anneau R des entiers d'une extension finie de $\mathbb{Q}_p$. Nous construirons d'abord μ_C.

On sait que $\hat{\mathbb{Z}}$ s'identifie canoniquement au produit $\prod_{\ell \in P} \mathbb{Z}_\ell$ où P désigne l'ensemble des nombres premiers ; pour tout z de $\hat{\mathbb{Z}}$ et tout ℓ de P on notera z_ℓ l'élément de $\mathbb{Z}_\ell$ tel que z s'identifie à $(z_\ell)_{\ell \in P}$; on dira que z_ℓ est la ℓ-composante de z. Rappelons le point suivant :

LEMME 3.1. <u>Soit ϵ une application localement constante de $\hat{\mathbb{Z}}$ dans un ensemble V. Il existe un entier naturel f tel que ϵ soit constante sur les classes modulo $f\hat{\mathbb{Z}}$ et la restriction $\epsilon_{|\mathbb{Z}}$ de ϵ à $\mathbb{Z}$ est une application périodique dont la période divise f.</u>

<u>Démonstration</u>. Pour chaque x de $\hat{\mathbb{Z}}$, il existe un entier f_x tel que la restriction de ϵ à $x+f_x\hat{\mathbb{Z}}$ est constante. On a $\hat{\mathbb{Z}} = \bigcup_{x\in\hat{\mathbb{Z}}} (x+f_x\hat{\mathbb{Z}})$; puisque $\hat{\mathbb{Z}}$ est compact, il existe $x_1,\ldots,x_n$ dans $\hat{\mathbb{Z}}$ tels que $\hat{\mathbb{Z}} = \bigcup_{i=1}^{n} (x_i+f_{x_i}\hat{\mathbb{Z}})$. Soit f un multiple commun des f_{x_i}, l'application ϵ est constante sur chaque classe modulo $f\hat{\mathbb{Z}}$ donc $\epsilon_{|\mathbb{Z}}$ est périodique et sa période divise f.

Ce lemme permet de poser la définition suivante :

DEFINITION 3.2. <u>Soit V un espace vectoriel sur $\mathbb{Q}$ et ϵ une application localement constante de $\hat{\mathbb{Z}}$ dans V. Pour tout entier $k \geq 1$ on définit</u> $L(1-k,\epsilon)$

comme l'élément de V égal à $L(1-k,\epsilon_{|\mathbb{Z}})$ (ce dernier élément ayant été défini à la fin du § 0).

Nous serons intéressés par le cas où V est une extension finie de $\mathbb{Q}_p$, c'est-à-dire que V sera un $\mathbb{Q}_p$-espace vectoriel ; nous poserons alors :

DEFINITION 3.3. *Soit* V *un espace vectoriel sur* $\mathbb{Q}_p$ *et* C *un élément de* $\hat{\mathbb{Z}}$. *Pour toute application localement constante* ϵ *de* $\hat{\mathbb{Z}}$ *dans* V *et tout entier* $k \geq 1$, *on pose* $\Delta_C(1-k,\epsilon) = L(1-k,\epsilon_C) - C_p^k L(1-k,\epsilon_C)$ *où* ϵ_C *est l'application (localement constante) de* $\hat{\mathbb{Z}}$ *dans* V *définie par* $\epsilon_C(x) = \epsilon(Cx)$ *pour tout* x *de* $\hat{\mathbb{Z}}$.

Du théorème 1.1 on déduit le théorème suivant :

THEOREME 3.4. *Soient* $\epsilon_1,\ldots,\epsilon_t$ *des applications localement constantes de* $\hat{\mathbb{Z}}$ *dans* $\mathbb{Q}_p$ *et* $k_1,\ldots,k_t$ *des entiers strictement positifs. On suppose que, pour tout* x *de* $\hat{\mathbb{Z}}$, *la somme* $\sum_{i=1}^{t} \epsilon_i(x)\, x_p^{k_i-1}$ *est dans* $\mathbb{Z}_p$. *Alors, pour tout* C *de* $\hat{\mathbb{Z}}^*$, *la somme* $\sum_{i=1}^{t} \Delta_C(1-k_i,\epsilon_i)$ *est dans* $\mathbb{Z}_p$.

Démonstration. Fixons un $C \in \hat{\mathbb{Z}}^*$. Les $L(1-k_i,\epsilon_{i,C})$ étant, pour $i=1,\ldots,t$, dans $\mathbb{Q}_p$ il existe un entier $N>0$ tel que $L(1-k_i,\epsilon_{i,C}) \in p^{-N}\mathbb{Z}_p$ pour tout i. Notons f un entier naturel tel que les ϵ_i sont constants sur les classes modulo $f\hat{\mathbb{Z}}$ (l'existence de f est assurée par le lemme 3.1). Désignons enfin par D un entier naturel congru à C modulo $fp^N\hat{\mathbb{Z}}$. On a $\epsilon_{i,C} = \epsilon_{i,D}$, puisque $C \equiv D \bmod f\hat{\mathbb{Z}}$, donc $L(1-k_i,\epsilon_{i,C}) = L(1-k_i,\epsilon_{i,D})$; de plus on a $C_p^k L(i-k_i,\epsilon_{i,C}) \equiv D^k L(1-k_i,\epsilon_{i,C}) \bmod \mathbb{Z}_p$ puisque $C_p \equiv D \bmod p^N\mathbb{Z}_p$, donc on a $\Delta_C(1-k_i,\epsilon_{i,C}) \equiv \Delta_D(1-k_i,\epsilon_{i,D}) \bmod \mathbb{Z}_p$. Mais C étant dans $\hat{\mathbb{Z}}^*$, la congruence $C \equiv D \bmod fp^N$ implique que $(D,fp)=1$, donc D est premier aux périodes des $\epsilon_{i|\mathbb{Z}}$ et à p. Par définition $\Delta_D(1-k_i,\epsilon_{i,D}) = \Delta_D(1-k_i,\epsilon_{i|\mathbb{Z},D})$ donc le théorème 1.1 montre que $\sum_{i=1}^{t} \Delta_D(1-k_i,\epsilon_{i,D}) \in \mathbb{Z}_p$; en conséquence $\sum_{i=1}^{t} \Delta_C(1-k_i,\epsilon_{i,C}) \in \mathbb{Z}_p$. C.Q.F.D.

De la même manière que l'on a démontré les corollaires 1.2 et 1.3 du théorème 1.1, on démontre le corollaire suivant de notre théorème :

COROLLAIRE 3.5. *Soit* V *un espace vectoriel de dimension finie sur* $\mathbb{Q}_p$ *et* L *un sous-*$\mathbb{Z}_p$*-module libre de* V *tel que* $\mathbb{Q}_p L = V$. *Soient* $\epsilon_1, \ldots, \epsilon_t$ *des applications localement constantes de* $\hat{\mathbb{Z}}$ *dans* V *et* $k_1, \ldots, k_t$ *des entiers strictement positifs. On suppose que, pour tout* x *de* $\hat{\mathbb{Z}}$, *la somme* $\sum_{i=1}^{t} \epsilon_i(x) x_p^{k_i - 1}$ *est dans* $p^n L$ *pour un* $n \geq 0$. *Alors, pour tout* C *de* $\hat{\mathbb{Z}}^*$, *la somme* $\sum_{i=1}^{t} \Delta_C(1-k_i, \epsilon_i)$ *est dans* $p^n L$.

Appliquons ce corollaire 3.5 au cas où V est une extension finie de $\mathbb{Q}_p$, où L est l'anneau des entiers R de V, où $t=1$ et où ϵ est à valeur dans R ; pour n'importe quel $k \geq 1$, on a bien $\epsilon(x) x_p^{k-1} \in R$ donc $\Delta_C(1-k, \epsilon)$ est dans R pour tout C de $\hat{\mathbb{Z}}^*$. Pour C fixé dans $\hat{\mathbb{Z}}^*$ et $k \geq 1$ fixé, l'application qui à ϵ associe $\Delta_C(1-k, \epsilon)$ est donc une application R linéaire de $\mathrm{loc}(\hat{\mathbb{Z}}, R)$ dans R. La proposition 2.3 permet alors d'affirmer qu'il existe une mesure et une seule sur $\hat{\mathbb{Z}}$ à valeur dans R dont la restriction à $\mathrm{loc}(\hat{\mathbb{Z}}, R)$ est l'application qui à ϵ associe $\Delta_C(1-k, \epsilon)$; nous notons $\mu_{C,k}$ cette mesure. Comme nous serons particulièrement intéressés par le cas $k=1$, nous posons la définition suivante :

DEFINITION 3.6. *Pour tout* $C \in \hat{\mathbb{Z}}^*$, *nous notons* μ_C *la mesure sur* $\hat{\mathbb{Z}}$ *à valeurs dans* R *dont la valeur* $\int_{\hat{\mathbb{Z}}} \epsilon \, d\mu_C$ *en un* ϵ *de* $\mathrm{loc}(\hat{\mathbb{Z}}, R)$ *est* $\Delta_C(0, \epsilon)$.

REMARQUE 3.7. Dans la notation μ_C l'anneau R n'apparait pas. Cela est justifié par le fait suivant : si S est l'anneau des entiers d'une extension finie du corps des fractions de R et si μ'_C est la mesure définie comme μ_C en remplaçant R par S, alors avec les notations de la remarque 2.6 on a $\mu'_C = \mu_C^S$; comme on a convenu dans cette remarque 2.5 de faire, pour toute mesure μ à valeur dans R et tout S contenant R, l'abus de notation $\mu = \mu^S$, il est normal de ne pas faire intervenir R dans la notation μ_C.

Le procédé suivant permet de construire à partir d'une mesure sur $\hat{\mathbb{Z}}$ une mesure sur $\mathbb{Z}_p$. Soit φ_p la projection canonique de $\hat{\mathbb{Z}}$ sur $\mathbb{Z}_p$; la composition avec φ_p est une application R linéaire Φ_p de $\mathrm{Cont}(\mathbb{Z}_p, R)$ dans

$\mathrm{Cont}(\hat{\mathbb{Z}},R)$. En conséquence, si μ est une mesure sur $\hat{\mathbb{Z}}$ à valeurs dans R, la composée $\mu\circ\Phi_p$ est une mesure sur $\mathbb{Z}_p$ à valeurs dans R que nous appelons la mesure image de μ par φ_p. Autrement dit, on pose la définition suivante :

DEFINITION 3.8. Soit μ une mesure sur $\hat{\mathbb{Z}}$ à valeurs dans R. La mesure ν image de μ par la projection de $\hat{\mathbb{Z}}$ sur $\mathbb{Z}_p$ est la mesure sur $\mathbb{Z}_p$ à valeurs dans R définie par $\int_{\mathbb{Z}_p} f(x)d\nu(x) = \int_{\hat{\mathbb{Z}}} f(y_p)\, d\mu(y)$ pour tout f de $\mathrm{Cont}(\mathbb{Z}_p,R)$.

Dans la suite nous adopterons les notations suivantes :

NOTATIONS 3.9. Si $C\in\hat{\mathbb{Z}}^*$ et $\alpha\in\mathrm{Cont}(\hat{\mathbb{Z}},R)$ nous notons $\mu_{C,\alpha}$ la mesure sur $\hat{\mathbb{Z}}$ à valeurs dans R de densité α par rapport à μ_C et $\nu_{C,\alpha}$ la mesure sur $\mathbb{Z}_p$ à valeurs dans R image de $\mu_{C,\alpha}$ par la projection de $\hat{\mathbb{Z}}$ sur $\mathbb{Z}_p$. On a donc $\mu_C = \mu_{C,1}$; de même nous noterons souvent ν_C à la place de $\nu_{C,1}$.

Terminons ce paragraphe par un calcul qui nous sera utile plus loin. On a :

PROPOSITION 3.10. Soit $\varepsilon\in\mathrm{loc}(\hat{\mathbb{Z}},R)$ et $k\geq 1$ un entier. On définit $f\in\mathrm{Cont}(\hat{\mathbb{Z}},R)$ par $f(x)=x_p^{k-1}\,\varepsilon(x)$ pour tout x de $\hat{\mathbb{Z}}$. Alors, si $C\in\hat{\mathbb{Z}}^*$, on a :

$$\int_{\hat{\mathbb{Z}}} f(x)\,d\mu_C(x) = \Delta_C(1-k,\varepsilon).$$

Démonstration. Pour chaque entier $N\geq 0$, notons δ_N la fonction de $\hat{\mathbb{Z}}$ dans $\mathbb{Z}$ dont la valeur en un x de $\hat{\mathbb{Z}}$ est i^{k-1} où i est l'entier compris entre 1 et p^N qui est congru à x_p modulo $p^N\mathbb{Z}_p$. Les $\varepsilon\delta_N$ sont localement constantes et tendent vers f lorsque N tend vers l'infini, donc $\int_{\hat{\mathbb{Z}}} f(x)\,d\mu_C(x)$ est la limite quand N tend vers l'infini des $\int_{\hat{\mathbb{Z}}} \varepsilon(x)\,\delta_N(x)\,d\mu_C(x) = \Delta_C(0,\varepsilon\delta_N)$. Mais, pour tout $x\in\hat{\mathbb{Z}}$, la différence $(\varepsilon\,\delta_N)(x) - \varepsilon(x)\,x_p^{k-1}$ est dans $p^N R$, donc le corollaire 3.5 (appliqué avec $n=N$, $L=R$ et $V=$ corps des fractions de R) montre que $\Delta_C(0,\varepsilon\delta_N)-\Delta_C(1-k,\varepsilon)$ est dans $p^N R$. On en déduit que les $\Delta_C(0,\varepsilon\delta_N)$ convergent vers $\Delta_C(1-k,\varepsilon)$ lorsque N tend vers l'infini ce qui achève la démonstration.

§ 4. MESURES SUR $\mathbb{Z}_p$.

R est toujours l'anneau des entiers d'une extension finie de $\mathbb{Q}_p$. Le but de ce paragraphe est d'associer à chaque mesure sur $\mathbb{Z}_p$ à valeurs dans R une série formelle à coefficients dans R.

Rappelons que l'application qui à x de $\mathbb{Z}_p$ associe $\binom{x}{n} = \frac{x(x-1)\ldots(x-n+1)}{n!}$ est une application continue de $\mathbb{Z}_p$ dans lui-même (c'est clairement une application continue de $\mathbb{Z}_p$ dans $\mathbb{Q}_p$ et elle prend des valeurs entières pour tout $x \in \mathbb{N}$). On a :

THEOREME 4.1 (Mahler). *Soit* f *une fonction continue de* $\mathbb{Z}_p$ *dans* R ; *il existe une suite* $(a_n)_{n\geq 0}$ *d'éléments de* R *qui tend vers* 0 *quand* n *tend vers l'infini telle que* $f(x) = \sum_{n\geq 0} a_n\binom{x}{n}$ *pour tout* x *de* $\mathbb{Z}_p$. *L'application qui à* f *associe la suite* $(a_n)_{n\geq 0}$ *est une bijection de* $\mathrm{Cont}(\mathbb{Z}_p, R)$ *sur l'ensemble des suites de* R *qui tendent vers* 0 *quand* n *tend vers l'infini.*

Démonstration (Katz). R étant un $\mathbb{Z}_p$-module libre de dimension finie, il suffit de démontrer le théorème pour $R = \mathbb{Z}_p$ (si $r_1, \ldots, r_n$ est une base de R sur $\mathbb{Z}_p$, on pose $f = \sum_{i=1}^{n} f_i r_i$ avec $f_i \in \mathrm{Cont}(\mathbb{Z}_p, \mathbb{Z}_p)$ et le théorème pour les f_i implique le théorème pour f). Nous aurons besoin du lemme suivant :

LEMME 4.2. *Soit* $\mathbb{F}_p$ *le corps à* p *éléments muni de la topologie discrète et* g *une application continue de* $\mathbb{Z}_p$ *dans* $\mathbb{F}_p$. *Il existe une suite* $(a_n)_{n\geq 0}$ *d'éléments de* $\mathbb{Z}_p$ *presque tous nuls telle que* $g(x)$ *est le résidu modulo* $p\mathbb{Z}_p$ *de* $\sum_{n\geq 0} a_n\binom{x}{n}$.

<u>Démonstration</u>. La fonction g est localement constante, donc il existe un $N > 0$ tel que g soit constante sur les classes modulo $p^N\mathbb{Z}_p$. Notons $\mathfrak{F}_N$ l'ensemble des applications de $\mathbb{Z}_p$ dans $\mathbb{F}_p$ qui sont constantes sur les classes modulo $p^N\mathbb{Z}_p$; $\mathfrak{F}_N$ est un espace vectoriel sur $\mathbb{F}_p$ de dimension p^N. Désignons par T une indéterminée ; pour tout entier naturel X on a, dans l'anneau de polynôme $\mathbb{Z}[T]$, l'égalité $(1+T)^{X+p^N} = (1+T)^X(1+T)^{p^N}$. En développant cette égalité et en tenant compte de la congruence $(1+T)^{p^N} \equiv 1+T^{p^N} \bmod p\mathbb{Z}[T]$ on voit que $\binom{X+p^N}{i} \equiv \binom{X}{i} \bmod p\mathbb{Z}$ pour $i=0,\ldots,p^N-1$. Ces dernières congruences étant valables pour tout entier naturel X, elles impliquent les congruences $\binom{x+p^N}{i} \equiv \binom{x}{i} \bmod p\mathbb{Z}_p$ pour tout x de $\mathbb{Z}_p$ et tout $i = 0,\ldots,p^N-1$. En conséquence, si l'on note φ_i l'application de $\mathbb{Z}_p$ dans $\mathbb{F}_p$ qui à x de $\mathbb{Z}_p$ associe la classe de $\binom{x}{i}$ modulo $p\mathbb{Z}_p$, les applications $\varphi_o,\ldots,\varphi_{p^N-1}$ sont des éléments de $\mathfrak{F}_n$. Ces applications sont linéairement indépendantes sur $\mathbb{F}_p$: en effet, supposons qu'il existe $\alpha_o,\ldots,\alpha_{p^N-1}$ dans $\mathbb{F}_p$ tel que $\sum_{i=o}^{p^N-1} \alpha_i\varphi_i(x) = 0$ pour tout x de $\mathbb{Z}_p$; en faisant $x = 0$, on voit que $\alpha_o = 0$ (puisque $\varphi_i(0) = 0$ si $i > 0$ et $\varphi(0) = 1$) ; de même en faisant $x = 1,2,\ldots,p^N-1$ on voit successivement que $\alpha_1, \alpha_2,\ldots,\alpha_{p^N-1}$ sont nuls. Le système $\varphi_o,\ldots,\varphi_{p^N-1}$ est donc une base de $\mathfrak{F}_N$ sur $\mathbb{F}_p$ et donc il existe $\alpha_o,\ldots,\alpha_{p^N-1}$ dans $\mathbb{F}_p$ tel que $g = \sum_{i=o}^{p^N-1} \alpha_i\varphi_i$. Pour $n = 0,\ldots, p^N-1$ choisissons un a_n dans $\mathbb{Z}_p$ dont la classe modulo $p\mathbb{Z}_p$ est α_n et pour $n \geq p^N$ posons $a_n = 0$; il est clair que la suite $(a_n)_{n\in\mathbb{N}}$ répond à notre question.

Revenons à la démonstration du théorème. Rappelons que nous nous sommes ramenés au cas $R = \mathbb{Z}_p$. Posons $f = f_o$ et notons g_o le résidu de f_o modulo $p\mathbb{Z}_p$. Le lemme 4.2 affirme l'existence d'une suite $(a_n(0))_{n\in\mathbb{N}}$ d'éléments de $\mathbb{Z}_p$ presque tous nuls tels que $g_o(x)$ soit le résidu modulo $p\mathbb{Z}_p$ de la somme $\sum_{n\geq 0} a_n(0)\binom{x}{n}$ que nous notons $S_o(x)$. La différence $f_o(x) - S_o(x)$ est dans $p\mathbb{Z}_p$; nous posons $f_1(x) = \frac{f_o(x)-S_o(x)}{p}$. En partant de f_1 à la place de f_o, on construit les $(a_n(1))_{n\in\mathbb{N}}$, S_1 et f_2 comme on a construit les $(a_n(0))_{n\in\mathbb{N}}$, S_o et f_1 ; en itérant le procédé on construit pour tout $i\in\mathbb{N}$ une suite $(a_n(i))_{n\in\mathbb{N}}$ d'éléments de $\mathbb{Z}_p$ presque tous nuls. Enfin, pour tout $n \in \mathbb{N}$, on pose $a_n = \sum_{i=0}^{\infty} a_n(i)p^i$. Soit $A_0 > 0$ fixé ; les $a_n(i)$ étant presque tous nuls pour i fixé, il existe un N_0 tel que $n \geq N_0$ implique $a_n(i) = 0$ pour tout $i \leq A_0$; en conséquence pour $n \geq N_0$ l'élément a_n de $\mathbb{Z}_p$ est dans $p^{A_0}\mathbb{Z}_p$; cela signifie que la suite $(a_n)_{n\in\mathbb{N}}$ tend vers 0 quand N tend vers l'infini. On vérifie alors facilement que $f(x) = \sum_{n\geq 0} a_n\binom{x}{n}$ ce qui achève la première partie de la démonstration. Montrons l'unicité de la suite $(a_n)_{n\in\mathbb{N}}$ attachée à f ; il suffit clairement pour cela de voir que l'égalité $0 = \sum_{n\geq 0} a_n\binom{x}{n}$ pour tout x de $\mathbb{Z}_p$ implique $a_n = 0$ pour tout n ; supposons le contraire et désignons par n_0 le plus petit entier tel que $a_{n_0} \neq 0$; pour tout $n > n_0$ on a $\binom{n_0}{n} = 0$, donc on a $0 = a_{n_0}\binom{n_0}{n_0} = a_{n_0}$ d'où une contradiction qui prouve notre assertion et montre que l'application qui à f associe $(a_n)_{n\in\mathbb{N}}$ est injective. Enfin la surjectivité est évidente car, la suite $(a_n)_{n\in\mathbb{N}}$ tendant vers 0 quand n tend vers l'infini, la somme $\sum_{n\geq 0} a_n\binom{x}{n}$ converge pour tout x de $\mathbb{Z}_p$ et définit une fonction continue de x. Notre démonstration est donc achevée.

Revenons aux mesures sur $\mathbb{Z}_p$ à valeurs dans R. Nous posons la définition suivante :

DEFINITION 4.3. <u>Soit</u> ν <u>une mesure sur</u> $\mathbb{Z}_p$ <u>à valeurs dans</u> R. <u>La série formelle</u> $F_\nu(T) = \sum_{n\geq 0} b_n T^n$ <u>où</u> $b_n = \int_{\mathbb{Z}_p} \binom{x}{n} d\nu(x)$ <u>qui est à coefficients dans</u> R <u>est appelée "série formelle associée à</u> ν".

On a :

PROPOSITION 4.4. <u>L'application qui à une mesure</u> ν <u>sur</u> $\mathbb{Z}_p$ <u>à coefficients dans</u> R, <u>associe la série formelle</u> $F_\nu(T)$ <u>associée à</u> ν <u>est une bijection de l'ensemble des mesures sur</u> $\mathbb{Z}_p$ <u>à valeurs dans</u> R <u>sur l'anneau</u> R[[T]] <u>des séries formelles à coefficients dans</u> R.

<u>Démonstration</u>. Montrons l'injectivité de notre application. Soit ν une mesure sur $\mathbb{Z}_p$ à valeurs dans R et, pour tout $n \in \mathbb{N}$, soit $b_n = \int_{\mathbb{Z}_p} \binom{x}{n} d\nu(x)$.

Soit $f \in \mathrm{Cont}(\mathbb{Z}_p, R)$; d'après le théorème 4.1 (théorème de Mahler), il existe une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de R qui tend vers 0 quand n tend vers l'infini et telle que $f(x) = \lim_{N\to\infty} \sum_{n=0}^{N} a_n\binom{x}{n}$. De la remarque 2.2 on déduit que

$$\int_{\mathbb{Z}_p} f(x)\,d\nu(x) = \lim_{N\to\infty} \int_{\mathbb{Z}_p} \Big(\sum_{n=0}^{N} a_n\binom{x}{n}\Big)\,d\nu(x) = \lim_{N\to\infty} \Big(\sum_{n=0}^{N} a_n b_n\Big)\ ;$$

cela montre que ν est entièrement déterminée par les b_n ce qui prouve l'injectivité cherchée. Montrons maintenant la surjectivité ; soit $F(T) = \sum_{n\geq 0} b_n T^n$ une série formelle à coefficients dans R. Si $f \in \mathrm{Cont}(\mathbb{Z}_p, R)$ alors $f(x) = \sum_{n\geq 0} a_n\binom{x}{n}$ pour une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de R qui tend vers 0 quand n tend vers l'infini. Les b_n étant dans R, la série $\sum_{n\geq 0} a_n b_n$ est convergente. On vérifie sans difficulté que l'application de $\mathrm{Cont}(\mathbb{Z}_p, R)$ dans R qui à f associe $\sum_{n\geq 0} a_n b_n$ est une mesure sur $\mathbb{Z}_p$ à valeurs dans R et que la série associée à cette mesure est $F(T)$. Cela montre la surjectivité et achève la démonstration.

REMARQUE 4.5. Soit toujours ν une mesure sur $\mathbb{Z}_p$ à valeur dans R. Pour tout entier $n > 0$ et tout $i = 0, \ldots, p^n - 1$ on définit $\chi_{n,i} \in \mathrm{loc}(\mathbb{Z}_p, R)$ en posant $\chi_{n,i}(x) = 1$ si $x \equiv i$ modulo $p^n\mathbb{Z}_p$ et $\chi_{n,i}(x) = 0$ sinon. On note $a_{n,i} = \int_{\mathbb{Z}_p} \chi_{n,i}(x)\,d\nu(x)$; alors, en désignant par $\tilde{i}$ la classe de i dans $\mathbb{Z}/p^n\mathbb{Z}$, l'élément $\alpha_n = \sum_{i=0}^{p^n-1} a_{n,i}\cdot\tilde{i}$ est dans l'algèbre $R[\mathbb{Z}/p^n\mathbb{Z}]$; on vérifie sans difficulté que la famille des α_n pour n décrivant $\mathbb{N}$ définit un élément α de la limite projective $\varprojlim R[\mathbb{Z}/p^n\mathbb{Z}]$ (la flèche de $R[\mathbb{Z}/p^n\mathbb{Z}]$ vers $R[\mathbb{Z}/p^m\mathbb{Z}]$ étant induite par la surjection canonique de $\mathbb{Z}/p^n\mathbb{Z}$ vers $\mathbb{Z}/p^m\mathbb{Z}$). On vérifie facilement que l'application qui à ν associe α est une bijection de l'ensemble des mesures sur $\mathbb{Z}_p$ à valeurs dans R sur $\varprojlim R[\mathbb{Z}/p^n\mathbb{Z}]$. Montrons comment l'on peut retrouver la série $F_\nu(T)$ construite précédemment à partir de α. Définissons le polynôme $A_n(T)$ par $A_n(T) = \sum_{i=0}^{p^n-1} a_{n,i}(1+T)^i$; développons-le, il vient $A_n(T) = \sum_{j=0}^{p^n-1}\Big(\sum_{i=j}^{p^n-1}\binom{i}{j} a_{n,i}\Big)T^j$. Fixons j ; pour tout n, on a $\sum_{i=j}^{p^n-1}\binom{i}{j}\chi_{n,i}(x) \equiv \binom{x}{j}$ modulo $\frac{1}{j!}\,p^n\,\mathbb{Z}_p$ donc

$$\sum_{i=j}^{p^n-1} \binom{i}{j} a_{n,i} = \sum_{i=j}^{p^n-1} \binom{i}{j} \int_{\mathbb{Z}_p} \chi_{n,i}(x)\, d\nu(x) \equiv \int_{\mathbb{Z}_p} \binom{x}{j}\, d\nu(x) \text{ modulo } \frac{1}{j!}\, p^n \mathbb{Z}_p.$$

Cela prouve que, lorsque n tend vers l'infini, le $j^{\text{ième}}$ coefficient de $A_n(T)$ tend vers le $j^{\text{ième}}$ coefficient de la série $F_\nu(T)$.

§ 5. LA FONCTION Γ_ν.

ν est toujours une mesure sur $\mathbb{Z}_p$ à valeur dans R. Rappelons que le groupe $\mathbb{Z}_p^*$ est le produit direct, de son sous-groupe de torsion μ et de son sous-groupe $1+2p\mathbb{Z}_p$ (μ est le groupe des racines $p-1^{\text{ième}}$ de l'unité si $p \neq 2$ et $\mu = \pm 1$ si $p=2$) ; pour tout x de $\mathbb{Z}_p^*$ on définit $\omega(x) \in \mu$ et $<x> \in 1+2p\mathbb{Z}_p$ par l'égalité $x = \omega(x) <x>$; si x est un élément de $\mathbb{Z}_p$ qui n'est pas dans $\mathbb{Z}_p^*$ on pose $<x> = 0$. On rappelle que, si y est dans $1+2p\mathbb{Z}_p$, l'application de $\mathbb{Z}$ dans $1+2p\mathbb{Z}_p$ qui à $x \in \mathbb{Z}$ associe y^x se prolonge de manière unique en une application de $\mathbb{Z}_p$ dans $1+2p\mathbb{Z}_p$; pour tout $s \in \mathbb{Z}_p$, nous notons y^s l'image de s par cette application. On définit ainsi une structure de $\mathbb{Z}_p$-module sur $1+2p\mathbb{Z}_p$; celui-ci est libre de dimension 1 ; nous choisissons une fois pour toute un $\mathbb{Z}_p$ générateur γ de $1+2p\mathbb{Z}_p$.

Il est clair que l'application de $\mathbb{Z}_p$ dans $\mathbb{Z}_p$ qui à x de $\mathbb{Z}_p$ associe $<x>$ est continue ; on en déduit sans difficulté que, pour tout $s \in \mathbb{Z}_p$, l'application de $\mathbb{Z}_p$ dans $\mathbb{Z}_p$ qui à x associe $<x>^{-s}$ est continue (avec bien sûr $<x>^{-s} = 0$ si $<x> = 0$). On pose alors :

DEFINITION 5.1. <u>Pour tout</u> s <u>de</u> $\mathbb{Z}_p$ <u>et toute mesure</u> ν <u>sur</u> $\mathbb{Z}_p$ <u>à valeurs dans</u> R <u>on définit</u> $\Gamma_\nu(s)$ <u>par</u> $\Gamma_\nu(s) = \int_{\mathbb{Z}_p} <x>^{-s} \, d\nu(x)$.

Si $(a_n)_{n\in\mathbb{N}}$ est une suite d'éléments de R, la série $\sum_{n\geq 0} a_n(\gamma^{-s}-1)^n$ converge pour tout s de $\mathbb{Z}_p$ puisque $\gamma^{-s}-1$ est dans $2p\mathbb{Z}_p$; il est clair que cette série définit une fonction continue de s, nous poserons :

DEFINITION 5.2. <u>Une application</u> f <u>de</u> $\mathbb{Z}_p$ <u>dans</u> R <u>est appelée fonction d'Iwasawa si il existe une suite</u> $(a_n)_{n\in\mathbb{N}}$ <u>d'éléments de</u> R <u>telle que</u> $f(s) = \sum_{n\geq 0} a_n(\gamma^{-s}-1)^n$ <u>pour tout</u> s <u>de</u> $\mathbb{Z}_p$.

REMARQUE 5.3. Dans la définition précédente, la fonction f détermine les a_n de manière unique ; en effet, cela est une conséquence directe de l'assertion suivantes (que nous réutiliserons plus loin) : soit K le corps des fractions de R et $(a_n)_{n\in\mathbb{N}}$ une suite d'éléments de K telle que la série $\sum_{n\geq 0} a_n x^n$ converge dans un voisinage V de 0 ; si, pour tout x de V, la somme $\sum_{n\geq 0} a_n x^n$ est nulle alors $a_n=0$ pour tout $n\in\mathbb{N}$. Supposons cette assertion fausse et notons n_o le plus petit entier tel que $a_{n_o}\neq 0$; pour tout x de V différent de 0, on a $0 = a_{n_o} + x\sum_{n\geq n_o} a_n x^{n-n_o-1}$; la série $\sum_{n\geq n_o} a_n x^{n-n_o-1}$ converge sur un voisinage de 0 (éventuellement plus petit que V). Soit W un voisinage compact de 0 contenu dans V et sur lequel $\sum_{n\geq n_o} a_n x^{n-n_o-1}$ converge ; cette dernière somme est bornée sur W, donc lorsque $x\neq 0$ tend vers 0 en restant dans W, la quantité $x\sum_{n\geq n_o} a_n x^n$ tend vers 0 ce qui contredit l'égalité $0 = a_{n_o} + x\sum_{n\geq n_o} a_n x^{n-n_o-1}$ et démontre notre assertion.

On va montrer que la fonction qui à s associe $\Gamma_\nu(s)$ est une fonction d'Iwasawa. Pour cela désignons par α l'application de $\mathbb{Z}_p^*$ dans $\mathbb{Z}_p$ définie par $\langle x\rangle = \gamma^{\alpha(x)}$ pour tout $x\in\mathbb{Z}_p^*$; pour tout $f\in\mathrm{Cont}(\mathbb{Z}_p,R)$ on note f_α la fonction de $\mathbb{Z}_p$ dans R définie par $f_\alpha(x)=0$ si $x\notin\mathbb{Z}_p^*$ et $f_\alpha(x)=f(\alpha(x))$ si $x\in\mathbb{Z}_p^*$. La fonction f_α est dans $\mathrm{Cont}(\mathbb{Z}_p,R)$ et l'application ψ_α de $\mathrm{Cont}(\mathbb{Z}_p,R)$ dans lui-même qui envoie f sur f_α est une application R linéaire. En conséquence la composée $\nu\circ\psi_\alpha$ est une mesure sur $\mathbb{Z}_p$ à valeurs dans R que nous notons $\alpha_*\nu$. Autrement dit on pose la définition suivante :

DEFINITION 5.4. <u>Soit</u> ν <u>une mesure sur</u> $\mathbb{Z}_p$ <u>à valeurs dans</u> R. <u>La mesure</u>

$\alpha_* \nu$ sur $\mathbb{Z}_p$ à valeurs dans R est définie par $\int_{\mathbb{Z}_p} f(x)\, d(\alpha_*\nu)(x) = \int_{\mathbb{Z}_p} f_\alpha(x)\, d\nu(x)$ pour tout f de $\mathrm{Cont}(\mathbb{Z}_p, R)$ (la fonction f_α est définie ci-dessus).

On a alors :

PROPOSITION 5.5. *Pour tout* s *de* $\mathbb{Z}_p$, *on a* $\Gamma_\nu(s) = \int_{\mathbb{Z}_p} (\gamma^{-s})^x d(\alpha_*\nu)(x)$.

Démonstration. Soit $f \in \mathrm{Cont}(\mathbb{Z}_p, R)$ la fonction définie, pour tout x de $\mathbb{Z}_p$, par $f(x) = (\gamma^{-s})^x$. On a $f_\alpha(x) = \langle x\rangle^{-s}$ pour tout x, donc

$$\int_{\mathbb{Z}_p} (\gamma^{-s})^x\, d(\alpha_*\nu)(x) = \int_{\mathbb{Z}_p} \langle x\rangle^{-s}\, d\nu(x) = \Gamma_\nu(s) \qquad \text{C.Q.F.D.}$$

Enfin on a le lemme suivant :

LEMME 5.6. *Soit* ν *une mesure sur* $\mathbb{Z}_p$ *à valeurs dans* R *et* $F_\nu(T)$ *la série de* $R[[T]]$ *qui lui est attachée. Si* δ *est un élément de* $1+2p\mathbb{Z}_p$ *on a* $\int_{\mathbb{Z}_p} \delta^x\, d\nu(x) = F_\nu(\delta - 1)$.

Démonstration. Posons $\delta = 1+m$; alors m est dans $2p\mathbb{Z}_p$ et $\delta^x = (1+m)^x = \sum_{n\geq 0} m^n \binom{x}{n}$. On en déduit $\int_{\mathbb{Z}_p} \delta^x\, d\nu(x) = \sum_{n\geq 0} \left(m^n \int_{\mathbb{Z}_p} \binom{x}{n}\, d\nu(x)\right) = F_\nu(m)$ par définition de $F_\nu(T)$ et cela achève la démonstration.

Ce lemme 5.6 joint à la proposition précédente donne immédiatement le résultat suivant :

THEOREME 5.7. *Pour tout* s *de* $\mathbb{Z}_p$ *on a* $\Gamma_\nu(s) = F_{\alpha_*\nu}(\gamma^{-s}-1)$ *et donc la fonction* Γ_ν *est une fonction Iwasawa.*

REMARQUE 5.8. L'application α, donc la mesure $\alpha_*\nu$ dépendent du choix de γ ; cela explique que dans l'égalité $\Gamma_\nu(s) = F_{\alpha_*\nu}(\gamma^{-s}-1)$ l'élément γ intervienne à droite et pas à gauche.

§ 6. LES FONCTIONS L p-ADIQUES.

On note $\overline{\mathbb{Q}}$ la cloture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ et on choisit une fois pour toute un plongement de $\overline{\mathbb{Q}}$ dans la cloture algébrique $\overline{\mathbb{Q}}_p$ de $\mathbb{Q}_p$.

Nous ferons les conventions suivantes :

Si ϵ est un caractère modulo l'entier positif f (i.e. ϵ est un homéomorphisme de groupe de $(\mathbb{Z}/f\mathbb{Z})^*$ vers $\mathbb{C}^*$) on convient de prolonger ϵ à $\mathbb{Z}/f\mathbb{Z}$ tout entier en lui attribuant la valeur 0 sur les éléments de $\mathbb{Z}/f\mathbb{Z}$ qui ne sont pas dans $(\mathbb{Z}/f\mathbb{Z})^*$. En composant ϵ ainsi prolongé avec la projection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/f\mathbb{Z}$, on obtient une fonction périodique de $\mathbb{Z}$ dans $\mathbb{C}$ que nous notons encore ϵ. Le caractère ϵ étant identifié à cette fonction périodique sur $\mathbb{Z}$, on peut comme au § 0 définir la fonction $L(s,\epsilon)$ méromorphe sur $\mathbb{C}$ (pour $\mathrm{Re}(s) > 1$, on a donc $L(s,\epsilon) = \sum_{n\geq 0} \epsilon(n)\, n^{-s}$). D'autre part, les valeurs de ϵ sont des racines de l'unité dont l'ordre divise $\varphi(f)$; ces valeurs sont donc dans $\overline{\mathbb{Q}}$ et le plongement que nous avons choisi permet de les considérer comme étant dans $\overline{\mathbb{Q}}_p$.

Ceci fait, il est clair que ces valeurs sont même dans l'anneau des entiers R de l'extension finie $\mathbb{Q}_p(\epsilon)$ de $\mathbb{Q}_p$ obtenue en adjoignant à $\mathbb{Q}_p$ les valeurs de ϵ. En considérant ϵ comme étant à valeurs dans R et en le composant avec la projection canonique de $\hat{\mathbb{Z}}$ sur $\hat{\mathbb{Z}}/f\hat{\mathbb{Z}} = \mathbb{Z}/f\mathbb{Z}$, on obtient une fonction localement constante de $\hat{\mathbb{Z}}$ dans R que nous notons encore ϵ. En identifiant le caractère ϵ à cette fonction localement constante, on peut comme au § 3, définir pour tout $C \in \hat{\mathbb{Z}}^*$ la mesure $\nu_{C,\epsilon}$ et pour tout $C \in \hat{\mathbb{Z}}^*$ et tout entier $k \geq 1$ l'élément $\Delta_C(1-k,\epsilon)$.

Nous aurons aussi besoin de définir le produit de deux caractères ; si ϵ est un caractère modulo f et si ϵ' est une caractère modulo f', le produit $\epsilon\epsilon'$ est le caractère modulo le p.p.c.m. $[f,f']$ de f et f' qui pour tout x de $\mathbb{Z}$ premier à $[f,f']$ vaut $\epsilon\epsilon'(x) = \epsilon(x)\,\epsilon'(x)$; on a alors $\epsilon\epsilon'(x) = \epsilon(x)\,\epsilon'(x)$ pour tout x de $\mathbb{Z}$ puisque si x n'est pas premier à $[f,f']$ les deux membres de l'égalité sont 0. De même, l'inverse ϵ^{-1} de ϵ est le caractère modulo f tel que, pour tout x de $\mathbb{Z}$ premier à f, on ait $\epsilon^{-1}(x) = \epsilon(x)^{-1}$. Enfin, définissons le caractère ω qui jouera dans la suite un rôle fondamental : ω est le caractère modulo p si $p \neq 2$ et modulo 4 si $p = 2$ tel que, pour tout x de $\mathbb{Z}$ premier à p, $\omega(x)$ est la racine $(p-1)^{\text{ième}}$ de l'unité de $\bar{\mathbb{Q}}$ dont l'image dans $\bar{\mathbb{Q}}_p$ est congrue à x modulo $p\mathbb{Z}_p$ si $p \neq 2$ et $\omega(x)$ est $+1$ ou -1 suivant que x est congru à $+1$ ou -1 modulo 4 si $p = 2$. Nous posons la définition suivante :

DEFINITION 6.1. <u>Soit</u> ϵ <u>un caractère modulo</u> f <u>et</u> C <u>un élément de</u> $\hat{\mathbb{Z}}^*$. <u>Pour tout</u> s <u>de</u> $\mathbb{Z}_p$, <u>on pose</u> $L_p(s,\epsilon,C) = \Gamma_{\nu_{C,\epsilon\omega^{-1}}}(s)$.

Le théorème 5.7 montre que $L_p(s,\epsilon,C)$ est une fonction d'Iwasawa. On a :

PROPOSITION 6.2. <u>Soit</u> ϵ <u>un caractère modulo</u> f <u>et</u> C <u>un élément de</u> $\hat{\mathbb{Z}}^*$; <u>pour tout entier</u> $k \geq 1$ <u>on a</u> $L_p(1-k,\epsilon,C) = (1-C_p^k\,\epsilon(C)\,\omega^{-k}(C))\,L(1-k,\epsilon\omega^{-k})$.

Avant de démontrer cette proposition, faisons quelques remarques. Le membre de gauche de l'égalité de la proposition est la valeur en $1-k$ (considéré comme élément de $\mathbb{Z}_p$) de la fonction d'Iwasawa $L_p(s,\epsilon,C)$ de la variable p-adique s. Dans le membre de droite intervient $L(1-k,\epsilon\omega^{-k})$ qui est la valeur en $1-k$ (considéré comme un complexe) de la fonction méromorphe $L(s,\epsilon\omega^{-k})$ de la variable complexe s. On a vu au § 0 que $L(1-k,\epsilon\omega^{-k})$ appartient en fait à $\bar{\mathbb{Q}}$ (et plus précisément même au corps engendré sur $\mathbb{Q}$ par les valeurs de $\epsilon\omega^{-k}$); dans notre égalité il faut considérer $L(1-k,\epsilon\omega^{-k})$ comme plongé dans $\bar{\mathbb{Q}}_p$ par le plongement choisi au début. La même remarque s'applique à $\epsilon(C)$ et $\omega^{-k}(C)$. Venons en à la démonstration :

Démonstration de 6.2. Par définition, on a

$$L_p(1-k,\epsilon,C) = \int_{\mathbb{Z}_p} <x>^{k-1} d\nu_{C,\epsilon\omega^{-1}}(x)$$
$$= \int_{\hat{\mathbb{Z}}} <y_p>^{k-1}(\epsilon\omega^{-1})(y)\, d\mu_C(y) = \int_{\hat{\mathbb{Z}}} <y_p>^{k-1}\ \epsilon(y)\,\omega^{-1}(y)\, d\mu_C(y).$$

Si y_p n'est pas dans $p\mathbb{Z}_p$, on a (par définition de ω et de $<\ >$) l'égalité $y_p = <y_p>\omega(y)$. Si y_p est dans $p\mathbb{Z}_p$, on a $\omega(y) = 0$ et $<y_p> = 0$, on a donc aussi $\omega^{-k}(y) = 0$. Cela donne dans tous les cas $<y_p>^{k-1}\omega^{-1}(y) = y_p^{k-1}\omega^{-k}(y)$; cela implique $L_p(1-k,\epsilon,C) = \int_{\hat{\mathbb{Z}}} y_p^{k-1}(\epsilon\omega^{-k})(y)\, d\mu_C(y)$.

Compte tenu de la proposition 3.10, on en tire $L_p(1-k,\epsilon,C) = \Delta_C(1-k,\epsilon\omega^{-k})$. Par définition, $\Delta_C(1-k,\epsilon\omega^{-k}) = L(1-k,\epsilon\omega^{-k}) - C_p^k L(1-k,(\epsilon\omega^{-k})_C)$. D'autre part, $\epsilon\omega^{-k}$ étant multiplicatif, on a $L(1-k,(\epsilon\omega^{-k})_C) = (\epsilon\omega^{-k})(C)\, L(1-k,\epsilon\omega^{-k})$; on conclut en reportant cette expression de $L(1-k,(\epsilon\omega^{-k})_C)$ dans l'égalité précédente.

Convenons, pour tout C de $\hat{\mathbb{Z}}^*$, de poser $<C> = <C_p>$; on a alors $C_p = <C>\omega(C)$; démontrons la proposition suivante qui sera fondamentale :

PROPOSITION 6.3. Soit ϵ un caractère modulo f et C un élément de $\hat{\mathbb{Z}}^*$;

1) l'égalité $\epsilon(C)<C> = 1$ implique $\epsilon(C) = 1$ et $<C> = 1$; de plus pour tout ϵ, il existe un $C \in \hat{\mathbb{Z}}^*$ tel que $\epsilon(C)<C> \neq 1$.

2) si $\epsilon(C)<C> \neq 1$, l'application qui à $s \in \mathbb{Z}_p$ associe $1-\epsilon(C)<C>^{1-s}$ ne s'annule pas pour $s \neq 1$; l'application qui à $s \in \mathbb{Z}_p \setminus \{1\}$ associe le quotient $\dfrac{L_p(s,\epsilon,C)}{1-\epsilon(C)<C>^{1-s}}$ est alors une application continue de $\mathbb{Z}_p \setminus \{1\}$ vers K (= corps des fractions de R) qui ne dépend pas de C.

Démonstration. 1) Si $\epsilon(C)<C> = 1$, alors $<C>$ est une racine de l'unité ; comme $<C>$ est dans $1+2p\mathbb{Z}_p$, cela implique $<C> = 1$ et donc $\epsilon(C) = 1$. En conséquence, pour tout $C \in \hat{\mathbb{Z}}^*$ tel que $<C> \neq 1$, on a $\epsilon(C)<C> \neq 1$, cela achève cette première partie.

2) Pour tout s de $\mathbb{Z}_p$, on a $<C>^{1-s} \in 1+2p\,\mathbb{Z}_p$; comme précédemment on en déduit que $\epsilon(C)<C>^{1-s} = 1$ si et seulement si $\epsilon(C) = 1$ et $<C>^{1-s} = 1$.

En conséquence, si $\epsilon(C) \neq 1$, on a $1-\epsilon(C)<C>^{1-s} \neq 0$ pour tout s de $\mathbb{Z}_p$. D'autre part, si $\epsilon(C)=1$, on a $<C> \neq 1$ puisque $\epsilon(C)<C> \neq 1$, donc $<C>^{1-s} \neq 1$ si $s \neq 1$ et donc $1-\epsilon(C)<C>^{1-s} \neq 0$ si $s \neq 1$. On en déduit évidemment que l'application qui à $s \in \mathbb{Z}_p \setminus \{1\}$ associe le quotient $\dfrac{L_p(s,\epsilon,C)}{1-\epsilon(C)<C>^{1-s}}$ est une application continue de $\mathbb{Z}_p \setminus \{1\}$ vers K. Pour tout entier $k \geq 1$, on a $<C>^k = C_p^k\, \omega(C)^{-k}$, donc la proposition précédente montre que la valeur de $\dfrac{L_p(s,\epsilon,C)}{1-\epsilon(C)<C>^{1-s}}$ en $s = 1-k$ est $L(1-k,\epsilon\omega^{-k})$; les $L(1-k,\epsilon\omega^{-k})$ ne dépendant pas de C et les $1-k$ pour $k \geq 1$ étant denses dans $\mathbb{Z}_p$, la fonction continue $\dfrac{L_p(s,\epsilon,C)}{1-\epsilon(C)<C>^{1-s}}$ ne dépend pas de C, C.Q.F.D.

Cette proposition 6.3 justifie la définition suivante :

DEFINITION 6.4. <u>Soit</u> ϵ <u>un caractère modulo</u> f <u>et</u> C <u>un élément de</u> $\hat{\mathbb{Z}}^*$ <u>tel que</u> $\epsilon(C)<C> \neq 1$. <u>On pose</u> $L_p(s,\epsilon) = \dfrac{L_p(s,\epsilon,C)}{1-\epsilon(C)<C>^{1-s}}$ <u>et on appelle cette fonction de</u> s <u>la fonction</u> L p-<u>adique du caractère</u> ϵ. <u>Cette fonction est continue sur</u> $\mathbb{Z}_p \setminus \{1\}$ <u>et, pour tout entier</u> $k \geq 1$, <u>on a</u> $L_p(1-k,\epsilon) = L(1-k,\epsilon\omega^{-k})$.

REMARQUE 6.5. Lorsque $p-1$ divise k, le caractère ω^{-k} est le caractère modulo p égal à 1. Cependant $\epsilon\omega^{-k}$ n'est pas égal à ϵ si p ne divise pas f : en effet, on a $(\epsilon\omega^{-k})(p) = 0$ puisque $\omega^{-k}(p) = 0$ mais $\epsilon(p) \neq 0$ puisque p ne divise pas f.

Enfin on a :

PROPOSITION 6.6. <u>Soit</u> ϵ <u>un caractère modulo</u> f <u>différent de</u> 1 (i.e. <u>il existe un</u> x <u>premier à</u> f <u>tel que</u> $\epsilon(x) \neq 1$), <u>alors</u> $L_p(s,\epsilon)$ <u>se prolonge en une fonction continue sur</u> $\mathbb{Z}_p$ <u>tout entier</u> ; <u>nous noterons encore</u> $L_p(s,\epsilon)$ <u>cette fonction continue</u>.

<u>Démonstration</u>. On choisit $C \in \hat{\mathbb{Z}}^*$ tel que $\epsilon(C) \neq 1$; comme on l'a remarqué dans la démonstration de la proposition 6.3, cela implique que $1-\epsilon(C)<C>^{1-s}$ ne s'annule pas sur $\mathbb{Z}_p$. Le quotient $\dfrac{L_p(s,\epsilon,C)}{1-\epsilon(C)<C>^{1-s}}$ définit donc une fonction continue

sur $\mathbb{Z}_p$ tout entier qui répond à notre question.

REMARQUE 6.7. Supposons que ϵ est tel qu'il existe un $C \in \hat{\mathbb{Z}}^*$ avec $\langle C\rangle = 1$ et $\epsilon(C) \neq 1$; on a alors $1-\epsilon(C)\langle C\rangle^{1-s} = 1-\epsilon(C)$ pour tout s de $\mathbb{Z}_p$. Le quotient $\frac{L_p(s,\epsilon,C)}{1-\epsilon(C)}$ est donc continu sur $\mathbb{Z}_p$; d'après la proposition 6.2 cette fonction continue coïncide avec $L_p(s,\epsilon)$ pour tous les s de la forme $1-k$ avec k entier positif ; il en résulte que $L_p(s,\epsilon) = \frac{L_p(s,\epsilon,C)}{1-\epsilon(C)}$ pour tout $s \in \mathbb{Z}_p$. Si de plus $1-\epsilon(C)$ est inversible dans l'anneau des entiers R du corps $\mathbb{Q}_p(\epsilon)$ (ce qui est équivalent à ce que l'ordre de la racine de l'unité $\epsilon(C)$ n'est pas une puissance de p) le quotient $\frac{L_p(s,\epsilon,C)}{1-\epsilon(C)}$ est une fonction d'Iwasawa (puisque $L_p(s,\epsilon,C)$ en est une) donc $L_p(s,\epsilon)$ est une fonction d'Iwasawa. Nous étudierons au § 7 la question de savoir pour quels ϵ la fonction $L_p(s,\epsilon)$ est une fonction d'Iwasawa.

Terminons ce chapitre par une remarque importante :

PROPOSITION 6.8. Soit ϵ un caractère modulo f impair (i.e. $\epsilon(-1) = -1$), alors $L_p(s,\epsilon) = 0$ pour tout s de $\mathbb{Z}_p$.

Démonstration. Rappelons que, de l'égalité formelle $\frac{Z e^{XZ}}{e^Z-1} = \frac{(-Z)e^{(1-X)(-Z)}}{e^{-Z}-1}$, on tire $B_k(1-X) = (-1)^k B_k(X)$ pour $k \geq 0$ et $B_k(X+1)-B_k(X) = kX^{k-1}$ pour $k \geq 1$. Soit ϵ une application périodique de $\mathbb{Z}$ dans $\mathbb{C}$ dont la période divise l'entier f (on ne suppose pas pour l'instant que ϵ est un caractère) ; pour $k \geq 1$, on a

$$L(1-k,\epsilon) = -\frac{f^{k-1}}{k}\sum_{t=1}^{f} \epsilon(t)B_k\left(\frac{t}{f}\right) = -\frac{f^{k-1}}{k}\left[\sum_{t=1}^{f} \epsilon(f-t)B_k\left(\frac{f-t}{f}\right) - \epsilon(0)(B_k(0)-B_k(1))\right].$$

En conséquence, si $k > 1$ ou si $k = 1$ et $\epsilon(0) = 0$, on a

$$L(1-k,\epsilon) = -\frac{f^{k-1}}{k}\sum_{t=1}^{f} \epsilon(f-t)B_k\left(\frac{f-t}{f}\right) = -\frac{f^{k-1}}{k}(-1)^k\sum_{t=1}^{f} \epsilon(-t)\,B_k\left(\frac{t}{f}\right) ;$$

en définissant $\tilde{\epsilon}$ par $\tilde{\epsilon}(x) = \epsilon(-x)$ pour tout x de $\mathbb{Z}$, on a donc $L(1-k,\epsilon) = (-1)^k L(1-k,\tilde{\epsilon})$. Supposons maintenant que ϵ est une application paire (resp. impaire) i.e. que $\tilde{\epsilon} = \epsilon$ (resp. $\tilde{\epsilon} = -\epsilon$) ; pour tout complexe s de partie réelle plus grande que 1 on voit sur la définition que $L(s,\epsilon) = L(s,\tilde{\epsilon})$ (resp.

$L(s,\varepsilon) = -L(s,\tilde{\varepsilon}))$; l'unicité du prolongement analytique permet d'en déduire que, pour tout entier $k \geq 1$, on a $L(1-k,\varepsilon) = L(1-k,\tilde{\varepsilon})$ (resp. $L(1-k,\varepsilon) = -L(1-k,\tilde{\varepsilon})$). De ces deux expressions de $L(1-k,\varepsilon)$ en fonction de $L(1-k,\tilde{\varepsilon})$ on déduit que, pour $k > 1$ ou $k = 1$ si $\varepsilon(0) = 0$, on a $L(1-k,\varepsilon) = 0$ si k et ε ne sont pas de même parité Supposons maintenant que ε soit un caractère ; on a alors $\varepsilon(0) = 0$ et $\varepsilon(-1) = \pm 1$. Si $\varepsilon(-1) = -1$, le caractère $\varepsilon\boldsymbol{\omega}^{-k}$ et l'entier k n'ont pas la même parité, donc $L(1-k, \varepsilon\boldsymbol{\omega}^{-k}) = 0$; on a donc $L_p(1-k,\varepsilon) = 0$ pour tout entier $k \geq 1$ ce qui implique que la fonction $L_p(s,\varepsilon)$ est identiquement nulle sur $\mathbb{Z}_p$, C.Q.F.D.

Les fonctions $L_p(s,\varepsilon)$ n'ont donc d'intérêt que pour les caractères ε pairs i.e. tels que $\varepsilon(-1) = +1$.

§ 7. UN THEOREME D'IWASAWA.

On désigne par ϵ un caractère pair modulo f et on conserve les conventions faites au début du § 6 (c'est-à-dire que l'on considère indifféremment ϵ comme un homomorphisme de $(\mathbb{Z}/f\mathbb{Z})^*$ vers $\mathbb{C}^*$, comme une application périodique de $\mathbb{Z}$ vers $\mathbb{C}$ ou R, ou encore comme une application localement constante de $\hat{\mathbb{Z}}$ vers R). Pour tout nombre premier ℓ divisant f, on note $\epsilon_{|\ell}$ la ℓ composante de ϵ c'est-à-dire, en notant $\ell^{n(\ell)}$ la plus grande puissance de ℓ qui divise f, la composée de ϵ et de l'injection canonique de $(\mathbb{Z}/\ell^{n(\ell)}\mathbb{Z})^*$ vers $(\mathbb{Z}/f\mathbb{Z})^*$. On convient de prolonger $\epsilon_{|\ell}$ à $\mathbb{Z}/\ell^{n(\ell)}\mathbb{Z}$ tout entier en lui attribuant la valeur 0 sur les éléments de $\mathbb{Z}/\ell^{n(\ell)}\mathbb{Z}$ qui ne sont pas dans $(\mathbb{Z}/\ell^{n(\ell)}\mathbb{Z})^*$. En composant $\epsilon_{|\ell}$ avec la projection canonique de $\mathbb{Z}_\ell$ sur $\mathbb{Z}_\ell/\ell^{n(\ell)}\mathbb{Z}_\ell = \mathbb{Z}/\ell^{n(\ell)}\mathbb{Z}$ on obtient une fonction définie sur $\mathbb{Z}_\ell$ à valeur dans $\mathbb{C}$ ou R que l'on note encore $\epsilon_{|\ell}$. Nous posons alors la définition suivante :

DEFINITION 7.1. _Soit_ ϵ _un caractère modulo_ f ; _nous dirons que_ ϵ _est de deuxième espèce si les deux conditions suivantes sont vérifiées_ :

1) _l'image de_ ϵ _est formée de racines de l'unité dont l'ordre est une puissance de_ p i.e. _l'ordre de_ ϵ _est une puissance de_ p.

2) _si_ ℓ _divise_ f _et_ $\ell \neq p$, _alors_ $\epsilon_{|\ell} = 1$.

L'essentiel de ce paragraphe est la démonstration du théorème suivant :

THEOREME 7.2. (Iwasawa). _Soit_ ϵ _un caractère pair modulo_ f. _Si_ ϵ

<u>n'est pas de seconde espèce,</u> $\frac{1}{2}L_p(s,\varepsilon)$ <u>est une fonction d'Iwasawa.</u>

La démonstration de ce théorème est longue ; nous allons établir une suite de propositions qui, juxtaposées, donneront le théorème. Rappelons que l'on a choisi une fois pour toute un générateur γ du $\mathbb{Z}_p$-module $1+2p\mathbb{Z}_p$ et que, pour tout z de $1+2p\mathbb{Z}_p$, on a défini $\alpha(z)$ par $z=\gamma^{\alpha(z)}$. Soit C un élément de $\hat{\mathbb{Z}}^*$; on a vu que la fonction $L_p(s,\varepsilon,C)$ est une fonction d'Iwasawa. Notons $f(T,\varepsilon,C)$ la série de $R[[T]]$ telle que $L_p(s,\varepsilon,C)=f(\gamma^{-s}-1,\varepsilon,C)$, on a :

PROPOSITION 7.3. <u>Pour tout caractère pair</u> ε, <u>la série formelle</u> $f(T,\varepsilon,C)$ <u>est dans</u> $2R[[T]]$.

<u>Démonstration.</u> Il n'y a rien à démontrer si $p\neq 2$. Nous supposons donc $p=2$. Par définition $f(T,\varepsilon,C)=\sum_{n\geq 0} f_nT^n$ avec $f_n=\int_{\mathbb{Z}_2}\binom{x}{n}\,d(\alpha_*\nu_{C,\varepsilon\omega^{-1}})(x)$; il faut donc montre que ces intégrales sont dans $2R$ pour tout $n\geq 0$. Nous allons montrer plus généralement que $\int_{\mathbb{Z}_2}\varphi(x)\,d(\alpha_*\nu_{C,\varepsilon\omega^{-1}})(x)$ est dans $2R$ pour toute fonction continue φ de $\mathbb{Z}_2$ dans R. On a (voir § 5)

$$\int_{\mathbb{Z}_2}\varphi(x)\,d(\alpha_*\nu_{C,\varepsilon\omega^{-1}})(x)=\int_{\hat{\mathbb{Z}}}\varphi_\alpha(y_2)\,\varepsilon(y)\,\omega^{-1}(y)\,d\mu_C(y).$$

Sur la définition de φ_α on vérifie que $\varphi_\alpha(-y_2)=\varphi_\alpha(y_2)$; les caractères ω^{-1} et ε étant respectivement impair et pair, la fonction de $\hat{\mathbb{Z}}$ vers R qui prend en $y\in\hat{\mathbb{Z}}$ la valeur $\varphi_\alpha(y_2)\,\varepsilon(y)\,\omega^{-1}(y)$ est une fonction impaire. Pour achever notre démonstration il suffit donc de montrer que, si f est une fonction continue impaire de $\hat{\mathbb{Z}}$ dans R, alors $\int_{\hat{\mathbb{Z}}} f(y)\,d\mu_C(y)\in 2R$. La mesure μ_C étant une mesure à valeurs dans $\mathbb{Z}_2$, il suffit de démontrer notre assertion pour une fonction f impaire à valeurs dans $\mathbb{Z}_2$. Introduisons la fonction δ sur $\hat{\mathbb{Z}}$ définie par $\delta(y)=1$ ou 0 suivant que $f(y)$ est congru à 1 modulo 4 ou pas ; il est clair que δ est localement constante, donc il existe un entier f tel que δ est constante sur les classes modulo $f\hat{\mathbb{Z}}$. On vérifie que pour tout y de $\hat{\mathbb{Z}}$ on a $f(y)\equiv\delta(y)-\delta(-y)$ modulo $2\mathbb{Z}_2$ (on raisonne séparément sur chaque classe modulo $4\hat{\mathbb{Z}}$ et on tient compte du fait que f est impaire).

On a donc

$$\int_{\hat{\mathbb{Z}}} f(y)\, d\mu_C(y) \equiv \int_{\hat{\mathbb{Z}}} \delta(y)\, d\mu_C(y) - \int_{\hat{\mathbb{Z}}} \delta(-y) d\mu_C(y) \text{ modulo } 2\,\mathbb{Z}_2 .$$

Définissons $\tilde{\delta}$ par $\tilde{\delta}(y) = \delta(-y)$; la congruence précédente se réécrit

$$\int_{\hat{\mathbb{Z}}} f(y)\, d\mu_C(y) \equiv \Delta_C(0,\delta) - \Delta_C(0,\tilde{\delta}) \text{ modulo } 2\,\mathbb{Z}_2 .$$

D'autre part, on a

$$L(0,\tilde{\delta}) = -\sum_{t=1}^{f} \tilde{\delta}(t)\left(\frac{t}{f}-\frac{1}{2}\right) = -\sum_{t=1}^{f-1} \tilde{\delta}(t)\left(\frac{t}{f}-\frac{1}{2}\right)$$

car, f étant impaire, on a $\delta(0) = \tilde{\delta}(0) = \delta(f) = \tilde{\delta}(f) = 0$; on a donc

$$L(0,\tilde{\delta}) = -\sum_{t=1}^{f-1} \delta(-t)\left(\frac{t}{f}-\frac{1}{2}\right) = -\sum_{t=1}^{f-1} \delta(f-t)\left(\frac{t}{f}-\frac{1}{2}\right) = -\sum_{u=1}^{f-1} \delta(u)\left(\frac{f-u}{f}-\frac{1}{2}\right) = \sum_{u=1}^{f-1} \delta(u)\left(\frac{u}{f}-\frac{1}{2}\right) = -L(0,\delta).$$

De même on montre que $L(0,\tilde{\delta}_C) = -L(0,\delta_C)$ donc $\Delta_C(0,\delta) - \Delta_C(0,\tilde{\delta}) = 2\,\Delta_C(0,\delta)$;

on a donc $\Delta_C(0,\delta) - \Delta_C(0,\tilde{\delta}) \in 2\,\mathbb{Z}_2$ ce qui montre $\int_{\hat{\mathbb{Z}}} f(y)\, d\mu_C(y) \in 2\,\mathbb{Z}_2$ et achève la démonstration.

Pour tout z de $\mathbb{Z}_p$, nous définissons $(1+T)^z$ comme étant la série formelle $\sum_{n\geq 0} \binom{z}{n} T^n$ où $\binom{z}{n} = \dfrac{z(z-1)\ldots(z-n+1)}{n!}$; comme nous l'avons remarqué au début du § 4, les $\binom{z}{n}$ sont dans $\mathbb{Z}_p$ donc $(1+T)^z$ est dans $\mathbb{Z}_p[[T]]$. Rappelons le lemme suivant (qui justifie la notation) :

LEMME 7.4. <u>Soit</u> $m \in 2p\mathbb{Z}_p$ <u>et</u> $z \in \mathbb{Z}_p$; <u>on a</u> $\sum_{n\geq 0} \binom{z}{n} m^n = (1+m)^z$.

<u>Démonstration</u>. On considère m comme fixé et on regarde les deux membres de l'égalité comme des fonctions de z ; en tant que telles, elles sont continues. D'autre part, notre égalité est vraie pour z entier positif ; les entiers positifs étant denses dans $\mathbb{Z}_p$, cette égalité est vraie pour tous les z de $\mathbb{Z}_p$.

Pour tout C de $\hat{\mathbb{Z}}^*$, posons $\alpha(C) = \alpha(\langle C \rangle)$ et $u(T,\epsilon,C) = 1 - \epsilon(C)\langle C\rangle(1+T)^{\alpha(C)}$; la série formelle $u(T,\epsilon,C)$ est dans $R[[T]]$ et on tire directement du lemme précédent le résultat suivant :

LEMME 7.5. <u>Pour tout</u> s <u>de</u> $\mathbb{Z}_p$ <u>et tout</u> C <u>de</u> $\hat{\mathbb{Z}}^*$ <u>on a</u>
$u(\gamma^{-s}-1, \epsilon, C) = 1 - \epsilon(C)\langle C\rangle^{1-s}$.

Le terme constant de la série formelle $u(T,\epsilon,C)$ est $1-\epsilon(C)<C>$. Supposons ce terme non nul i.e. supposons $\epsilon(C)<C>\neq 1$ et désignons par K le corps des fractions de R (donc $K=\mathbb{Q}_p(\epsilon)$) ; la série formelle $u(T,\epsilon,C)$ est inversible dans $K[[T]]$; en conséquence le quotient $\frac{f(T,\epsilon,C)}{u(T,\epsilon,C)}$ est dans $K[[T]]$; on a la proposition suivante :

PROPOSITION 7.6. <u>Soit</u> C <u>un élément de</u> $\hat{\mathbb{Z}}^*$ <u>tel que</u> $\epsilon(C)<C>\neq 1$. <u>Le quotient</u> $\frac{f(T,\epsilon,C)}{u(T,\epsilon,C)}$ <u>est un élément de</u> $K[[T]]$ <u>indépendant de</u> C ; <u>nous le noterons</u> $g(T,\epsilon)$.

<u>Démonstration</u>. Posons $\frac{f(T,\epsilon,C)}{u(T,\epsilon,C)}=g(T,\epsilon,C)$. Le lemme 7.5 et la proposition 6.3 montrent que, pour tout s de $\mathbb{Z}_p\setminus\{1\}$, le quotient $\frac{f(\gamma^{-s}-1,\epsilon,C)}{u(\gamma^{-s}-1,\epsilon,C)}$ est défini et indépendant de C ; cela signifie que, pour tout x de $2p\,\mathbb{Z}_p$ différent de $\gamma^{-1}-1$, le quotient $\frac{f(x,\epsilon,C)}{u(x,\epsilon,C)}$ est défini et indépendant de C. Posons maintenant $g(T,\epsilon,C)=\sum_{n\geq 0} g_n(\epsilon,C)T^n$; l'expression des $g_n(\epsilon,C)$ en fonction des coefficients de $u(T,\epsilon,C)$ et de ceux de $f(T,\epsilon,C)$ montre que $(1-\epsilon(C)<C>)^{n+1}g_n(\epsilon,C)$ est dans R. On en déduit que, pour x assez proche de zéro, la série $\sum g_n(\epsilon,C)x^n$ converge. Choisissons un voisinage de zéro dans lequel, d'une part la série précédente converge, et , d'autre part la série $u(x,\epsilon,C)$ ne s'annule pas (un tel voisinage existe puisque $u(0;\epsilon,C)\neq 0$) ; on vérifie que, pour tout x de ce voisinage, on a $\frac{f(x,\epsilon,C)}{u(x,\epsilon,C)}=g(x,\epsilon,C)$. En conséquence on a trouvé un voisinage de 0 sur lequel les valeurs de la série $g(x,\epsilon,C)$ ne dépendent pas de C ; la remarque 5.3 permet d'en déduire que la série $g(T,\epsilon,C)$ ne dépend pas de C, C.Q.F.D.

COROLLAIRE 7.7. <u>La fonction</u> $L_p(s,\epsilon)$ (resp. $\frac{1}{2}L_p(s,\epsilon)$) <u>est une fonction d'Iwasawa si et seulement si la série formelle</u> $g(T,\epsilon)$ <u>est dans</u> $R[[T]]$ (resp. $2R[[T]]$) ; <u>dans ce cas</u> $L_p(s,\epsilon)=g(\gamma^{-s}-1,\epsilon)$ <u>pour tout</u> s <u>de</u> $\mathbb{Z}_p$.

<u>Démonstration</u>. Si $L_p(s,\epsilon)$ est une fonction d'Iwasawa, il existe $h(T)\in R[[T]]$ tel que $L_p(s,\epsilon)=h(\gamma^{-s}-1)$ pour tout s de $\mathbb{Z}_p$. Si $C\in\hat{\mathbb{Z}}^*$ est tel que $<C>\epsilon(C)\neq 1$,

on a donc $\frac{f(\gamma^{-s}-1,\epsilon,C)}{u(\gamma^{-s}-1,\epsilon,C)} = h(\gamma^{-s}-1)$. On a vu dans la démonstration précédente que, pour x suffisamment près de 0, on a $\frac{f(x,\epsilon,C)}{u(x,\epsilon,C)} = g(x,\epsilon)$. On a donc $h(x) = g(x,\epsilon)$ pour x suffisamment près de 0 ; on en déduit (Remarque 5.3) que $h(T) = g(T,\epsilon)$. Réciproquement, on vérifie sans difficulté que, si $g(T,\epsilon)$ est dans $R[[T]]$, alors $\frac{f(\gamma^{-s}-1,\epsilon,C)}{u(\gamma^{-s}-1,\epsilon,C)} = L_p(s,\epsilon) = g(\gamma^{-s}-1,\epsilon)$ pour tout s de $\mathbb{Z}_p$ ce qui prouve le corollaire.

Ce corollaire 7.7. implique directement la proposition suivante :

PROPOSITION 7.8. Le théorème 7.2 est équivalent à l'assertion suivante : si ϵ n'est pas de seconde espèce, alors $g(T,\epsilon)$ est dans $2R[[T]]$.

C'est cette dernière assertion que nous allons démontrer. Commençons par un cas particulier :

PROPOSITION 7.9. Si l'image de ϵ contient une racine de l'unité dont l'ordre n'est pas une puissance de p alors $g(T,\epsilon)$ est dans $2R[[T]]$.

Démonstration. Soit $C \in \hat{\mathbb{Z}}^*$ tel que l'ordre de la racine de l'unité $\epsilon(C)$ ne soit pas une puissance de p ; l'élément $\epsilon(C)$ n'est pas congru à 1 modulo l'idéal maximal de R donc $1-\epsilon(C)\langle C\rangle$ est une unité dans R. En conséquence la série $u(T,\epsilon,C)$ est inversible dans $R[[T]]$ et notre proposition résulte de la proposition 7.3.

Il reste donc à étudier le cas des caractères dont l'image est formée de racines de l'unité dont l'ordre est une puissance de p, c'est-à-dire des caractères vérifiant la condition 1) de la définition 7.1 ; parmi ceux-ci, seuls sont à considérer les caractères ne vérifiant pas la condition 2) de cette définition puisque nous ne considérons pas les caractères de seconde espèce. Voici un premier cas :

PROPOSITION 7.10. La série formelle $g(T,\epsilon)$ est dans $2R[[T]]$ si ϵ est un caractère modulo f différent du caractère 1 qui vérifie l'une ou l'autre des deux conditions suivantes :

a) p ne divise pas f

b) p <u>divise</u> f <u>et</u> $\varepsilon_{|p} = 1$.

<u>Démonstration</u>. Le caractère ε étant différent du caractère modulo f égal à 1, l'une ou l'autre des conditions a) ou b) implique l'existence d'un nombre premier ℓ différent de p divisant f et tel que $\varepsilon_{|\ell} \neq 1$. Choisissons $C \in \hat{\mathbb{Z}}^*$ vérifiant $C_r = 1$ pour tout nombre premier $r \neq \ell$ et $\varepsilon_{|\ell}(C_\ell) \neq 1$. On a $\langle C\rangle = 1$ donc $\alpha(C) = 0$; on a aussi $\varepsilon(C) = \varepsilon_{|\ell}(C_\ell) \neq 1$ donc $u(T,\varepsilon,C) = 1-\varepsilon(C)$ et la proposition 7.6 montre que $g(T,\varepsilon) = \frac{f(T,\varepsilon,C)}{1-\varepsilon(C)}$. D'autre part, soit $D \in \hat{\mathbb{Z}}^*$ défini par $D_\ell = 1$ si $\ell \neq p$ et $D_p = \gamma$. On a $\langle D\rangle = \gamma$ donc $\alpha(D) = 1$. Si a) ou b) est réalisée, on a aussi $\varepsilon(D) = 1$; dans ce cas $u(T,\varepsilon,D) = 1-\gamma(1+T) = 1-\gamma-\gamma T$. Enfin, $\varepsilon(D)\langle D\rangle = \gamma$ étant différent de 1, la proposition 7.6 montre que $g(T,\varepsilon) = \frac{f(T,\varepsilon,D)}{1-\gamma-\gamma T}$. Or, l'élément $\varepsilon(C)$ est une racine de l'unité dont l'ordre est une puissance de p ; l'élément $1-\varepsilon(C)$ divise donc $1-\gamma$ dans R, c'est-à-dire qu'il existe $v \in R$ tel que $1-\gamma = v(1-\varepsilon(C))$. On a $g(T,\varepsilon) = \frac{f(T,\varepsilon,D)}{1-\gamma-\gamma T} = \frac{-vf(T,\varepsilon,C)}{-v(1-\varepsilon(C))} = \frac{f(T,\varepsilon,D)-vf(T,\varepsilon,C)}{-\gamma T}$. L'élément γ étant une unité dans R, on déduit de la proposition 7.3 que $g(T,\varepsilon)$ est dans $\frac{2}{T}R[[T]]$. Comme $g(T,\varepsilon)$ est dans $K[[T]]$, on en déduit que $g(T,\varepsilon)$ est dans $2R[[T]]$ C.Q.F.D.

Pour terminer la démonstration du théorème 7.2, il ne nous reste plus qu'à étudier le cas des caractères ε modulo f qui ne sont pas de deuxième espèce mais qui vérifient les deux conditions suivantes :

I) l'image de ε est formée de racines de l'unité dont l'ordre est une puissance de p,

II) p divise f et $\varepsilon_{|p} \neq 1$.

Posons alors $f = f'p^n$ avec $(f',p) = 1$; on a $\varepsilon = \varepsilon'\theta$ où $\varepsilon' = \prod_{\ell | f'} \varepsilon_{|\ell}$ et $\theta = \varepsilon_{|p}$; le caractère θ est de seconde espèce puisque ε vérifie I).

On a la proposition :

PROPOSITION 7.11. <u>Soit</u> θ <u>un caractère modulo une puissance de</u> p <u>et de seconde espèce. Si</u> ε <u>et</u> ε' <u>sont deux caractères qui vérifient</u> $\varepsilon = \varepsilon'\theta$, <u>alors</u>

pour tout C de $\hat{\mathbb{Z}}^*$ on a l'égalité $f(T,\varepsilon,C) = f(\theta_{|p}(\gamma)(1+T)-1,\varepsilon',C)$ (la substitution de T par $\theta_{|p}(\gamma)(1+T)-1$ est licite car d'une part $f(T,\varepsilon',C)$ et $\theta_{|p}(\gamma)(1+T)-1$ sont dans $R[[T]]$ et d'autre part le terme constant de $\theta_{|p}(\gamma)(1+T)-1$ est dans l'idéal maximal de R).

Avant de démontrer cette proposition, montrons comment elle entraîne le résultat suivant qui, compte tenu de la proposition 7.8 et des cas déjà règlés, achève la démonstration du théorème 7.2 :

PROPOSITION 7.12. Soit ε un caractère modulo f qui n'est pas de seconde espèce mais qui vérifie les conditions I) et II) énoncées ci-dessus. La série formelle $g(T,\varepsilon)$ est dans $2R[[T]]$.

Démonstration. Posons, comme ci-dessus, $f = f'p^n$, $\varepsilon' = \prod_{\ell | f'} \varepsilon_{|\ell}$ et $\theta = \varepsilon_{|p}$ de sorte que $\varepsilon = \varepsilon'\theta$. Choisissons C dans $\hat{\mathbb{Z}}^*$ tel que $<C> \neq 1$. Comme nous l'avons remarqué (démonstration de la proposition 6.3, 1)) on a alors $\varepsilon(C)<C> \neq 1$ et $\varepsilon'(C)<C> \neq 1$; on a donc $g(T,\varepsilon) = \frac{f(T,\varepsilon,C)}{u(T,\varepsilon,C)}$. Le caractère θ étant un caractère modulo une puissance de p, on a $\theta(C) = \theta_{|p}(C_p)$; de plus, l'image de θ donc celle de $\theta_{|p}$ étant formée de racines de l'unité dont l'ordre est une puissance de p, on a $\theta_{|p}(C_p) = \theta_{|p}(<C_p>) = [\theta_{|p}(\gamma)]^{\alpha(C)}$. On a donc $\varepsilon(C) = \varepsilon'(C)[\theta_{|p}(\gamma)]^{\alpha(C)}$ et donc $u(T,\varepsilon,C) = u(\theta_{|p}(\gamma)(1+T)-1,\varepsilon',C)$. Compte tenu de la proposition 7.11, on en tire $g(T,\varepsilon) = \frac{f(\theta_{|p}(\gamma)(1+T)-1,\varepsilon',C)}{u(\theta_{|p}(\gamma)(1+T)-1,\varepsilon',C)} = g(\theta_{|p}(\gamma)(1+T)-1,\varepsilon')$. Enfin, ε n'étant pas de seconde espèce, ε' n'est pas le caractère modulo f' égal à 1 donc la proposition 7.10 montre que $g(T,\varepsilon')$ est dans $2R[[T]]$; on en déduit que $g(\theta_{|p}(\gamma)(1+T)-1,\varepsilon')$ est dans $2R[[T]]$ c'est-à-dire que $g(T,\varepsilon)$ est dans $2R[[T]]$, C.Q.F.D.

Il reste à démontrer la proposition 7.11 :

Démonstration de la proposition 7.11. La série $f(T,\varepsilon,C)$ est la série attachée à la mesure $\alpha_*\nu_{C,\varepsilon\omega^{-1}}$. Montrons que cette mesure est la mesure dont la densité par rapport à $\alpha_*\nu_{C,\varepsilon'\omega^{-1}}$ est la fonction qui à $x \in \mathbb{Z}_p$ associe $\theta_{|p}(\gamma)^x$: soit $f \in \mathrm{Cont}(\mathbb{Z}_p,R)$ on a

$$\int_{\mathbb{Z}_p} f(x)d(\alpha_* \nu_{C,\varepsilon\omega^{-1}})(x) = \int_{\hat{\mathbb{Z}}} f_\alpha(y_p)\varepsilon\omega^{-1}(y)d\mu_C(y) = \int_{\hat{\mathbb{Z}}} f_\alpha(y_p)\theta(y)\varepsilon'\omega^{-1}(y)d\mu_C(y) ;$$

mais θ étant un caractère modulo une puissance de p on a $\theta(y) = \theta_{|p}(y_p)$; de plus θ étant de seconde espèce on a $\theta_{|p}(y_p) = \theta_{|p}(<y_p>)$; en conséquence si y_p est dans $\mathbb{Z}_p^*$ on a $\theta(y) = \theta_{|p}(\gamma)^{\alpha(y_p)}$ et, $f_\alpha(y_p)$ étant nul si y n'est pas dans $\mathbb{Z}_p^*$, on a $f_\alpha(y_p)\theta(y) = f_\alpha(y_p)\theta_{|p}(\gamma)^{\alpha(y_p)}$ pour tout y de $\hat{\mathbb{Z}}$; notre intégrale est donc égale à

$$\int_{\hat{\mathbb{Z}}} f_\alpha(y_p)\theta_{|p}(\gamma)^{\alpha(y_p)} \varepsilon'(y)\, d\mu_C(y) = \int_{\mathbb{Z}_p} f(x)\, \theta_{|p}(\gamma)^x\, d(\alpha_* \nu_{C,\varepsilon'})(x)$$

et cela montre que $\alpha_*\nu_{C,\varepsilon}$ est la mesure dont la densité par rapport à $\alpha_*\nu_{C,\varepsilon'}$ est la fonction qui à x associe $\theta_{|p}(\gamma)^x$. On conclut alors avec le lemme suivant :

LEMME 7.13. <u>Soit ν une mesure sur $\mathbb{Z}_p$ à valeurs dans R et $F_\nu(T)$ la série de R[[T]] associée à ν. Si β est un élément $1+2p\mathbb{Z}_p$ et si $F_{\nu,\beta}(T)$ est la série associée à la mesure dont la densité par rapport à ν est la fonction qui à x associe β^x, on a $F_{\nu,\beta}(T) = F_\nu(\beta(1+T)-1)$.</u>

<u>Démonstration</u>. Du lemme 5.6 on tire, pour tout δ de $1+2p\,\mathbb{Z}_p$, l'égalité $F_{\nu,\beta}(\delta-1) = \int_{\mathbb{Z}_p} \delta^x\beta^x\, d\nu(x)$; ce même lemme montre que cette intégrale est $F_\nu(\delta\beta-1)$, donc pour tout δ de $1+2p\mathbb{Z}_p$ on a $F_{\nu,\beta}(\delta-1) = F_\nu[\beta((\delta-1)+1)-1]$; on en tire (remarque 5.3) que $F_{\nu,\beta}(T) = F_\nu(\beta(T+1)-1)$ C.Q.F.D.

Le théorème 7.2 est donc démontré ; complètons le par le résultat suivant :

PROPOSITION 7.14. <u>Soit θ un caractère modulo une puissance de p qui est de seconde espèce ; si C est un élément de $\hat{\mathbb{Z}}^*$ tel que $C_p = \gamma$, alors $g(T,\theta) = \dfrac{f(T,\theta,C)}{1-\gamma\theta(\gamma)-\gamma\theta(\gamma)T}$ et $\frac{1}{2}f(T,\theta,C)$ est inversible dans R[[T]] (comme $1-\gamma\theta(\gamma)$ est dans l'idéal maximal de R, on en déduit que $g(T,\theta)$ n'est pas dans R[[T]]).</u>

<u>Démonstration</u>. La proposition 7.1. montre que $f(T,\theta,C) = f(\theta_{|p}(\gamma)(1+T)-1,1,C)$ où 1 désigne le caractère modulo p égal à 1. Notre assertion est équivalente à

$\frac{1}{2}f(0,\theta,C)\in R^*$, donc à $\frac{1}{2}f(\theta_{|p}(\gamma)-1,1,C)\in R^*$. On sait (proposition 7.3) que $f(T,1,C)$ est dans $2R[[T]]$, donc on a $\frac{1}{2}f(\theta_{|p}(\gamma)-1,1,C)\equiv\frac{1}{2}f(0,1,C)$ modulo $(\theta_{|p}(\gamma)-1)R$. Mais $f(0,1,C)=L_p(0,1,C)$ qui, d'après la proposition 6.2, est $(1-\gamma\omega^{-1}(C))L(0,\omega^{-1})$; de plus on a $L(0,\omega^{-1})=-\sum_{t=1}^{p-1}\omega^{-1}(t)B_1(\frac{t}{p})=-\sum_{t=1}^{p-1}\omega^{-1}(t)\frac{t}{p}\equiv\frac{1}{p}$ modulo $\mathbb{Z}_p$ si $p\neq 2$ et $L(0,\omega^{-1})=\frac{1}{2}$ si $p=2$. Du choix de C résulte que $\omega^{-1}(C)=1$, donc $\frac{1}{2}f(0,1,C)=\frac{1}{2}(1-\gamma)L(0,\omega^{-1})$ est une unité puisque γ est un générateur de $1+2p\mathbb{Z}_p$; c'est ce qu'on voulait.

REMARQUE 7.15. Il reste à étudier le cas des caractères de seconde espèce qui ne sont pas définis modulo une puissance de p ; le lemme 8.7 du paragraphe suivant montre que ce cas se ramène à celui étudié dans la proposition précédente (en effet le caractère primitif associé à un caractère de seconde espèce est défini modulo une puissance de p).

REMARQUE 7.16. Retrouvons quelques congruences classiques. Soit $k>1$ un entier ; on a $L_p(1-k,\omega^k)=L(1-k,\omega^k\omega^{-k})=(1-p^{k-1})\zeta(1-k)$ (puisque $L(s,\omega^k\omega^{-k})=(1-p^{-s})\zeta(s)$ pour tout complexe s). Si $p-1$ ne divise pas k, $L_p(s,\omega^k)$ est une fonction d'Iwasawa à coefficients dans $\mathbb{Z}_p$, donc $(1-p^{k-1})\zeta(1-k)$ est dans $\mathbb{Z}_p$; toujours dans ce cas, si $k\equiv k' \bmod (p-1)p^n$ pour un entier $n\geq 0$, on a $\omega^k=\omega^{k'}$ et $\gamma^{k-1}-1\equiv\gamma^{k'-1}-1 \bmod p^{n+1}\mathbb{Z}_p$ donc $(1-p^{k-1})\zeta(1-k)\equiv(1-p^{k'-1})\zeta(1-k') \bmod p^{n+1}\mathbb{Z}_p$. Si $p-1$ divise k, le caractère ω^k est le caractère modulo p égal à 1 ; notons le 1 et notons C l'élément de $\hat{\mathbb{Z}}^*$ tel que $C_p=1+2p$ et $C_\ell=1$ si $\ell\neq p$; on a

$$(1-p^{k-1})\zeta(1-k)=L_p(1-k,1)=\frac{f(\gamma^{k-1}-1,1,C)}{1-\gamma^k} \quad \text{et donc}$$

$(1-p^{k-1})p\,B_k=\frac{-2pk}{1-\gamma^k}(\frac{1}{2}f(\gamma^{k-1}-1,1,C)$; compte tenu de la prop. 7.3 et de $\frac{-2pk}{1-\gamma^k}\equiv 1 \bmod p\mathbb{Z}_p$ on voit que $(1-p^{k-1})pB_k\equiv\frac{1}{2}f(0,1,C) \bmod p\mathbb{Z}_p$; le calcul de $f(0,1,C)$ fait dans la démonstration de la proposition 7.14 montre alors que $(1-p^{k-1})p\,B_k\equiv -1 \bmod p\mathbb{Z}_p$ d'où $p\,B_k\equiv -1 \bmod p\mathbb{Z}_p$.

§ 8. LE CALCUL DE $L_p(s,\epsilon)_{|s=1}$.

Ce paragraphe est indépendant du § 7 et peut donc se lire directement après le § 6. Comme on l'a vu dans la proposition 6.6, les fonctions $L_p(s,\epsilon)$ sont continues sur $\mathbb{Z}_p$ si le caractère ϵ est différent du caractère modulo f égal à 1 ; nous allons calculer $L_p(1,\epsilon)$ dans ce cas. De plus nous allons montrer que, si ϵ est le caractère égal à 1 modulo f, alors $L_p(s,\epsilon)$ qui est continue sur $\mathbb{Z}_p \setminus \{1\}$ ne peut pas se prolonger en une fonction continue sur $\mathbb{Z}_p$.

Rappelons qu'un caractère ϵ modulo f et un caractère ϵ' modulo f' sont dits équivalents si, pour tout x de $\mathbb{Z}$ premier à f et à f', on a $\epsilon(x) = \epsilon'(x)$. Un caractère modulo f est dit primitif s'il n'est équivalent à aucun caractère modulo un diviseur strict de f. Tout caractère est clairement équivalent à un caractère primitif et à un seul ; nous posons la définition suivante :

DEFINITION 8.1. *Soit* ϵ *un caractère modulo* f, *nous notons* ϵ^{pr} *le caractère primitif équivalent à* ϵ ; *le caractère* ϵ^{pr} *est un caractère modulo un entier* $f(\epsilon)$ *que nous appelons le conducteur de* ϵ.

On a alors

LEMME 8.2. *Soit* ϵ *un caractère modulo* f ; *notons* $S(\epsilon)$ *l'ensemble des nombres premiers* $\ell \neq p$ *qui divisent* f *sans diviser le conducteur* $f(\epsilon)$ *de* ϵ.

On a $L_p(s,\epsilon) = L_p(s,\epsilon^{pr}) \prod_{\ell \in S(\epsilon)} \left(1 - \frac{\epsilon^{pr}(\ell)}{\ell} <\ell>^{1-s}\right)$.

Démonstration. Soit k un entier positif et divisible par $p-1$ si $p \neq 2$, et par 2 si $p=2$. Le caractère ω^{-k} est le caractère modulo p égal à 1, donc le caractère $\varepsilon\omega^{-k}$ est le caractère modulo le p.p.c.m. $[f,p]$ de f et p qui, pour x premier à $[f,p]$, vaut $\varepsilon(x)$. Les diviseurs premiers de $[f,p]$ coïncidant avec ceux de fp, la fonction complexe $L(s,\varepsilon\omega^{-k})$ est égale au produit infini $\prod_{\ell \nmid fp} (1-\varepsilon(\ell)\ell^{-s})^{-1}$ pour les s de partie réelle plus grande que 1. De même on a $L(s,\varepsilon^{pr}\omega^{-k}) = \prod_{\ell \nmid f(\varepsilon)p} (1-\varepsilon^{pr}(\ell)\ell^{-s})^{-1}$

pour tout complexe s tel que $\mathrm{Re}(s) > 1$ et tout entier positif k divisible par $p-1$. On a donc $L(s,\varepsilon\omega^{-k}) = L(s,\varepsilon^{pr}\omega^{-k}) \prod_{\ell \in S(\varepsilon)} (1-\varepsilon^{pr}(\ell)\ell^{-s})$ pour tout complexe s tel que $\mathrm{Re}(s) > 1$; l'unicité du prolongement analytique montre que cette égalité reste vraie sur tout $\mathbb{C}$. En particulier, on a $L(1-k,\varepsilon\omega^{-k}) = L(1-k,\varepsilon^{pr}\omega^{-k}) \prod_{\ell \in S(\varepsilon)} (1-\frac{\varepsilon^{pr}(\ell)}{\ell}\ell^{k})$; mais, $p-1$ divisant k on a $\ell^k = \langle \ell \rangle^k$ donc (définition 6.4) notre égalité se réécrit $L_p(1-k,\varepsilon) = L_p(1-k,\varepsilon^{pr}) \prod_{\ell \in S(\varepsilon)} (1-\frac{\varepsilon^{pr}(\ell)}{\ell}\langle \ell \rangle^{k})$. D'autre part, l'ensemble des $1-k$ lorsque k décrit les entiers positifs divisibles par $p-1$ est dense dans $\mathbb{Z}_p$ et la fonction qui à $s \in \mathbb{Z}_p$ associe $\prod_{\ell \in S(\varepsilon)} (1-\frac{\varepsilon^{pr}(\ell)}{\ell}\langle \ell \rangle^{1-s})$ est continue et prend la valeur $\prod_{\ell \in S(\varepsilon)} (1-\frac{\varepsilon^{pr}(\ell)}{\ell}\langle \ell \rangle^{k})$ pour $s = 1-k$; on déduit donc de l'égalité précédente que $L_p(s,\varepsilon) = L_p(s,\varepsilon^{pr}) \prod_{\ell \in S(\varepsilon)} (1-\frac{\varepsilon^{pr}(\ell)}{\ell}\langle \ell \rangle^{1-s})$ C.Q.F.D.

Le lemme précédent ramène l'étude de $L_p(s,\varepsilon)$ en $s=1$ à celle de $L_p(s,\varepsilon^{pr})$ en $s=1$; dans la suite nous supposerons donc que ε est primitif i.e. $\varepsilon = \varepsilon^{pr}$ et donc $f = f(\varepsilon)$. Par définition $L_p(s,\varepsilon) = \dfrac{L_p(s,\varepsilon,C)}{1-\varepsilon(C)\langle C \rangle^{1-s}}$ pour tout $C \in \hat{\mathbb{Z}}^*$ tel que $\varepsilon(C)\langle C \rangle \neq 1$, où $L_p(s,\varepsilon,C)$ est défini, pour tout s de $\mathbb{Z}_p$, par $L_p(s,\varepsilon,C) = \int_{\mathbb{Z}_p} \langle x \rangle^{-s} \, d\nu_{C,\varepsilon\omega^{-1}}(x)$. Posons la définition suivante :

DEFINITION 8.3. Nous notons φ la fonction continue de $\mathbb{Z}_p$ dans lui-même définie par $\varphi(x) = x^{-1}$ si x est dans $\mathbb{Z}_p^*$ et $\varphi(x) = 0$ si x n'est pas dans $\mathbb{Z}_p^*$.

Avec cette définition de φ on a :

PROPOSITION 8.4. $L_p(1,\epsilon,C) = \int_{\mathbb{Z}_p} 1\, d(\varphi\, \nu_{C,\epsilon})(x)$ _où_ 1 _est la fonction constante égale à_ 1 _et où_ $\varphi\,\nu_{C,\epsilon}$ _est la mesure de densité_ φ _par rapport à_ $\nu_{C,\epsilon}$.

Démonstration.

$$L_p(1,\epsilon,C) = \int_{\mathbb{Z}_p} \langle x\rangle^{-1}\, d\nu_{C,\epsilon\omega^{-1}}(x) = \int_{\mathbb{Z}_p} \langle x\rangle^{-1}\omega^{-1}(x)\, d\nu_{C,\epsilon}(x)\ ;$$

mais $\langle x\rangle^{-1}\,\omega^{-1}(x) = \varphi(x)$, donc $L_p(1,\epsilon,C) = \int_{\mathbb{Z}_p} \varphi(x)\, d\nu_{C,\epsilon}(x) = \int_{\mathbb{Z}_p} 1\, d(\varphi\,\nu_{C,\epsilon})(x)$.

COROLLAIRE 8.5. $L_p(1,\epsilon,C)$ _est le terme constant de la série de_ $R[[T]]$ _associée à la mesure_ $\varphi\nu_{C,\epsilon}$.

En vertu de ce corollaire 8.5, il suffit pour calculer $L_p(1,\epsilon)$ de calculer la série associée à la mesure $\varphi\nu_{C,\epsilon}$; nous allons calculer cette série. Ce calcul sera long. Commençons par calculer la série $F_{\nu_{C,\epsilon}}(T)$ attachée à $F_{\nu_{C,\epsilon}}$. Nous aurons besoin des préliminaires suivants :

PROPOSITION 8.6. _Soit_ ν _une mesure sur_ $\mathbb{Z}_p$ _à valeurs dans_ R _et_ ν_1 _la mesure dont la densité par rapport à_ ν _est l'injection de_ $\mathbb{Z}_p$ _dans_ R. _On a_ $F_{\nu_1}(T) = (T+1)\frac{d}{dT}F_\nu(T)$ _où_ $\frac{d}{dT}$ _est l'opérateur de dérivation par rapport à_ T.

Démonstration. Soit $F_\nu(T) = \sum_{n\geq 0} b_n T^n$ et $F_{\nu_1}(T) = \sum_{n\geq 0} c_n T^n$; on a donc $b_n = \int_{\mathbb{Z}_p} \binom{x}{n}\, d\nu(x)$ et $c_n = \int_{\mathbb{Z}_p} \binom{x}{n}\, d\nu_1(x) = \int_{\mathbb{Z}_p} x\binom{x}{n}\, d\nu(x)$. L'assertion du lemme équivaut à $c_n = (n+1)b_{n+1} + n\,b_n$; cette égalité résulte de l'identité $x\binom{x}{n} = (n+1)\binom{x}{n+1} + n\binom{x}{n}$ qui se vérifie sans difficulté.

Dans la suite on notera D l'opérateur qui à une série formelle $F(T)$ associe la série formelle $DF(T) = (T+1)\frac{d}{dT}F(T)$. La proposition précédente admet le corollaire suivant :

COROLLAIRE 8.7. _Soit_ ν _une mesure sur_ $\mathbb{Z}_p$ _à valeurs dans_ R _et_ $F_\nu(T)$ _la série de_ $R[[T]]$ _qui lui est associée. Pour tout entier_ $n \geq 0$, _on a_

$D^n F_\nu(0) = \int_{\mathbb{Z}_p} x^n \, d\nu(x)$.

Démonstration. De la proposition précédente résulte que $D^n F_\nu(T)$ est la série associée à la mesure ν_n dont la densité par rapport à ν est l'application de $\mathbb{Z}_p$ dans R qui envoie x sur x^n. En conséquence, le terme constant $D^n F_\nu(0)$ de cette série est $\int_{\mathbb{Z}_p} \binom{x}{0} d\nu_n(x) = \int_{\mathbb{Z}_p} x^n d\nu(x)$ C.Q.F.D.

Désignons alors par K le corps des fractions de R et par $K[[T]]$ et $K[[X]]$ les anneaux de séries formelles sur K avec respectivement T et X comme indéterminée. Si e^X est la série $\sum_{n\geq 0} \frac{X^n}{n!}$ de $K[[X]]$, l'application Φ qui à $F(T)$ de $K[[T]]$ associe $G(X) = F(e^X-1)$ dans $K[[X]]$ est un isomorphisme de $K[[T]]$ sur $K[[X]]$ dont l'isomorphisme réciproque est l'application qui à $G(X)$ de $K[[X]]$ associe $F(T) = G(\log(1+T))$ si $\log(1+T) = \sum_{n\geq 1} \frac{(-1)^{n+1}T^n}{n}$ (la vérification de ce fait est un calcul standard). Posons alors la définition suivante :

DEFINITION 8.8. <u>Soit ν une mesure sur $\mathbb{Z}_p$ à valeurs dans R et $F_\nu(T)$ la série de $R[[T]]$ qui lui est associée. On note $G^\nu(X)$ la série de $K[[X]]$ image de $F_\nu(T)$ par l'application Φ définie ci-dessus.</u>

On a alors :

PROPOSITION 8.9. <u>Soit ν une mesure sur $\mathbb{Z}_p$ à valeurs dans R. Si $G^\nu(X) = \sum_{n\geq 0} c_n X^n$, on a $c_n = \frac{1}{n!} \int_{\mathbb{Z}_p} x^n d\nu(x)$.</u>

Démonstration. Notons d l'opérateur de dérivation $\frac{d}{dX}$ dans $K[[X]]$; on a $n!c_n = d^n G^\nu(0)$. D'autre part on vérifie facilement que $d \circ \Phi = \Phi \circ D$, donc que $d^n \circ \Phi = \Phi \circ D^n$. Si $F_\nu(T)$ est la série de $R[[T]]$ associée à ν, on a $\Phi(F_\nu(T)) = G^\nu(X)$; on a donc $d^n G^\nu(X) = \Phi(D^n F_\nu(T))$. En conséquence $n!c_n = d^n G^\nu(0)$ est le terme constant de l'image par Φ de $D^n F_\nu(T)$; celui-ci, comme on le voit sur la définition de Φ, est le terme constant de $D^n F_\nu(T)$. On a donc $n!c_n = D^n F_\nu(0)$ et notre proposition résulte du corollaire 8.7.

Pour calculer $F_{\nu_{C,\epsilon}}(T)$, il suffit donc de calculer $G^{\nu_{C,\epsilon}}(X)$ et de substituer $\log(1+T)$ à X dans cette dernière série ; c'est ce que nous allons faire. On a :

PROPOSITION 8.10. Soit ϵ un caractère primitif modulo f et C un élément de $\hat{\mathbb{Z}}^*$, alors

1) si $f \neq 1$ on a $G^{\nu_{C,\epsilon}}(X) = -\sum_{t=1}^{f-1} \epsilon(t) \frac{e^{Xt}}{e^{Xf}-1} + C_p \epsilon(C) \sum_{t=1}^{f-1} \frac{e^{XtC_p}}{e^{XfC_p}-1}$.

2) si $f = 1$ (donc $\epsilon(x) = 1$ pour tout x de $\mathbb{Z}$ et $\nu_{C,\epsilon} = \nu_C$) on a

$$G^{\nu_C}(X) = -\frac{e^X}{e^X-1} + C_p \frac{e^{C_pX}}{e^{C_pX}-1}.$$

Démonstration. Pour tout $n \geq 0$, on a $\int_{\mathbb{Z}_p} x^n d\nu_{C,\epsilon}(x) = \int_{\hat{\mathbb{Z}}} y_p^n \epsilon(y) d\mu_C(y)$; on a vu (prop. 3.10) que cette dernière intégrale vaut $\Delta_C(-n,\epsilon)$ donc $\int_{\mathbb{Z}_p} x^n d\nu_{C,\epsilon}(x) = \Delta_C(-n,\epsilon)$. Mais $\Delta_C(-n,\epsilon) = (1-C_p^{n+1}\epsilon(C))\, L(-n,\epsilon)$ puisque ϵ est un caractère, donc on tire de la proposition 8.9 que $G^{\nu_{C,\epsilon}}(X) = \sum_{n\geq 0} L(-n,\epsilon) \frac{X^n}{n!} - \epsilon(C) C_p \sum_{n\geq 0} L(-n,\epsilon) \frac{(XC_p)^n}{n!}$.

Posons $h(X) = \sum_{n\geq 0} L(-n,\epsilon) \frac{X^n}{n!}$; l'égalité précédente se réécrit $G^{\nu_{C,\epsilon}}(X) = h(X) - \epsilon(C)\, C_p h(XC_p)$. Supposons maintenant que $f \neq 1$; on a

$L(-n,\epsilon) = -\frac{f^n}{n+1} \sum_{t=1}^{f} \epsilon(t) B_{n+1}(\frac{t}{f})$ donc

$$h(X) = -\sum_{n\geq 0}\left[\frac{f^n}{n+1}\left(\sum_{t=1}^{f} \epsilon(t) B_{n+1}(\tfrac{t}{f})\right)\frac{X^n}{n!}\right] = -\frac{1}{Xf}\left[\sum_{n\geq 0}\left(\sum_{t=1}^{f} \epsilon(t) B_{n+1}(\tfrac{t}{f})\right)\frac{(Xf)^{n+1}}{(n+1)!}\right].$$

Puisque ϵ est primitif, l'hypothèse $f \neq 1$ implique l'existence d'un x premier à f tel que $\epsilon(x) \neq 1$ et donc $\sum_{t=1}^{f} \epsilon(t) = 0$; en conséquence $\sum_{t=1}^{f} \epsilon(t) B_0(\frac{t}{f}) = 0$ et

$$h(X) = -\frac{1}{Xf}\left[\sum_{k\geq 0}\left(\sum_{t=1}^{f} \epsilon(t) B_k(\tfrac{t}{f})\right)\frac{(Xf)^k}{k!}\right] = -\frac{1}{Xf}\left[\sum_{t=1}^{f} \epsilon(t)\left(\sum_{k\geq 0} B_k(\tfrac{t}{f})\frac{(Xf)^k}{k!}\right)\right]$$

$$= -\frac{1}{Xf}\sum_{t=1}^{f} \epsilon(t) \frac{Xfe^{Xt}}{e^{Xf}-1}$$

puisque $\sum_{k\geq 0} B_k(Y)\frac{U^k}{k!} = \frac{Ue^{UY}}{e^U-1}$ par définition des polynômes B_k. Enfin, $\epsilon(f)$ étant égal à 0 puisque $f \neq 1$, on a $h(X) = -\sum_{t=1}^{f-1} \epsilon(t) \frac{e^{Xt}}{e^{Xf}-1}$; on achève la démonstration de la première égalité en reportant cette valeur de $h(X)$ dans l'égalité $G^{\nu_{C,\epsilon}}(X) = h(X) - \epsilon(C)\, C_p h(XC_p)$.

Si $f = 1$, on a $L(-n,\epsilon) = L(-n,1) = -\frac{B_{n+1}(1)}{n+1}$. Si $n > 0$ on vérifie que $B_{n+1}(1) = B_{n+1}(0)$; de plus $-B_1(1) = B_1(0)$ et $B_o(0) = 1$. Pour tout $k \geq 0$ on pose $B_k(0) = B_k$; on a alors

$$h(X) = -\frac{1}{X}\Big(\sum_{n\geq 0} B_{n+1}\frac{X^{n+1}}{(n+1)!}\Big) + 2B_1 = -\frac{1}{X}\Big(\sum_{k\geq 0} B_k \frac{X^k}{k!}\Big) + 2B_1 + \frac{B_o}{X}$$

soit $h(X) = -\frac{1}{e^X-1} - 1 + \frac{1}{X} = -\frac{e^X}{e^X-1} + \frac{1}{X}$. On achève la démonstration de la seconde égalité en reportant cette expression de $h(X)$ dans $G^{\nu_{C,1}}(X) = G^{\nu_C}(X) = h(X) - C_p h(XC_p)$.

COROLLAIRE 8.11. <u>Soit</u> ϵ <u>un caractère primitif modulo</u> f <u>et</u> C <u>un élément de</u> $\hat{\mathbb{Z}}^*$; <u>si</u> $f \neq 1$ <u>on a</u> $F_{\nu_{C,\epsilon}}(T) = -\sum_{t=1}^{f-1} \epsilon(t) \frac{(1+T)^t}{(1+T)^f-1} + C_p\, \epsilon(C) \sum_{t=1}^{f-1} \frac{(1+T)^{tC_p}}{(1+T)^{fC_p}-1}$; <u>si</u> $f = 1$ <u>on a</u> $F_{\nu_C}(T) = -\frac{1+T}{T} + C_p \frac{(1+T)^{C_p}}{(1+T)^{C_p}-1}$.

Il reste maintenant à déduire la série $F_{\varphi\nu_{C,\epsilon}}(T)$ de la série $F_{\nu_{C,\epsilon}}(T)$. Pour cela définissons pour toute mesure ν sur $\mathbb{Z}_p$ à valeurs dans R la mesure $\tilde{\nu}$ de la façon suivante :

si f est une fonction continue de $\mathbb{Z}_p$ dans R nous notons $\tilde{f}$ la fonction définie par $\tilde{f}(x) = f(x)$ si x est dans $\mathbb{Z}_p^*$ et $\tilde{f}(x) = 0$ si x est dans $\mathbb{Z}_p$ mais pas dans $\mathbb{Z}_p^*$; il est clair que $\tilde{f}$ est une fonction continue de $\mathbb{Z}_p$ dans R et que l'on définit une mesure $\tilde{\nu}$ sur $\mathbb{Z}_p$ à valeur dans R par $\int_{\mathbb{Z}_p} f(x)\,d\tilde{\nu}(x) = \int_{\mathbb{Z}_p} \tilde{f}(x)\,d\nu(x)$. On a :

LEMME 8.12. <u>Soit</u> ν <u>une mesure sur</u> $\mathbb{Z}_p$ <u>à valeurs dans</u> R <u>et</u> φ <u>la fonction définie en 8.3 ; on note</u> $\varphi\nu$ <u>la mesure de densité</u> φ <u>par rapport à</u> ν <u>et</u>

$(\varphi\nu)_1$ <u>la mesure dont la densité par rapport à</u> $\varphi\nu$ <u>est l'injection canonique de</u> $\mathbb{Z}_p$ <u>dans</u> R. <u>On a</u> $(\varphi\nu)_1 = \tilde{\nu}$.

<u>Démonstration</u>. Pour tout $f \in \mathrm{Cont}(\mathbb{Z}_p, R)$, on a

$$\int_{\mathbb{Z}_p} f(x)\, d[(\varphi\nu)_1](x) = \int_{\mathbb{Z}_p} x f(x)\, d(\varphi\nu)(x) = \int_{\mathbb{Z}_p} x\varphi(x) f(x)\, d\nu(x) = \int_{\mathbb{Z}_p} \tilde{f}(x)\, d\nu(x) = \int_{\mathbb{Z}_p} f(x)\, d\tilde{\nu}(x)$$

ce qui prouve notre assertion.

LEMME 8.13. <u>Soit</u> ν <u>une mesure sur</u> $\mathbb{Z}_p$ <u>à valeurs dans</u> R <u>et</u> $F_\nu(T)$ <u>la série de</u> $R[[T]]$ <u>qui lui est associée. La série</u> $F_{\tilde{\nu}}(T)$ <u>associée à</u> $\tilde{\nu}$ <u>est donnée par</u> $F_{\tilde{\nu}}(T) = F_\nu(T) - \frac{1}{p} \sum_{\zeta \in \mu_p} F_\nu(\zeta(1+T)-1)$, <u>si</u> μ_p <u>désigne le groupe des racines de l'unité de</u> $\overline{\mathbb{Q}}_p$ <u>dont l'ordre divise</u> p.

<u>Démonstration</u>. $\zeta - 1$ est un entier p-adique de $\mathbb{Q}_p(\zeta)$ non inversible, donc ζ^x est bien défini pour tout x de $\mathbb{Z}_p$. Si x n'est pas dans $\mathbb{Z}_p^*$, on a $\zeta^x = 1$. Si x est dans $\mathbb{Z}_p^*$, l'application qui à ζ de μ_p associe ζ^x est une bijection de μ_p sur lui-même et donc $\sum_{\zeta \in \mu_p} \zeta^x = 0$. En conséquence, pour tout x de $\mathbb{Z}_p$ et tout f de $\mathrm{Cont}(\mathbb{Z}_p, R)$, on a $\tilde{f}(x) = (1 - \frac{1}{p} \sum_{\zeta \in \mu_p} \zeta^x) f(x)$; on a donc

$$\int_{\mathbb{Z}_p} f(x)\, d\tilde{\nu}(x) = \int_{\mathbb{Z}_p} f(x)\, d\nu(x) - \frac{1}{p} \Big[\sum_{\zeta \in \mu_p} \int_{\mathbb{Z}_p} \zeta^x f(x)\, d\nu(x) \Big]$$

et on conclut avec le lemme 7.13.

Pour toute série formelle $F(T)$ de $R[[T]]$ nous posons $\widetilde{F(T)} = F(T) - \frac{1}{p} \sum_{\zeta \in \mu_p} F(\zeta(1+T)-1)$; on a alors :

PROPOSITION 8.14. <u>Soit</u> ν <u>une mesure sur</u> $\mathbb{Z}_p$ <u>à valeur dans</u> R <u>et</u> $F_\nu(T)$ <u>la série de</u> $R[[T]]$ <u>qui lui est associée. La série</u> $F_{\varphi\nu}(T)$ <u>associée à la mesure</u> $\varphi\nu$ <u>vérifie les deux conditions suivantes</u> :

1) $D F_{\varphi\nu}(T) = \widetilde{F_\nu(T)}$

2) $F_{\varphi\nu}(T) = \widetilde{F_{\varphi\nu}(T)}$.

Démonstration. D'après la proposition 8.6, la série $DF_{\varphi\nu}(T)$ est égale à la série $F_{(\varphi\nu)_1}(T)$; le lemme 8.12 montre que cette série est égale à $F_{\widetilde{\nu}}(T)$ qui est $\widetilde{F_\nu(T)}$ d'où 1). Pour 2) il suffit de remarquer que $\varphi\nu = \widehat{\varphi\nu}$ ce qui est clair.

Rappelons que nous cherchons à calculer $F_{\varphi\nu_{C,\epsilon}}(T)$ et que nous connaissons (corollaire 8.11) $F_{\nu_{C,\epsilon}}(T)$. En vertu de la proposition 8.14, nous avons donc à regarder l'équation $DX(T) = \widetilde{F}_{\nu_{C,\epsilon}}(T)$ où $X(T)$ est l'inconnue. Pour cela introduisons le sous-anneau An de $\bar{\Phi}_p[[T]]$ formé des séries $\sum_{n\geq 0} a_n T^n$ telles que $\sum_{n\geq 0} a_n \xi^n$ converge pour tout ξ de $\bar{\Phi}_p$ dont la valeur absolue p-adique est plus petite que 1. L'anneau An contient $R[[T]]$; de plus, pour tout $F(T)$ de An et tout ζ de μ_p, la série $F(\zeta(1+T)-1)$ est bien définie puisque la valeur absolue p-adique de $\zeta - 1$ est plus petite que 1 ; on peut donc poser $\widetilde{F}(T) = F(T) - \frac{1}{p}\sum_{\zeta\in\mu_p} F(\zeta(1+T)-1)$ pour tout $F(T)$ de An. L'opérateur D se définit sur An comme sur $R[[T]]$ et il envoie An dans lui-même. On a

LEMME 8.15. <u>Soit</u> $F(T)$ <u>un élément de</u> An ; <u>si l'équation</u> $DX(T) = F(T)$ <u>admet une solution</u> $X_o(T)$ <u>dans</u> An, <u>alors</u> $\widetilde{X}_o(T)$ <u>est une solution du système de deux équations</u> $DY(T) = \widetilde{F}(T)$ <u>et</u> $\widetilde{Y}(T) = Y(T)$ <u>et c'est la seule</u>.

Démonstration. L'opérateur D est linéaire, donc $D\widetilde{X}_o(T) = \widetilde{DX_o}(T) = \widetilde{F}(T)$; de plus on a $\widetilde{\widetilde{X}}_o(T) = \widetilde{X}_o(T)$ puisque, pour toute série $G(T)$ de An, on a $\widetilde{\widetilde{G}}(T) = \widetilde{G}(T)$: en effet, si $\zeta\in\mu_p$, on a $\widetilde{G}(\zeta(1+T)-1) = G(\zeta(1+T)-1) - \frac{1}{p}\sum_{\eta\in\mu_p} G(\zeta\eta(1+T)-1)$ donc on a $\sum_{\zeta\in\mu_p}\widetilde{G}(\zeta(1+T)-1) = 0$ ce qui implique $\widetilde{\widetilde{G}}(T) = \widetilde{G}(T)$.

Il reste à voir que $\widetilde{X}_o(T)$ est la seule solution de notre système de deux équations en $Y(T)$; supposons que $Y_o(T)$ en est une autre, alors $D(\widetilde{X}_o(T) - Y_o(T)) = 0$ donc $Y_o(T) = \widetilde{X}_o(T) + C$ où C est une constante ; de plus $\widetilde{Y}_o(T) = Y_o(T) = \widetilde{X}_o(T) + \widetilde{C}$ et $\widetilde{C} = 0$ donc $Y_o(T) = \widetilde{X}_o(T)$ ce qui achève la démonstration.

Cherchons maintenant une solution dans An à l'équation $DX(T)=F_{\nu_{C,\epsilon}}(T)$. Pour cela nous aurons besoin de définir le logarithme de certaines séries formelles. Nous notons ord_p la valuation dans $\overline{\mathbb{Q}}_p$ normalisée par $\mathrm{ord}_p(p) = 1$; si ξ est dans $\overline{\mathbb{Q}}_p^*$, on a donc $\mathrm{ord}_p(\xi) > 0$ si et seulement si la valeur absolue de ξ est plus petite que 1. Pour tout ξ de $\overline{\mathbb{Q}}_p^*$ tel que $\mathrm{ord}_p(\xi) > 0$, on vérifie facilement que la série $\sum_{n\geq 1}(-1)^{n+1}\frac{\xi^n}{n}$ converge ; on note $\log_p(1+\xi)$ sa somme. La fonction $\log_p$ est donc définie sur l'ensemble des x de $\overline{\mathbb{Q}}_p^*$ tels que $\mathrm{ord}_p(x-1) > 0$; il est clair que cet ensemble est un sous-groupe multiplicatif de $\overline{\mathbb{Q}}_p^*$ et on vérifie que, si x_1 et x_2 sont dans ce groupe, on a $\log_p x_1 + \log_p x_2 = \log_p(x_1 x_2)$. On prolonge cette fonction $\log_p$ à $\overline{\mathbb{Q}}_p^*$ tout entier de la manière suivante : si $x \in \overline{\mathbb{Q}}_p^*$, il existe deux entiers rationnels non nuls e et a tels que $x^e = p^a v$ avec v dans $\overline{\mathbb{Q}}_p^*$ tel que $\mathrm{ord}_p(v) = 0$; de plus il existe un entier positif f tel que $\mathrm{ord}_p(v^{p^f-1}-1) > 0$; on pose alors $\log_p(x) = \frac{1}{e(p^f-1)}\log_p(v^{p^f-1})$. On vérifie que $\log_p(x)$ ne dépend ni du choix de e ni du choix de f et que $\log_p$ est un homomorphisme du groupe multiplicatif $\overline{\mathbb{Q}}_p^*$ vers le groupe additif $\overline{\mathbb{Q}}_p$. Passons aux séries formelles ; on pose toujours $\log(1+T) = \sum_{n\geq 1}(-1)^{n+1}\frac{T^n}{n}$. Si $F(T)$ est une série de $\overline{\mathbb{Q}}_p[[T]]$ dont le terme constant est égal à 1, on peut substituer $F(T)-1$ à T dans la série $\log(1+T)$; on note $(\log\circ F)(T)$ le résultat de cette substitution. Si le terme constant f_o de $F(T)$ est non nul, on pose $(\log\circ F)(T) = \log_p(f_o) + (\log\circ f_o^{-1}F)(T)$. On a :

LEMME 8.16. <u>Soit</u> $F(T)$ <u>un élément de</u> $\overline{\mathbb{Q}}_p[[T]]$ <u>dont le terme constant est non nul.</u> <u>Si</u> $F'(T)$ <u>désigne la dérivée de</u> $F(T)$, <u>alors la dérivée de</u> $(\log\circ F)(T)$ <u>est</u> $\frac{F'(T)}{F(T)}$.

<u>Démonstration</u>. Supposons d'abord que $F(T) = 1+G(T)$ avec $G(T)$ dans $T\overline{\mathbb{Q}}_p[[T]]$; on a $(\log\circ F)(T) = \sum_{n\geq 1}(-1)^{n+1}\frac{G(T)^n}{n}$, donc $(\log\circ F)'(T) = G'(T)\sum_{n\geq 1}(-1)^{n+1}G(T)^{n-1} = \frac{G'(T)}{1+G(T)} = \frac{F'(T)}{F(T)}$. Si le terme constant f_o de $F(T)$ est non nul, on a $(\log\circ F)(T) = \log_p(f_o) + (\log\circ f_o^{-1}F)(T)$ donc

$$(\log\circ F)'(T) = \frac{(f_o^{-1}F)'(T)}{f_o^{-1}F(T)} = \frac{F'(T)}{F(T)} .$$

LEMME 8.17. Soit K une extension finie de $\mathbb{Q}_p$ contenant le groupe μ_p des racines de l'unité de $\overline{\mathbb{Q}}_p$ d'ordre divisant p et soit R son anneau des entiers. Soit $F(T)$ une série formelle de $R[[T]]$ dont le terme constant f_o est inversible dans R, alors :

1) $(\log\circ F)(T)$ est une série formelle de An.

2) $\widetilde{(\log\circ F)}(0) = \log_p(F(0)) - \frac{1}{p}\sum_{r\in\mu_p} \log_p(F(r-1))$.

Démonstration. 1) Posons $F(T) = \sum_{n\geq 0} f_n T^n$ et $(\log\circ F)(T) = \sum_{n\geq 0} g_n T^n$; pour tout $n \geq 1$, g_n est de la forme $\sum_{i=1}^{n} \frac{a_i}{i}$ où les a_i sont des sommes et des différences de produits de coefficients de $f_o^{-1}F(T)$; on a donc $\mathrm{ord}_p(a_i) \geq 0$ pour tout i, donc $\mathrm{ord}_p(g_n) \geq -\mathrm{Sup}\{\mathrm{ord}_p(i)\ ;\ i = 1,\ldots,n\}$; on en déduit que $\sum_{n\geq 0} g_n T^n$ est dans An, ce qu'on voulait.

2) On vérifie directement que $\widetilde{(\log\circ F)}(T) = \widetilde{(\log\circ f_o^{-1}F)}(T)$ et que $\log_p(F(0)) - \frac{1}{p}\sum_{r\in\mu_p} \log_p(F(r-1)) = \log_p(f_o^{-1}F(0)) - \frac{1}{p}\sum_{r\in\mu_p} \log_p(f_o^{-1}F(r-1))$; on peut donc supposer $f_o = 1$, ce que nous faisons dans la suite. On a alors $\widetilde{(\log\circ F)}(0) = (\log\circ F)(0) - \frac{1}{p}\sum_{r\in\mu_p} (\log\circ F)(r-1)$. L'égalité $(\log\circ F)(0) = \log_p(F(0))$ est claire ; le théorème 2 de [1], chap. 4, § 5; prouve l'égalité $(\log\circ F)(r-1) = \log_p(F(r-1))$ pour tout r de μ_p ; cela achève la démonstration.

On est maintenant en mesure de démontrer le théorème suivant :

THEOREME 8.18. Si ϵ est le caractère unité (i.e. $\epsilon(x) = 1$ pour tout x de $\mathbb{Z}$) et si C est un élément de $\hat{\mathbb{Z}}^*$, on a $L_p(1,\epsilon,C) = (1-\frac{1}{p})\log_p(C_p)$.

Démonstration. Posons $H(T) = \frac{(1+T)^{C_p}-1}{T}$, c'est un élément de $\mathbb{Z}_p[[T]]$ dont le terme constant C_p est inversible. Le lemme 8.17, 1) montre que $(\log\circ H)(T)$ est dans An. De plus on tire du lemme 8.16 que $D(\log\circ H)(T) = -\frac{1+T}{T} + C_p\,\frac{(1+T)^{C_p}}{(1+T)^{C_p}-1}$

c'est-à-dire (corollaire 8.11) que $D(\log\circ H)(T) = F_{\nu_C}(T)$. En conséquence, on tire de la proposition 8.14 et du lemme 8.15 que $F_{\varphi\nu_C}(T) = (\widetilde{\log\circ H})(T)$ et donc (corollaire 8.5) $L_p(1,\epsilon,C) = (\widetilde{\log\circ H})(0)$. On conclut à l'aide du lemme 8.17, 2) que $L_p(1,\epsilon,C) = (1-\frac{1}{p})\log_p C_p - \frac{1}{p}\sum_{r\in\mu_p\setminus\{1\}} \log_p(\frac{r^{C_p}-1}{r-1})$; mais $\prod_{r\in\mu_p\setminus\{1\}} \frac{r^{C_p}-1}{r-1} = 1$, donc $\sum_{r\in\mu_p\setminus\{1\}} \log_p(\frac{r^{C_p}-1}{r-1}) = 0$ donc $L_p(1,\epsilon,C) = (1-\frac{1}{p})\log_p C_p$, C.Q.F.D.

COROLLAIRE 8.19. Si ϵ est le caractère unité, la fonction $L_p(s,\epsilon)$ ne peut pas se prolonger en une fonction continue sur $\mathbb{Z}_p$ tout entier.

Démonstration. $L_p(s,\epsilon) = \dfrac{L_p(s,\epsilon,C)}{1-\langle C\rangle^{1-s}}$ si C est un élément de $\hat{\mathbb{Z}}^*$ tel que $\langle C\rangle \neq 1$. Le dénominateur de $L_p(s,\epsilon)$ s'annule en $s=1$ et le numérateur vaut $(1-\frac{1}{p})\log_p(C_p)$; montrons qu'il n'est pas nul ce qui impliquera notre assertion : on a $C_p = \omega(C_p)\langle C_p\rangle$ donc $\log_p(C_p) = \log_p(\langle C_p\rangle)$; par définition $\langle C_p\rangle = \langle C\rangle$, donc $\langle C_p\rangle$ est différent de 1 ; comme $\langle C_p\rangle \neq 1$ est dans $1+2p\mathbb{Z}_p$, on a $\log_p(\langle C_p\rangle) \neq 0$ (en effet $\log_p$ induit une bijection de $1+2p\mathbb{Z}_p$ sur $2p\mathbb{Z}_p$ comme on peut le voir dans [1], chap. IV, § 5, par exemple).

REMARQUE 8.20. Le lemme 8.2 joint au corollaire 8.19 montre que, si f est un entier positif quelconque et si 1_f est le caractère modulo f égal à 1, la fonction $L_p(s,1_f)$ ne peut pas se prolonger en une fonction continue sur $\mathbb{Z}_p$ tout entier. Cela montre en particulier que $L_p(s,1_f)$ n'est pas une fonction d'Iwasawa, donc (corollaire 7.7) que $G(T,1_f)$ n'est pas dans $R[[T]]$.

Il reste à regarder le cas $\epsilon \neq 1$. On a :

THEOREME 8.21. Soit ϵ un caractère primitif pair modulo f qui n'est pas le caractère unité ; si ζ est une racine primitive $f^{\text{ième}}$ de 1 et si $\tau(\epsilon) = \sum_{t=1}^{f-1} \epsilon(t)\zeta^t$, on a $L_p(1,\epsilon) = -\frac{\tau(\epsilon)}{f}(1-\frac{\epsilon(p)}{p})\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\epsilon}(b)\log_p(1-\zeta^{-b})$ où $\bar{\epsilon}(b) = \epsilon(b)^{-1}$ si $b\in(\mathbb{Z}/f\mathbb{Z})^*$.

Démonstration. Commençons par établir deux lemmes :

LEMME 8.22. Soit C un élément de $\hat{\mathbb{Z}}^*$, on a

$$F_{\nu_{C,\epsilon}}(T) = -\frac{\tau(\epsilon)}{f}\Big[\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\epsilon}(b)\Big(\frac{\zeta^{-b}(1+T)}{\zeta^{-b}(1+T)-1} - C_p\,\frac{\zeta^{-bC}(1+T)^{C_p}}{\zeta^{-bC}(1+T)^{C_p}-1}\Big)\Big]$$

en posant $\zeta^{-bC} = \zeta^x$ où x est un entier congru à $-bC$ modulo $f\hat{\mathbb{Z}}$.

Démonstration. On convient de poser $\bar{\epsilon}(b) = 0$ pour tout b non inversible modulo f. Soit U une indéterminée ; on a $\sum_{t=1}^{f-1} \epsilon(t)\,\frac{U^t}{U^f-1} = \sum_{b\in\mathbb{Z}/f\mathbb{Z}} \frac{A_b}{U-\zeta^b}$ avec $A_b = \frac{1}{f}\sum_{t=1}^{f-1} \epsilon(t)\,\frac{\zeta^{bt}}{\zeta^{-b}}$ soit $A_b = \frac{\zeta^b}{f}\,\tau(\epsilon)\,\bar{\epsilon}(b)$. De l'expression de $F_{\nu_{C,\epsilon}}(T)$ donnée dans le corollaire 8.11, on tire alors

$$F_{\nu_{C,\epsilon}}(T) = -\frac{\tau(\epsilon)}{f}\Big[\sum_{b\in\mathbb{Z}/f\mathbb{Z}} \Big(\frac{\bar{\epsilon}(b)}{\zeta^{-b}(1+T)-1} - C_p\,\epsilon(C)\,\frac{\bar{\epsilon}(b)}{\zeta^{-b}(1+T)^{C_p}-1}\Big)\Big].$$

Le caractère ϵ n'étant pas le caractère unité, le caractère $\bar{\epsilon}$ n'est pas non plus le caractère unité donc $\sum_{b\in\mathbb{Z}/f\mathbb{Z}} \bar{\epsilon}(b) = 0$; on en déduit

$$\sum_{b\in\mathbb{Z}/f\mathbb{Z}} \frac{\bar{\epsilon}(b)}{\zeta^{-b}(1+T)-1} = \sum_{b\in\mathbb{Z}/f\mathbb{Z}} \Big(\frac{\bar{\epsilon}(b)}{\zeta^{-b}(1+T)-1} + \bar{\epsilon}(b)\Big) = \sum_{b\in\mathbb{Z}/f\mathbb{Z}} \frac{\bar{\epsilon}(b)\,\zeta^{-b}(1+T)}{\zeta^{-b}(1+T)-1}.$$

De même on a $\sum_{b\in\mathbb{Z}/f\mathbb{Z}} \frac{\bar{\epsilon}(b)}{\zeta^{-b}(1+T)^{C_p}-1} = \sum_{b\in\mathbb{Z}/f\mathbb{Z}} \frac{\bar{\epsilon}(b)\,\zeta^{-b}(1+T)^{C_p}}{\zeta^{-b}(1+T)^{C_p}-1}$; cette dernière expression est égale à

$$\bar{\epsilon}(C)\sum_{b\in\mathbb{Z}/f\mathbb{Z}} \frac{\bar{\epsilon}(bC^{-1})\zeta^{-b}(1+T)^{C_p}}{\zeta^{-b}(1+T)^{C_p}-1} = \bar{\epsilon}(C)\sum_{b\in\mathbb{Z}/f\mathbb{Z}} \frac{\bar{\epsilon}(b)\,\zeta^{-bC}(1+T)^{C_p}}{\zeta^{-bC}(1+T)^{C_p}-1};$$

en remplaçant ces valeurs dans l'expression de $F_{\nu_{C,\epsilon}}(T)$ trouvée ci-dessus et en se rappelant que $\bar{\epsilon}(b) = 0$ si $b \notin (\mathbb{Z}/f\mathbb{Z})^*$, on obtient le lemme.

LEMME 8.23. Pour tout $b \in (\mathbb{Z}/f\mathbb{Z})^*$, posons $H_b(T) = \frac{\zeta^{-bC}(1+T)^{C_p}-1}{\zeta^{-b}(1+T)-1}$; la série $H_b(T)$ est dans $R[[T]]$ et son terme constant est dans R^* (R est l'anneau des entiers d'une extension finie de $\mathbb{Q}_p$ qui contient ζ).

<u>Démonstration</u>. $H_b(T)$ est le quotient de deux séries de $R[[T]]$; si f n'est pas une puissance de p, leurs termes constants qui sont respectivement $\zeta^{-bC}-1$ et $\zeta^{-b}-1$ sont dans R^* et il n'y a pas de problème. Si f est une puissance de p, alors $\zeta^{-b}-1$ n'est pas dans R^*, donc le coefficient de T est le premier coefficient de $\zeta^{-b}(1+T)-1$ à être dans R^*; en conséquence le théorème de préparation de Weierstrass p-adique ([14], [8]) affirme l'existence d'un $Q(T)\in R[[T]]$ et d'un $r\in R$ tels que $\zeta^{-bC}(1+T)^{C_p}-1=(\zeta^{-b}(1+T)-1)\,Q(T)+r$. Pour calculer r, faisons $T=\zeta^{b}-1$, il vient $\zeta^{-bC}\,\zeta^{bC_p}-1=r$; mais ζ étant d'ordre une puissance de p, on a $\zeta^{bC}=\zeta^{bC_p}$ donc $r=0$ et donc $H_b(T)=Q(T)\in R[[T]]$. Enfin, le terme constant de $H_b(T)=Q(T)$ est le quotient $\dfrac{\zeta^{-bC}-1}{\zeta^{-b}-1}$ qui est bien dans R^*.

Revenons à la démonstration du théorème.

Soit b dans $(\mathbb{Z}/f\mathbb{Z})^*$; le lemme 8.23 associé au lemme 8.17, 1) montre que $(\log\circ H_b)(T)$ est dans An. De plus on tire du lemme 8.16 que

$$D(\log\circ H_b)(T)=-\frac{\zeta^{-b}(1+T)}{\zeta^{-b}(1+T)-1}+C_p\,\frac{\zeta^{-bC}(1+T)^{C_p}}{\zeta^{-bC}(1+T)-1}\text{ ; posons}$$

$G(T)=\dfrac{\tau(\epsilon)}{f}\displaystyle\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\bar{\epsilon}(b)\,(\log\circ H_b)(T)$, le lemme 8.22 et ce qu'on vient de faire montrent que $G(T)$ est dans An et $DG(T)=F_{\nu_{C,\epsilon}}(T)$. On tire donc de la proposition 8.14 et du lemme 8.15 que $F_{\varphi\nu_{C,\epsilon}}(T)=\tilde{G}(T)$ et donc (corollaire 8.5) on a $L_p(1,\epsilon,C)=\tilde{G}(0)$. En explicitant $\tilde{G}(0)$, il vient $L_p(1,\epsilon,C)=\dfrac{\tau(\epsilon)}{f}\displaystyle\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\bar{\epsilon}(b)\widetilde{(\log\circ H_b)}(0)$ qui, d'après le lemme 8.17, 2) est $\dfrac{\tau(\epsilon)}{f}\displaystyle\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\bar{\epsilon}(b)(\log_p(H_b(0))-\frac{1}{p}\sum_{r\in\mu_p}\log_p(H_b(r-1)))$.

Si $\zeta^{-b}r\neq 1$, on a $H_b(r-1)=\dfrac{\zeta^{-bC}r^{C_p}-1}{\zeta^{-b}r-1}$; mais $r^{C_p}=r^{C}$ puisque r est une racine $p^{\text{ième}}$ de l'unité (ici $r^C=r^x$ si x est un entier congru à C modulo $p\hat{\mathbb{Z}}$) donc $H_b(r-1)=\dfrac{(\zeta^{-b}r)^C-1}{\zeta^{-b}r-1}$ ce qui montre que $H_b(r-1)$ ne dépend que de la valeur du produit $\zeta^{-b}r$. Si $\zeta^{-b}r=1$, alors ζ est une racine de l'unité d'ordre p donc $f=p$ (c'est le cas où ϵ est une puissance paire de ω) ; par définition de $H_b(T)$

on a $\zeta^{-bC}(1+T)^{C_p}-1 = (\zeta^{-b}(1+T)-1)H_b(T)$ ce qui donne en dérivant

$\zeta^{-bC}C_p(1+T)^{C_p-1} = \zeta^{-b}H_b(T) + (\zeta^{-b}(1+T)-1)H_b'(T)$; faisons $T = r-1 = \zeta^b-1$ de sorte que $\zeta^{-b}r = 1$, il vient $\zeta^{-bC}C_p\zeta^{b(C_p-1)} = \zeta^{-b}H_b(r-1) = \zeta^{-b}H_b(\zeta^b-1)$ d'où $H_b(\zeta^b-1) = \zeta^{-bC}\zeta^{bC_p}C_p$; mais ζ est une racine $p^{\text{ième}}$ de l'unité, donc $\zeta^{bC} = \zeta^{bC_p}$ et $H_b(\zeta^b-1) = C_p$ est indépendant de b. La quantité $H_b(r-1)$ ne dépendant que de la valeur de $\zeta^{-b}r$, il en est de même de $\log_p(H_b(r-1))$; nous poserons dans la suite $\log_p(H_b(r-1)) = h(\zeta^{-b}r)$. Avec cette notation on a donc

$$L_p(1,\epsilon,C) = \frac{\tau(\epsilon)}{f}\Big(\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\bar{\epsilon}(b)h(\zeta^{-b}) - \sum_{\substack{b\in(\mathbb{Z}/f\mathbb{Z})^*\\ r\in\mu_p}}\bar{\epsilon}(b)\,h(\zeta^{-b}r)\Big).$$

Pour achever la démonstration nous devons regarder séparément le cas où p divise f et celui où p ne divise pas f.

Si p divise f. Dans ce cas $\zeta^{\frac{f}{p}}$ est une racine de l'unité d'ordre p ; convenons de poser $h(\zeta^{-b}r) = 0$ si b n'est pas dans $(\mathbb{Z}/f\mathbb{Z})^*$, on a alors

$$\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\bar{\epsilon}(b)h(\zeta^{-b}r) = \sum_{\substack{b\in\mathbb{Z}/f\mathbb{Z}\\ a\in\mathbb{Z}/p\mathbb{Z}}}\bar{\epsilon}(b)h(\zeta^{-b+\frac{af}{p}}).$$

Pour tout B de $\mathbb{Z}/f\mathbb{Z}$ et tout a de $\mathbb{Z}/p\mathbb{Z}$, il existe un élément et un seul de $\mathbb{Z}/f\mathbb{Z}$ que nous notons $b_{a,B}$ tel que $-b_{a,B}+\frac{af}{p} = B$ dans $\mathbb{Z}/f\mathbb{Z}$; avec cette notation notre somme se réécrit $\sum_B h(\zeta^B)(\sum_{a\in\mathbb{Z}/p\mathbb{Z}}\bar{\epsilon}(b_{a,B}))$. Mais, lorsque a décrit $\mathbb{Z}/p\mathbb{Z}$, les $\frac{af}{p}$ décrivent le sous-groupe d'ordre p de $\mathbb{Z}/f\mathbb{Z}$ et les $b_{a,B}$ décrivent la classe de $-B$ modulo ce sous-groupe ; le caractère $\bar{\epsilon}$ étant primitif, on en déduit que $\sum_{a\in\mathbb{Z}/p\mathbb{Z}}\bar{\epsilon}(b_{a,B}) = 0$ pour tout B. En revenant à la formule donnant $L_p(1,\epsilon,C)$ on trouve donc $L_p(1,\epsilon,C) = \frac{\tau(\epsilon)}{f}\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\bar{\epsilon}(b)\,h(\zeta^{-b})$; mais $h(\zeta^{-b}) = \log_p\big(\frac{\zeta^{-bC}-1}{\zeta^{-b}-1}\big) = \log_p(\zeta^{-bC}-1) - \log_p(\zeta^{-b}-1)$ donc

$$\begin{aligned}L_p(1,\epsilon,C) &= \frac{\tau(\epsilon)}{f}\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\bar{\epsilon}(b)(\log_p(\zeta^{-bC}-1)-\log_p(\zeta^{-b}-1))\\ &= \frac{\tau(\epsilon)}{f}(\epsilon(C)-1)\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\bar{\epsilon}(b)\log_p(\zeta^{-b}-1).\end{aligned}$$

Enfin si C est tel que $\varepsilon(C) \neq 1$ on a $L_p(1,\varepsilon) = \dfrac{L_p(1,\varepsilon,C)}{1-\varepsilon(C)} = -\dfrac{\tau(\varepsilon)}{f} \sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\varepsilon}(b)\log_p(\zeta^{-b}-1)$

qui est la formule cherchée compte tenu de $\varepsilon(p) = 0$ puisque p divise f et de $\log_p(\zeta^{-b}-1) = \log_p(1-\zeta^{-b})$.

Si p ne divise pas f. Dans ce cas $\zeta^{-b}r \neq 1$ quel que soit b dans $(\mathbb{Z}/f\mathbb{Z})^*$ et r dans μ_p, donc $h(\zeta^{-b}r) = \log_p\left(\dfrac{(\zeta^{-b}r)^C-1}{\zeta^{-b}r-1}\right)$. La somme double $\sum_{\substack{b\in(\mathbb{Z}/f\mathbb{Z})^* \\ r\in\mu_p}} \bar{\varepsilon}(b)\, h(\zeta^{-b}r)$ est donc $\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\varepsilon}(b)\left[\sum_{r\in\mu_p} \log_p\left(\dfrac{(\zeta^{-b}r)^C-1}{\zeta^{-b}r-1}\right)\right]$ et on a

$$\sum_{r\in\mu_p} \log_p\left(\frac{(\zeta^{-b}r)^C-1}{\zeta^{-b}r-1}\right) = \log_p\left[\prod_{r\in\mu_p} ((\zeta^{-b}r)^C-1)\right] - \log_p\left[\prod_{r\in\mu_p} (\zeta^{-b}r-1)\right] ;$$

mais l'identité $X^p-1 = \prod_{r\in\mu_p}(X-r)$ montre que $\prod_{r\in\mu_p}(\zeta^{-b}r-1) = r^{-p}(\zeta^{-bp}-1) = \zeta^{-bp}-1$; de même, r^C décrivant μ_p quand r décrit μ_p, on a $\prod_{r\in\mu_p}((\zeta^{-b}r)^C-1) = \zeta^{-pbC}-1$. Notre somme double est donc égale à

$$\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\varepsilon}(b)\log_p(\zeta^{-bpC}-1) - \sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\varepsilon}(b)\log_p(\zeta^{-bp}-1) =$$

$$= (\varepsilon(pC) - \varepsilon(p)) \sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\varepsilon}(b)\log_p(\zeta^{-b}-1)$$

puisque p et pC sont inversibles modulo $f\hat{\mathbb{Z}}$. En revenant à la formule donnant $L_p(1,\varepsilon,C)$, on trouve donc

$$L_p(1,\varepsilon,C) = \frac{\tau(\varepsilon)}{f}\left[\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\varepsilon}(b)h(\zeta^{-b}) - \frac{\varepsilon(pC)-\varepsilon(p)}{p} \sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\varepsilon}(b)\log_p(\zeta^{-b}-1)\right] ;$$

comme précédemment, on voit que $\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\varepsilon}(b)h(\zeta^{-b}) = (\varepsilon(C)-1) \sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\varepsilon}(b)\log_p(\zeta^{-b}-1)$, donc compte tenu de $\varepsilon(pC)-\varepsilon(p) = \varepsilon(p)(\varepsilon(C)-1)$, il vient

$L_p(1,\varepsilon,C) = (\varepsilon(C)-1)\dfrac{\tau(\varepsilon)}{f}\left(1-\dfrac{\varepsilon(p)}{p}\right) \sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\varepsilon}(b)\log_p(\zeta^{-b}-1)$. Enfin, si C est tel que $\varepsilon(C) \neq 1$ on a

$$L_p(1,\varepsilon) = \frac{L_p(1,\varepsilon,C)}{1-\varepsilon(C)} = -\frac{\tau(\varepsilon)}{f}\left(1-\frac{\varepsilon(p)}{p}\right) \sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\varepsilon}(b)\log_p(\zeta^{-b}-1)$$

ce qui est la formule cherchée compte tenu de $\log_p(\zeta^{-b}-1) = \log_p(1-\zeta^{-b})$. Notre démonstration est achevée.

REMARQUE 8.24. On définit parfois $\tau(\epsilon)$ par la formule $\tau(\epsilon) = \sum_{t=1}^{f-1} \epsilon(t)\zeta^{-t}$; cela ne change rien ici puisque, ϵ étant pair, on a $\sum_{t=1}^{f-1} \epsilon(t)\zeta^{t} = \sum_{t=1}^{f-1} \epsilon(t)\zeta^{-t}$. D'autre part on a $\log_p(1-\zeta^b) = \log_p(1-\zeta^{-b})$ puisque $1-\zeta^b = -\zeta^b(1-\zeta^{-b})$; c'est pourquoi on trouve dans certains textes la formule $L_p(1,\epsilon) = -\frac{\tau(\epsilon)}{f}(1-\frac{\epsilon(p)}{p}) \sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\epsilon}(b)\log_p(1-\zeta^b)$ à la place de celle du théorème 8.21.

REMARQUE 8.25. Rappelons que, si ϵ est un caractère complexe qui est primitif modulo f et qui n'est pas le caractère unité, alors la fonction complexe $L(s,\epsilon)$ est holomorphe sur $\mathbb{C}$ tout entier ; sa valeur en $s=1$ est alors $L(1,\epsilon) = \frac{-\tau(\epsilon)}{f} \sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} \bar{\epsilon}(b)\log(1-\zeta^{-b})$ si $\tau(\epsilon) = \sum_{t=1}^{f} \epsilon(t)\zeta^t$ et si $\bar{\epsilon}$ est le caractère conjugué de ϵ. Bien que cette formule ressemble à celle que nous venons d'établir pour $L_p(1,\epsilon)$, elle n'a rien à voir avec elle car il n'y a rien de commun entre Log et $\log_p$. Rappelons rapidement comment on calcule $L(1,\epsilon)$: on choisit une racine de l'unité ζ d'ordre f dans $\mathbb{C}$; pour chaque $b\in\mathbb{Z}/f\mathbb{Z}$, on note ψ_b la fonction de $\mathbb{Z}/f\mathbb{Z}$ dans $\mathbb{C}$ définie par $\psi_b(x) = \zeta^{-bx}$; pour tout caractère primitif ϵ, on a $\epsilon(x) = \sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*} A_b\psi_b(x)$ avec $A_b = \frac{\tau(\epsilon)}{f}\bar{\epsilon}(b)$ (c'est là que "primitif" intervient) ; les séries de Dirichlet $\sum_{n\geq 1} \psi_b(n)n^{-s}$ et $\sum_{n\geq 1}\epsilon(n)n^{-s}$ convergent pour $\mathrm{Re}(s) > 0$ (car les sommes partielles $\sum_M^N \psi_b(n)$ et $\sum_M^N \epsilon(n)$ sont bornées indépendamment de M et N) donc on a $L(s,\epsilon) = \frac{\tau(\epsilon)}{f}\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\bar{\epsilon}(b)L(s,\psi_b)$ pour tout s de ce domaine ; en particulier $L(1,\epsilon) = \frac{\tau(\epsilon)}{f}\sum_{b\in(\mathbb{Z}/f\mathbb{Z})^*}\bar{\epsilon}(b)L(1,\psi_b)$; on conclut alors en remarquant que $L(1,\psi_b) = \sum_{n\geq 1}\frac{\zeta^{-nb}}{n} = -\mathrm{Log}(1-\zeta^{-b})$.

§ 0. RAPPELS SUR LES CORPS ABELIENS.

Considérons tout d'abord un corps de nombre K ; nous notons D la valeur absolue de son discriminant, R son régulateur, h son nombre de classes, w le nombre de racines de l'unité contenues dans K et r_1 et $2r_2$ le nombre des plongements réels et complexes de K. Si I désigne l'ensemble des idéaux entiers non nuls de K, la série $\sum_{\underline{a}\in I} N(\underline{a})^{-s}$ où $N\underline{a}$ est la norme de l'idéal $\underline{a}$ converge pour tout complexe s de partie réelle plus grande que 1 ; sa somme est une fonction holomorphe sur ce domaine qui se prolonge en une fonction méromorphe sur $\mathbb{C}$ tout entier que nous notons ζ_K. On a ([7] par exemple) :

RESULTAT 0.1. <u>Le seul pôle de</u> ζ_K <u>est un pôle simple en</u> $s=1$ <u>de résidu</u> $\mathrm{Res}_{s=1}\zeta_K(s) = \dfrac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{D}}$ <u>(où</u> $\sqrt{D}$ <u>est le nombre positif dont le carré est</u> D).

RESULTAT 0.2. <u>Soit</u> $\xi_K(s) = A^s\,\Gamma(\frac{s}{2})^{r_1}\,\Gamma(s)^{r_2}\,\zeta_K(s)$ <u>avec</u> $A = 2^{-r_2}\sqrt{D}\;\pi^{-(r_1+2r_2)/2}$. <u>La fonction</u> ξ_K <u>est méromorphe sur</u> $\mathbb{C}$ <u>et vérifie l'équation fonctionnelle</u> $\xi_K(s) = \xi_K(1-s)$.

Supposons maintenant que K est un corps abélien sur $\mathbb{Q}$; nous notons G son groupe de Galois. Pour tout entier positif f on désigne par μ_f le groupe des racines $f^{\text{ièmes}}$ de l'unité ; on sait qu'il existe un f tel que $K \subset \mathbb{Q}(\mu_f)$. En associant à un élément σ de $\mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q})$ l'élément x de $(\mathbb{Z}/f\mathbb{Z})^*$ tel que $\sigma(\zeta) = \zeta^x$ pour tout ζ de μ_f, on identifie $\mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q})$ et $(\mathbb{Z}/f\mathbb{Z})^*$; par l'intermédiaire de cette identification le groupe $(\mathbb{Z}/f\mathbb{Z})^*$ se projette canoniquement sur G si $K \subset \mathbb{Q}(\mu_f)$. Si ϵ est un caractère de G (i.e. un homomorphisme du groupe G vers le groupe $\mathbb{C}^*$) et si f est un entier tel que $K \subset \mathbb{Q}(\mu_f)$, on note ϵ_f le caractère modulo f obtenu en composant ϵ et la projection canonique de $(\mathbb{Z}/f\mathbb{Z})^*$ sur G. Le caractère primitif équivalent à ϵ_f ne dépend pas de f ; on le note ϵ^{pr} et on note $f(\epsilon)$ l'entier positif modulo lequel il est défini ; on dit que $f(\epsilon)$ est le conducteur du caractère ϵ de G. On note $\hat{G}$ le groupe des caractères de G. Pour tout ϵ de $\hat{G}$, on pose $L(s,\epsilon) = L(s,\epsilon^{pr})$ pour s dans $\mathbb{C}$ (on rappelle que $L(s,\epsilon^{pr}) = \sum\limits_{\substack{n\geq 0\\ (n,f(\epsilon))=1}} \epsilon^{pr}(n)n^{-s}$ définit une fonction holomorphe sur le demi-plan $\mathrm{Re}(s) > 1$ et se prolonge en une fonction méromorphe sur $\mathbb{C}$ tout entier). On a ([7] par exemple).

RESULTAT 0.3. <u>Si</u> $\epsilon \neq 1$ <u>est un élément de</u> $\hat{G}$, <u>la fonction</u> $L(s,\epsilon)$ <u>est holomorphe sur</u> $\mathbb{C}$ (si $\epsilon = 1$, <u>on a clairement</u> $L(s,1) = \zeta_{\mathbb{Q}}(s)$ <u>donc</u> $L(s,1)$ <u>a un pôle simple de résidu égal à</u> 1 <u>en</u> $s=1$).

RESULTAT 0.4. $\zeta_K(s) = \prod\limits_{\epsilon\in\hat{G}} L(s,\epsilon)$; <u>en isolant</u> $\epsilon = 1$ <u>dans le produit</u>, <u>cela donne</u> $\zeta_K(s) = \zeta_{\mathbb{Q}}(s) \prod\limits_{\substack{\epsilon\in\hat{G}\\ \epsilon\neq 1}} L(s,\epsilon)$.

Pour ϵ dans $\hat{G}$, définissons $\delta(\epsilon)$ par l'égalité $\epsilon^{pr}(-1) = (-1)^{\delta(\epsilon)}$ avec $\delta(\epsilon) = 0$ ou 1 ; on a clairement $\delta(\epsilon) = 0$ ou 1 suivant que le sous-corps de K formé des éléments invariants par le noyau de ϵ est réel ou imaginaire ; nous dirons que ϵ est pair ou réel si $\delta(\epsilon) = 0$ et qu'il est impair ou imaginaire si $\delta(\epsilon) = 1$. Nous posons $\Lambda(s,\epsilon) = f(\epsilon)^{s/2}\,\pi^{-s/2}\,\Gamma(\frac{s+\delta(\epsilon)}{2})\,L(s,\epsilon)$ où Γ est la fonction gamma. En définissant $\tau(\epsilon)$ par $\tau(\epsilon) = \sum\limits_{t=1}^{f(\epsilon)} \epsilon(t)\, e^{\frac{2\pi i}{f(\epsilon)}t}$, on a ([7] par exemple).

RESULTAT 0.5. <u>Si</u> ϵ <u>est un élément de</u> $\hat{G}$ <u>et si</u> $\bar{\epsilon}$ <u>est le conjugué de</u> ϵ, <u>on a l'équation fonctionnelle</u> $\Lambda(1-s,\bar{\epsilon}) = \frac{\tau(\epsilon)}{\sqrt{f(\epsilon)}\, i^{\delta(\epsilon)}}\,\Lambda(s,\epsilon)$.

Tirons quelques conséquences des rappels précédents. On suppose toujours que K est abélien sur $\mathbb{Q}$, alors :

PROPOSITION 0.6. <u>On a</u> $D = \prod_{\epsilon\in\hat{G}} f(\epsilon)$ et $i^{r_2}\sqrt{D} = \prod_{\epsilon\in\hat{G}} \tau(\epsilon)$.

<u>Démonstration</u>. Posons $\Lambda_K(s) = \prod_{\epsilon\in\hat{G}} \Lambda(s,\epsilon)$. Nous traitons séparément le cas où K est réel et celui ou K est complexe. Si K est réel, on a

$$\Lambda_K(s) = \Big(\prod_{\epsilon\in\hat{G}} L(s,\epsilon)\Big)\Big(\prod_{\epsilon\in\hat{G}} f(\epsilon)\Big)^{s/2}\pi^{-r_1 s/2}\Gamma(\tfrac{s}{2})^{r_1} \quad\text{et}\quad \xi_K(s) = \zeta_K(s)(\sqrt{D})^s \pi^{-r_1 s/2}\Gamma(\tfrac{s}{2})^{r_1} ;$$

compte-tenu du résultat 0.4, on tire de ces deux égalités que

$$\Lambda_K(s) = \xi_K(s)\,\frac{\Big(\prod_{\epsilon\in\hat{G}} f(\epsilon)\Big)^{s/2}}{(\sqrt{D})^s}. \text{ On a donc } \Lambda_K(1-s) = \xi_K(1-s)\,\frac{\Big(\prod_{\epsilon\in\hat{G}} f(\epsilon)\Big)^{(1-s)/2}}{(\sqrt{D})^{1-s}} ;$$

du résultat 0.5, on tire $\Lambda_K(1-s) = \Big(\prod_{\epsilon\in\hat{G}} \frac{\tau(\epsilon)}{\sqrt{f(\epsilon)}}\Big)\Lambda_K(s)$ ($\delta(\epsilon) = 0$ pour tout ϵ puisque K est réel) ; on a donc, en tenant compte du résultat 0.2, l'égalité

$$\Big(\prod_{\epsilon\in\hat{G}} \frac{\tau(\epsilon)}{\sqrt{f(\epsilon)}}\Big)\Lambda_K(s) = \xi_K(s)\,\frac{\Big(\prod_{\epsilon\in\hat{G}} f(\epsilon)\Big)^{(1-s)/2}}{(\sqrt{D})^{1-s}}. \text{ On en tire } \Big(\prod_{\epsilon\in\hat{G}} \frac{\tau(\epsilon)}{\sqrt{f(\epsilon)}}\Big) = \frac{\Big(\prod_{\epsilon\in\hat{G}} f(\epsilon)\Big)^{1/2-s}}{(\sqrt{D})^{1-2s}}$$

soit $\dfrac{\Big(\prod_{\epsilon\in\hat{G}} \tau(\epsilon)\Big)}{\Big(\prod_{\epsilon\in\hat{G}} \sqrt{f(\epsilon)}\Big)} = \Big(\dfrac{\prod_{\epsilon\in\hat{G}} f(\epsilon)}{D}\Big)^{1/2-s}$; cette égalité étant vraie pour tout s, on en

déduit $\prod_{\epsilon\in\hat{G}} f(\epsilon) = D$ et $\prod_{\epsilon\in\hat{G}} \tau(\epsilon) = \prod_{\epsilon\in\hat{G}} \sqrt{f(\epsilon)}$, ce qui donne notre résultat dans ce cas.

Supposons maintenant K complexe ; on a alors $\xi_K(s) = \zeta_K(s)(2\pi)^{-r_2 s}(\sqrt{D})^s\Gamma(s)^{r_2}$ et $\Lambda_K(s) = \Big(\prod_{\epsilon\in\hat{G}} L(s,\epsilon)\Big)\Big(\prod_{\epsilon\in\hat{G}} f(\epsilon)\Big)^{s/2}\Big(\pi^{-s/2}\Gamma(\tfrac{s}{2})\,\pi^{-s/2}\Gamma(\tfrac{s+1}{2})\Big)^{r_2}$. Compte tenu du résultat 0.4 et de la formule classique $\Gamma(\frac{s}{2})\Gamma(\frac{s+1}{2}) = \sqrt{2\pi}\;2^{1/2-s}\,\Gamma(s)$ on tire de ces deux égalités que $\Lambda_K(s) = (2\sqrt{\pi})^{r_2}\,\xi_K(s)\,\dfrac{\Big(\prod_{\epsilon\in\hat{G}} f(\epsilon)\Big)^{s/2}}{(\sqrt{D})^s}$; on termine la démonstration comme dans le cas réel en remarquant que $\sum_{\epsilon\in\hat{G}} \delta(\epsilon) = r_2$.

Supposons maintenant que le corps abélien K est complexe ; on a $r_1 = 0$ et $2r_2 = [K:\mathbb{Q}]$; nous posons pour allèger les notations $r_2 = r$. Nous notons K^+ le sous-corps réel maximal de K ; on a $[K:K^+] = 2$ puisque K^+ est le corps des invariants de la conjugaison complexe (qui est bien définie puisque K est abélien).

On désigne alors par D^+ la valeur absolue du discriminant de K^+, par h^+ son nombre de classes et par R^+ son régulateur. On a :

LEMME 0.7. Le quotient h/h^+ est un entier naturel que nous notons h^- et que nous appelons nombre de classes relatif de K.

Démonstration. Soit H (resp. H^+) l'extension abélienne non ramifiée maximale de K (resp. K^+). Par la théorie du corps de classe on sait que h (resp. h^+) est le degré de l'extension H/K (resp. H^+/K^+). L'extension K/K^+ étant totalement ramifiée aux places à l'infini, on a $H^+ \cap K = K^+$ donc le degré de H^+K/K est égal au degré de H^+/K^+ i.e. à h^+. D'autre part H^+K est une extension non ramifiée de K donc H^+K est inclus dans H. En conséquence le degré h^+ de H^+K/K divise le degré h de H/K, ce qui démontre notre lemme.

Notons $\hat{G}^+$ le sous-groupe de $\hat{G}$ formé des caractères pairs et $\hat{G}^-$ le sous-ensemble de $\hat{G}$ formé des caractères impairs. Un caractère est dans $\hat{G}^+$ si et seulement si son noyau contient $\mathrm{Gal}(K^+/K)$ donc $\hat{G}^+$ s'identifie canoniquement au groupe des caractères de $\mathrm{Gal}(K^+/\mathbb{Q})$. On a

PROPOSITION 0.8. Posons $Q = 2^{r-1}\dfrac{R^+}{R}$; on a $h^- = Q\,w \prod_{\epsilon \in \hat{G}^-} \left(\frac{1}{2} L(0,\epsilon)\right)$ (on rappelle que w est le nombre de racines de l'unité contenues dans K).

Démonstration. On a (résultats 0.1 et 0.4) $\mathrm{Res}_{s=1}\zeta_K(s) = \dfrac{(2\pi)^r h\,R}{w\sqrt{D}} = \prod_{\substack{\epsilon\in\hat{G}\\ \epsilon\neq 1}} L(1,\epsilon)$.

De même, le corps K^+ est un corps réel de degré r, donc

$\mathrm{Res}_{s=1}\zeta_{K^+}(s) = \dfrac{2^r h^+ R^+}{2\sqrt{D^+}} = \prod_{\substack{\epsilon\in\hat{G}^+\\ \epsilon\neq 1}} L(1,\epsilon)$. De ces deux égalités on déduit

$\prod_{\epsilon\in\hat{G}^-} L(1,\epsilon) = \dfrac{2\pi^r}{w}\,\dfrac{h}{h^+}\,\dfrac{R}{R^+}\sqrt{\dfrac{D^+}{D}}$. D'autre part, le résultat 0.5 donne, pour tout ϵ de $\hat{G}^-$, l'égalité $\Gamma(\frac{1}{2})L(0,\bar{\epsilon}) = \dfrac{\tau(\epsilon)}{\sqrt{f(\epsilon)}\,i}\, f(\epsilon)^{1/2}\,\pi^{-1/2}\,\Gamma(1)\,L(1,\epsilon)$ soit

$\sqrt{\pi}\,L(0,\bar{\epsilon}) = \dfrac{\tau(\epsilon)}{i\sqrt{\pi}}\,L(1,\epsilon)$. Lorsque ϵ décrit $\hat{G}^-$, $\bar{\epsilon}$ décrit aussi $\hat{G}^-$, donc

$\prod_{\epsilon\in\hat{G}^-} L(1,\epsilon) = (\pi i)^r \prod_{\epsilon\in\hat{G}^-} \frac{L(0,\epsilon)}{\tau(\epsilon)}$ et donc $h^- = \frac{h}{h^+} = \frac{w}{2}\,\frac{R^+}{R}\sqrt{\frac{D}{D^+}}\, i^r \prod_{\epsilon\in\hat{G}^-}\frac{L(0,\epsilon)}{\tau(\epsilon)} =$
$Q\,w\left(\prod_{\epsilon\in\hat{G}^-} \frac{1}{2}L(0,\epsilon)\right)\sqrt{\frac{D}{D^+}}\ \frac{i^r}{\prod_{\epsilon\in\hat{G}^-}\tau(\epsilon)}$. On conclut en remarquant que
$\prod_{\epsilon\in\hat{G}^-}\tau(\epsilon) = \frac{\prod_{\epsilon\in\hat{G}}\tau(\epsilon)}{\prod_{\epsilon\in\hat{G}^+}\tau(\epsilon)}$ est, d'après la proposition 0.6, égal à $\frac{i^r\sqrt{D}}{\sqrt{D^+}}$.

Notons E le groupe des unités de K et $\mu(K)$ le sous-groupe de torsion de E. De même notons E^+ le groupe des unités de K^+ ; le sous-groupe de torsion de E^+ est ± 1 et le quotient $E^+/\{\pm 1\}$ s'injecte canoniquement dans $E/\mu(K)$. Ces deux quotients étant des groupes libres de rang $r-1$, l'indice $[E/\mu(K) : E^+/\{\pm 1\}]$ qui est le cardinal $[E/(E^+\mu(K))]$ est fini ; on a :

PROPOSITION 0.9. La constante Q de la proposition précédente est égale à $[E/(E^+\mu(K))]$.

Démonstration. Par le théorème des diviseurs élémentaires, on sait qu'il existe une famille $e_1,\dots,e_{r-1}$ d'unités de K et une famille $x_1,\dots,x_{r-1}$ d'entiers positifs telles que les classes modulo $\mu(K)$ de $e_1,\dots,e_{r-1}$ forment une base de $E/\mu(K)$ et que les classes de $e_1^{x_1},\dots,e_{r-1}^{x_{r-1}}$ forment une base du sous-groupe $E^+/\{\pm 1\}$ de $E/\mu(K)$. Notons $\sigma_1,\dots,\sigma_r$ les r éléments de $\mathrm{Gal}(K^+/\mathbb{Q})$; par définition on a

$$R^+ = r^{-1}\begin{vmatrix} 1 & \log|\sigma_1(e_1^{x_1})| & \dots & \log|\sigma_1(e_{r-1}^{x_{r-1}})| \\ \vdots & & & \\ 1 & \log|\sigma_r(e_1^{x_1})| & \dots & \log|\sigma_r(e_{r-1}^{x_{r-1}})| \end{vmatrix}$$

où $|\sigma_i(e_j^{x_j})|$ désigne la valeur absolue ordinaire du réel $\sigma_i(e_j^{x_j})$. Pour $i = 1,\dots,r$ choisissons un prolongement de σ_i que nous notons encore σ_i. On a :

$$R = r^{-1}\begin{vmatrix} 1 & \log|\sigma_1(e_1)|^2 & \dots & \log|\sigma_1(e_{r-1})|^2 \\ \vdots & & & \\ 1 & \log|\sigma_r(e_1)|^2 & \dots & \log|\sigma_r(e_{r-1})|^2 \end{vmatrix}$$

où $|\sigma_i(e_j)|$ désigne la valeur absolue ordinaire du complexe $|\sigma_i(e_j)|$. De ces deux égalités, on tire $x_1 \dots x_{r-1} R = 2^{r-1} R^+$ soit $x_1 \dots x_r = 2^{r-1} \frac{R^+}{R}$. Mais le produit $x_1 \dots x_{r-1}$ est l'indice de $E^+/\{\pm 1\}$ dans $E/\mu(K)$, donc l'égalité précédente prouve notre assertion.

On a aussi le résultat suivant :

PROPOSITION 0.10. <u>La constante</u> Q <u>est égale à</u> 1 <u>ou</u> 2.

<u>Démonstration.</u> Pour tout e de E, le quotient $\frac{e}{\bar{e}}$ où $\bar{e}$ est le conjugué de e est une racine de l'unité : en effet $\frac{e}{\bar{e}}$ est un entier de K et, pour toute place infinie v de K, on a $|e|_v = |\bar{e}|_v$ en désignant par $|\ |_v$ la valeur absolue de K associée à v ; on a donc $|\frac{e}{\bar{e}}|_v = 1$ pour toutes les places à l'infini v et on conclut à l'aide du lemme suivant :

LEMME 0.11. <u>Soit</u> α <u>un entier de</u> K <u>tel que</u> $|\alpha|_v = 1$ <u>pour toute place à l'infini</u> v <u>de</u> K, <u>alors</u> α <u>est une racine de l'unité</u>.

<u>Démonstration</u>. Choisissons une place à l'infini v_o ; si α^1 est un conjugué de α, on a $|\alpha^1|_{v_o} = 1$ puisque $|\alpha^1|_{v_o} = |\alpha|_v$ pour une place à l'infini v. Le polynôme minimal de α est un polynôme de $\mathbb{Z}[X]$ dont le degré est majoré par le degré du corps K. De plus, l'expression de ces coefficients en fonction des conjugués de α montre que leur valeur absolue (pour $|\ |_{v_o}$) est majorée indépendamment de α ; ces coefficients étant dans $\mathbb{Z}$ ils ne peuvent prendre qu'un nombre fini de valeurs ; en conséquence l'ensemble des entiers α de K tels que $|\alpha|_v = 1$ pour toute place à l'infini v est fini ; cet ensemble étant stable par multiplication, on en déduit qu'il existe un entier n tel que $\alpha^n = 1$. C.Q.F.D.

Revenons à la démonstration de la proposition 0.10. Considérons l'application θ de E dans $\mu(K)$ définie par $\theta(e) = \frac{e}{\bar{e}}$ pour e dans E ; c'est clairement un homomorphisme de groupe ; de plus $\theta(e) = 1$ si e est dans E^+ et $\theta(e) = e^2$ si e est dans $\mu(K)$. En conséquence θ définit par passage au quotient un homomorphisme de $E/(E^+\mu(K))$ vers $\mu(K)/\mu(K)^2$ que l'on note encore θ. Ce dernier groupe étant le groupe à deux éléments (puisque $\mu(K)$ est cyclique d'ordre pair), on achèvera la démonstration en démontrant que θ est injectif. Montrons l'injectivité de θ : soit $e \in E$ tel que $\frac{e}{\bar{e}} = \zeta^2$ avec ζ dans $\mu(K)$; on a $\frac{e}{\bar{e}} = \frac{\zeta}{\bar{\zeta}}$ donc $\bar{e}\zeta = e\bar{\zeta}$ ce qui montre que $e\bar{\zeta} = \overline{e\bar{\zeta}}$ i.e. que $e\bar{\zeta}$ est dans E^+ ; en conséquence la classe de e dans le quotient $E/(E^+\mu(K))$ est la classe neutre et donc θ est injectif.

Dans la suite nous serons particulièrement intéressés par le cas des corps cyclotomiques ; on a pour ces corps la proposition suivante :

PROPOSITION 0.12. <u>Soit</u> K <u>un corps cyclotomique et soit</u> N <u>le plus petit entier tel que</u> K <u>est engendré sur</u> $\mathbb{Q}$ <u>par une racine de l'unité d'ordre</u> N ; <u>si</u> $N \geq 3$ <u>on a</u> $Q = 1$ <u>si</u> N <u>est la puissance d'un nombre premier et</u> $Q = 2$ <u>sinon</u>.

<u>Démonstration</u> (Iwasawa). On reprend les notations de la proposition précédente ; on a $Q = 1$ ou 2 suivant que θ n'est pas surjective ou est surjective. Supposons que $N = p^n$ pour un nombre premier p et notons ζ une racine de l'unité d'ordre N ; si p est impair, $-\zeta$ engendre le groupe μ_{2N} qui est $\mu(K)$ donc $-\zeta$ n'est pas dans $\mu(K)^2$; si $p=2$, $-\zeta$ engendre le groupe μ_N qui est encore $\mu(K)$ donc $-\zeta$ n'est toujours pas dans $\mu(K)^2$. Supposons que la classe de $-\zeta$ dans $\mu(K)/\mu(K)^2$ est atteinte par θ ; il existerait alors un e dans E tel que $\frac{e}{\bar{e}} = -\zeta$; de $\frac{1-\zeta}{1-\bar{\zeta}} = -\zeta$ on tire alors que $\frac{e}{1-\zeta} = \frac{\bar{e}}{1-\bar{\zeta}}$ c'est-à-dire que $\frac{e}{1-\zeta}$ est dans K^+. D'autre part, p est totalement ramifié dans $K/\mathbb{Q}$; notons ord_p la valuation de K associée à l'unique idéal premier contenant p et normalisée par $\mathrm{ord}_p(p) = 1$. On a $\mathrm{ord}_p(\frac{e}{1-\zeta}) = -\mathrm{ord}_p(1-\zeta) = -\frac{1}{\varphi(p^n)}$ où φ est l'indicateur d'Euler ; cela contredit le fait que $\frac{e}{1-\zeta}$ est dans K^+ puisque, pour tout x de K^+, $\mathrm{ord}_p(x)$ est le quotient d'un nombre pair par $\varphi(p^n)$ et donc on a démontré que θ n'est pas surjectif.

Supposons que N n'est pas la puissance d'un nombre premier ; on désigne encore par ζ une racine de l'unité d'ordre N. Si N est impair, on a $\mu(K)=\mu_N \times \{\pm 1\}$ et le quotient $\mu(K)/\mu(K)^2$ est engendré par $-\zeta$. Mais $1-\zeta$ est dans E, donc l'égalité $\frac{1-\zeta}{\overline{1-\zeta}} = -\zeta$ montre que θ est surjective. Si N est pair il est divisible par 4 (sinon K serait obtenu en adjoignant à $\mathbb{Q}$ une racine de l'unité d'ordre $\frac{N}{2}$ ce qui contredirait la minimalité de N). Puisque N est pair, ζ n'est pas dans $\mu(K)^2$; puisque 4 divise N, -1 est dans $\mu(K)^2$; en conséquence $-\zeta$ n'est pas dans $\mu(K)^2$ et on achève la démonstration comme ci-dessus.

§1. LES CLASSES RELATIVES DES CORPS CYCLOTOMIQUES.

Soient p un nombre premier et m un entier positif tel que $(m,p)=1$. Pour tout entier $n \geqslant 0$ on pose $q_n = mp^{n+1}$ si $p \neq 2$ et $q_n = m2^{n+2}$ si $p=2$. On note μ_{q_n} le groupe des racines q_n-ièmes de l'unité, K_n le corps $\mathbb{Q}(\mu_{q_n})$, h_n^- le nombre de classes relatif de K_n et e_n^- le plus grand entier tel que $p^{e_n^-}$ divise h_n^-. On va montrer qu'il existe trois entiers μ^-, λ^- et ν^- avec $\mu^- \geqslant 0$ et $\lambda^- \geqslant 0$ tels que, pour n assez grand, $e_n^- = \mu^- p^n + \lambda^- n + \nu^-$ (Ferrero et Washington ont démontré que $\mu^- = 0$ ce qui avait été conjecturé par Iwasawa, mais nous ne parlerons pas de ce résultat ici). Signalons qu'il existe une démonstration algébrique de cette formule (on note e_n et e_n^+ les plus grands entiers tels que p^{e_n} et $p^{e_n^+}$ divisent respectivement le nombre de classes de K_n et le nombre de classes du sous-corps réel maximal K_n^+ de K_n, on montre algébriquement qu'il existe des entiers μ, λ, ν, μ^+, λ^+, ν^+ tels que $e_n = \mu p^n + \lambda n + \nu$ et $e_n^+ = \mu^+ p^n + \lambda^+ n + \nu^+$ pour n assez grand ; on en déduit par soustraction $e_n^- = \mu^- p^n + \lambda^- n + \nu^-$ avec $\mu^- = \mu - \mu^+$, $\lambda^- = \lambda - \lambda^+$ et $\nu^- = \nu - \nu^+$; Ferrero et Washington ont démontré que $\mu = 0$, il en résulte que μ^+ et μ^- sont nuls). Nous allons donner ici une démonstration reposant sur les techniques développées dans la partie I de ce cours.

Nous supposerons dans ce paragraphe que p est impair ; le cas $p=2$ se traite de manière analogue. Posons $G_n = \mathrm{Gal}(K_n/\mathbb{Q})$; on identifie le groupe G_n au groupe $(\mathbb{Z}/q_n\mathbb{Z})^*$ en associant à $\sigma \in G_n$ l'élément $x \in (\mathbb{Z}/q_n\mathbb{Z})^*$ tel que $\sigma(\zeta) = \zeta^x$ pour tout ζ de μ_{q_n}. Le groupe $\hat{G}_n$ des caractères de G_n s'identifie donc au groupe des caractères modulo q_n ; si ε est un élément de $\hat{G}_n$, on note (comme au §0) ε^{pr} le caractère primitif équivalent au caractère modulo q_n associé à ε. Le groupe $(\mathbb{Z}/q_n\mathbb{Z})^*$ est canoniquement isomorphe à $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^* \times [(1+p\mathbb{Z})/(1+p^{n+1}\mathbb{Z})]$; on note Δ et R_n les sous-groupes de G_n qui s'identifient respectivement à $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$ et à $(1+p\mathbb{Z})/(1+p^{n+1}\mathbb{Z})$; on a donc $G_n = \Delta \times R_n$ et $\hat{G}_n = \hat{\Delta} \times \hat{R}_n$ si $\hat{\Delta}$ et $\hat{R}_n$ sont les sous-groupes de $\hat{G}_n$ formés des caractères dont les noyaux contiennent respectivement R_n et Δ. Comme au §6 de la partie I de ce cours, on choisit une fois pour toute un plongement de la clôture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$ inclus dans $\mathbb{C}$ dans la clôture algébrique $\bar{\mathbb{Q}}_p$ de $\mathbb{Q}_p$; on reprend le vocabulaire et les conventions introduites dans ce §6 de la partie I. En particulier ω est le caractère modulo p dont la valeur en un x de $\mathbb{Z}$ premier à p est la racine $p-1$<u>ième</u> de l'unité congrue à x modulo $p\mathbb{Z}_p$; on note ω_n l'élément de $\hat{G}_n$ qui s'identifie au caractère modulo q_n équivalent à ω ; le caractère ω_n est dans $\hat{\Delta}$. Enfin on note ord_p la valuation de $\bar{\mathbb{Q}}_p$ normalisée par $\mathrm{ord}_p(p) = 1$; on a donc $e_n^- = \mathrm{ord}_p(h_n^-)$.

LEMME 1.1. <u>On a</u> $e_n^- = n+1+\mathrm{ord}_p\left(\prod_{\left\{\substack{\theta\in\hat{R}_n \\ \varepsilon\in\hat{\Delta}^-}\right.} L(0,\varepsilon\theta)\right)$.

<u>Démonstration</u>. On a vu (proposition 0.8) que $h_n^- = Q\,w \prod_{\varepsilon\in\hat{G}_n^-}(\frac{1}{2}\,L(0,\varepsilon))$ et que (proposition 0.10) $Q=1$ ou 2. Puisque $p \neq 2$, on en tire $e_n^- = \mathrm{ord}_p(h_n^-) = \mathrm{ord}_p(w) + \mathrm{ord}_p(\prod_{\varepsilon\in\hat{G}_n^-} L(0,\varepsilon))$; on conclut en remarquant que $\mathrm{ord}_p(w) = n+1$ et que le groupe $\hat{G}_n^-$ est le produit direct

$\hat{\Delta}^- \times \hat{R}_n$.

Montrons la proposition suivante :

PROPOSITION 1.2. <u>On a</u> $\mathrm{ord}_p(\prod_{\theta\in\hat{R}_n} L(0,\omega_n^{-1}\theta)) = -(n+1)$.

<u>Démonstration</u>. Par définition (voir §0) on a, pour tout θ de $\hat{R}_n$, l'égalité $L(0,\omega_n^{-1}\theta) = L(0,(\omega_n^{-1}\theta)^{pr})$. Le conducteur de $\omega_n^{-1}\theta$ est une puissance de p mais n'est pas 1 puisque $\omega_n^{-1}\theta$ est distinct du caractère unité quel que soit θ dans $\hat{R}_n$. Le produit $\omega^{-1}\theta^{pr}$ de $\omega^{-1} = (\omega_n^{pr})^{-1}$ qui est un caractère modulo p par θ^{pr} qui est un caractère modulo une puissance de p est un caractère modulo une puissance de p équivalent à $(\omega_n^{-1}\theta)^{pr}$; on a donc $L(0,\omega^{-1}\theta^{pr}) = L(0,(\omega_n^{-1}\theta)^{pr})$. On sait (I, §6, définition 6.4) que $L(0,\omega^{-1}\theta^{pr}) = L_p(0,\theta^{pr})$ et que $L_p(0,\theta^{pr}) = \dfrac{L_p(0,\theta^{pr},C)}{1-\theta^{pr}(C)\langle C\rangle}$ si C est un élément de $\hat{\mathbb{Z}}^*$ tel que $\theta^{pr}(C)\langle C\rangle \neq 1$. Rappelons (I, §6, définition 6.1 et I, §5, théorème 5.7) que $L_p(s,\theta^{pr},C)$ est une fonction d'Iwasawa ; cela signifie que, si R est l'anneau des entiers d'une extension finie de $\mathbb{Q}_p$ qui contient les valeurs de θ^{pr} et si γ est un générateur du $\mathbb{Z}_p$-module $1+2p\,\mathbb{Z}_p$, alors il existe une série $f(T,\theta^{pr},C) \in R[[T]]$ telle que $f(\gamma^{-s}-1,\theta^{pr},C) = L_p(s,\theta^{pr},C)$ pour tout s de $\mathbb{Z}_p$. Le caractère θ^{pr} étant (avec le vocabulaire de I, §7, définition 7.1) un caractère modulo une puissance de p de seconde espèce, on a (I, §7, proposition 7.11) l'égalité $f(T,\theta^{pr},C) = f(\theta^{pr}|_p(\gamma)(1+T)-1,1,C)$ où le caractère 1 désigne le caractère unité modulo 1 (i.e. celui qui vaut 1 pour tout x de $\mathbb{Z}$). On a donc $L_p(0,\theta^{pr}) = \dfrac{f(\theta^{pr}|_p(\gamma)-1,1,C)}{1-\theta^{pr}(C)\langle C\rangle}$; choisissons $C \in \hat{\mathbb{Z}}^*$ tel que $C_p = 1+p$; on a alors $\langle C\rangle = 1+p$ et $\theta^{pr}(C)$ est une racine de l'unité qui engendre l'image de θ^{pr} . En conséquence, lorsque θ décrit $\hat{R}_n$, les $\theta^{pr}(C)$ décrivent le groupe μ_{p^n} des racines p^n <u>ièmes</u> de l'unité. De même lorsque θ décrit $\hat{R}_n$, les $\theta^{pr}|_p(\gamma)$

décrivent aussi le groupe μ_{p^n} . On a donc l'égalité

$\prod_{\theta\in\hat{R}_n} L_p(0,\theta^{pr}) = \prod_{\zeta\in\mu_{p^n}} \frac{f(\zeta-1,1,C)}{1-\zeta(1+p)}$, c'est-à-dire compte-tenu de ce qu'on a fait au début de la démonstration

$\prod_{\theta\in\hat{R}_n} L(0,\omega_n^{-1}\theta) = \prod_{\zeta\in\mu_{p^n}} \frac{f(\zeta-1,1,C)}{1-\zeta-p\zeta}$. D'autre part, si ζ est une racine de l'unité d'ordre p^r on a $\operatorname{ord}_p(1-\zeta-p\zeta)^{-1} = -\frac{1}{\varphi(p^r)}$. Montrons que, pour tout ζ de μ_{p^n} on a $\operatorname{ord}_p(f(\zeta-1,1,C)) = 0$: on a $f(\zeta-1,1,C) \equiv f(0,\zeta-1,C)$ modulo $(\zeta-1)R$ puisque $f(T,1,C)\in R[[T]]$; comme $\operatorname{ord}_p(\zeta-1) > 0$, il suffit pour montrer notre assertion de montrer que $\operatorname{ord}_p(f(0,1,C)) = 0$; mais $f(0,1,C) = (1-\langle C\rangle)L_p(0,1) = -p\,L(0,\omega^{-1}) = p\sum_{t=1}^{p-1}\omega^{-1}(t)B_1(\frac{t}{p}) = \sum_{t=1}^{p-1}\omega^{-1}(t)t$ puisque $B_1(X) = X-\frac{1}{2}$ et que $\sum_{t=1}^{p-1}\omega^{-1}(t) = 0$; enfin, par définition de ω , on a $\omega(t)\equiv t$ modulo $p\mathbb{Z}_p$, donc $\omega^{-1}(t)t \equiv 1$ modulo $p\mathbb{Z}_p$, donc $f(0,1,C) \equiv p-1$ modulo $p\mathbb{Z}_p$ ce qui montre que $\operatorname{ord}_p(f(0,1,C)) = 0$. On a donc

$\operatorname{ord}_p(\prod_{\theta\in\hat{R}_n} L(0,\omega_n^{-1}\theta)) = \sum_{r=0}^{n}(\sum_{\zeta\in\mu^*_{p^r}} -\frac{1}{\varphi(p^r)})$ si $\mu^*_{p^r}$ désigne l'ensemble des racines de l'unité d'ordre p^r ; le cardinal de $\mu^*_{p^r}$ étant $\varphi(p^r)$ on a $\operatorname{ord}_p(\prod_{\theta\in\hat{R}_n} L(0,\omega_n^{-1}\theta)) = -(n+1)$, C.Q.F.D.

COROLLAIRE 1.3. <u>On a</u> $e_n^- = \operatorname{ord}_p\left(\prod_{\begin{cases}\theta\in\hat{R}_n\\ \varepsilon\in\hat{\Delta}^-\setminus\{\omega_n^{-1}\}\end{cases}} L(0,\varepsilon\theta)\right)$.

<u>Démonstration</u>. Claire en juxtaposant le lemme 1.1 et la proposition 1.2.

PROPOSITION 1.4. <u>On a</u> $e_n^- = e_0^- + \operatorname{ord}_p\left(\prod_{\begin{cases}\theta\in\hat{R}_n\setminus\{1\}\\ \varepsilon\in\hat{\Delta}^+\setminus\{1\}\end{cases}} L_p(0,\varepsilon^{pr}\theta^{pr})\right)$.

Démonstration. Le corollaire 1.3 appliqué avec $n=0$ montre que $\mathrm{ord}_p\left(\prod_{\varepsilon\in\hat{\Delta}^-\setminus\{\omega_n^{-1}\}} L(0,\varepsilon)\right) = e_o^-$. On tire donc du corollaire 1.3 que

$$e_n^- = e_o^- + \mathrm{ord}_p\left(\prod_{\substack{\theta\in\hat{R}_n\setminus\{1\}\\ \varepsilon\in\hat{\Delta}^-\setminus\{\omega_n^{-1}\}}} L(0,\varepsilon\theta)\right).$$

Pour tout $\theta\in\hat{R}_n\setminus\{1\}$ et tout $\varepsilon\in\hat{\Delta}^-$, le conducteur de $\varepsilon\theta$ est divisible par p ; il en résulte que les deux caractères $(\varepsilon\theta)^{pr}$ et $(\varepsilon\omega_n)^{pr}\theta^{pr}(\omega_n^{-1})^{pr}$ sont définis modulo le même entier, donc sont égaux ; les fonctions L qui leur sont associées sont les mêmes ; en particulier on a
$L(0,(\varepsilon\theta)^{pr}) = L(0,(\varepsilon\omega_n)^{pr}\theta^{pr}(\omega_n^{-1})^{pr})$; mais, par définition,
$L(0,(\varepsilon\theta)^{pr}) = L(0,\varepsilon\theta)$ et $(\omega_n^{-1})^{pr} = \omega^{-1}$; on a donc
$L(0,\varepsilon\theta) = L(0,(\varepsilon\omega_n)^{pr}\theta^{pr}\omega^{-1})$; enfin (I, §6, définition 6.4) on a
$L(0,(\varepsilon\omega_n)^{pr}\theta^{pr}\omega^{-1}) = L_p(0,(\varepsilon\omega_n)^{pr}\theta^{pr})$ et la proposition résulte de ce que $\varepsilon\omega_n$ décrit $\hat{\Delta}^+\setminus\{1\}$ lorsque ε décrit $\hat{\Delta}^-\setminus\{\omega_n^{-1}\}$.

Nous sommes maintenant en mesure de démontrer la formule annoncée au début de ce paragraphe :

THEOREME 1.5. <u>Il existe trois entiers positifs ou nuls</u> μ^-, λ^- <u>et</u> ν^- <u>tels que</u> $e_n^- = \mu^- p^n + \lambda^- n + \nu^-$.

Démonstration. Désignons par R l'anneau des entiers d'une extension finie de $\mathbb{Q}_p$ contenant les racines de l'unité d'ordre $\varphi(mp)p^n$, de sorte que R contient l'image de tous les caractères de $\hat{G}_n$. Pour tout $\varepsilon\in\hat{\Delta}^+\setminus\{1\}$ et $\theta\in\hat{R}_n$, on vérifie que $\varepsilon^{pr}\theta^{pr}$ n'est pas de seconde espèce (I, §7, définition 7.1) ; en conséquence (I, §7, théorème 7.2) la fonction $L_p(s,\varepsilon^{pr}\theta^{pr})$ est une fonction d'Iwasawa ; comme en I, §7 notons $g(T,\varepsilon^{pr}\theta^{pr})$ la série de $R[[T]]$ telle que $L_p(s,\varepsilon^{pr}\theta^{pr}) = g(\gamma^{-s}-1,\varepsilon^{pr}\theta^{pr})$ où γ est un générateur du $\mathbb{Z}_p$-module $1+2p\mathbb{Z}_p$. Les caractères θ^{pr} étant, pour tout $\theta\in\hat{R}_n$, des caractères modulo une puissance de p et de seconde espèce, on tire de la proposition 7.11 du §7 de la partie I que $g(T,\varepsilon^{pr}\theta^{pr}) = g(\theta^{pr}|_p(\gamma)(1+T)-1,\varepsilon^{pr})$. Lorsque θ décrit $\hat{R}_n\setminus\{1\}$, les $\theta^{pr}|_p(\gamma)$ décrivent $\mu_{p^n}\setminus\{1\}$, donc

$$\prod_{\substack{\theta\in\hat{R}_n\setminus\{1\}\\ \varepsilon\in\hat{\Delta}^+\setminus\{1\}}} L_p(0,\varepsilon^{pr}\theta^{pr}) = \prod_{\zeta\in\mu_{p^n}\setminus\{1\}}\ \prod_{\varepsilon\in\hat{\Delta}^+\setminus\{1\}} g(\zeta-1,\varepsilon^{pr}) .$$

Posons alors $g(T) = \prod_{\varepsilon\in\hat{\Delta}^+\setminus\{1\}} g(T,\varepsilon^{pr})$; nous aurons besoin du lemme suivant :

LEMME 1.6. <u>La série</u> $g(T)$ <u>est dans</u> $\mathbb{Z}_p[[T]]$.

Avant de démontrer ce lemme, voyons comment il permet de conclure la démonstration du théorème. Désignons par μ^- le plus grand entier tel que p^{μ^-} divise tous les coefficients de $g(T)$ et par λ^- le plus petit entier tel que p^{μ^-+1} ne divise pas le coefficient de T^{λ^-} dans $g(T)$; le théorème de préparation de Weierstrass p-adique ([13],[8]) montre que $g(T)=p^{\mu^-}(T^{\lambda^-}+b_{\lambda^--1}T^{\lambda^--1}+\dots+b_o)u(T)$ où les b_i pour $i=0,\dots,\lambda-1$ sont dans $p\mathbb{Z}_p$ et où $u(T)$ est dans $(\mathbb{Z}_p[[T]])^*$. En conséquence, si ζ est une racine de l'unité d'ordre p^r, on a $\mathrm{ord}_p(g(\zeta-1))=\mu^-+\mathrm{ord}_p[(\zeta-1)^{\lambda^-}+b_{\lambda^--1}(\zeta-1)^{\lambda^--1}+\dots+b_o]$; compte-tenu de $\mathrm{ord}_p(\zeta-1) = \dfrac{1}{\varphi(p^r)}$ et de $\mathrm{ord}_p(b_i)\geqslant 1$ pour $i=0,\dots,\lambda^--1$, on déduit de l'égalité précédente que $\mathrm{ord}_p(g(\zeta-1)) = \mu^-+\dfrac{\lambda^-}{\varphi(p^r)}$ dès que $\varphi(p^r)>\lambda^-$. Pour tout r notons de nouveau μ_r^* l'ensemble des racines de l'unité d'ordre p^r; supposons n assez grand pour que $\varphi(p^n)>\lambda^-$ et notons r_o le plus grand entier tel que $\varphi(p^{r_o})\leqslant\lambda^-$. On a alors

$$\mathrm{ord}_p\left[\prod_{\zeta\in\mu_{p^n}\setminus\{1\}}\left(\prod_{\varepsilon\in\hat{\Delta}^+\setminus\{1\}} g(\zeta-1,\varepsilon^{pr})\right)\right] = \sum_{\zeta\in\mu_{p^n}\setminus\{1\}} \mathrm{ord}_p(g(\zeta-1)) =$$

$\mu^-(p^n-1)+(n-r_o)\lambda^-+X$ où

$X = \sum_{r=1}^{r_o}\left(\sum_{\zeta\in\mu_r^*}\mathrm{ord}_p[(\zeta-1)^{\lambda^-}+b_{\lambda^--1}(\zeta-1)^{\lambda^--1}+\dots+b_o]\right)$. En juxtaposant ce qui vient d'être dit et la proposition 1.4, on obtient $e_n^- = \mu^- p^n + \lambda^- n + X - r_o \lambda^- + e_o^-$ soit $e_n^- = \mu^- p^n + \lambda^- n + \nu^-$ qui est la formule cherchée. Il ne reste plus qu'à démontrer le lemme :

<u>Démonstration du lemme</u> 1.6. Montrons d'abord que, pour tout s de $\mathbb{Z}_p$, on a $g(\gamma^{-s}-1) \in \mathbb{Z}_p$ si γ est le générateur de $1+2p\mathbb{Z}_p$ choisi ci-dessus. Les $1-k$ pour k entier, $k \geqslant 1$ et k divisible par $p-1$ étant denses dans $\mathbb{Z}_p$, il suffit de montrer que $g(\gamma^{k-1}-1) \in \mathbb{Z}_p$ pour tous ces k. Pour un tel k, on a $g(\gamma^{k-1}-1) = \prod_{\varepsilon \in \Delta^+ \setminus \{1\}} g(\gamma^{k-1}-1, \varepsilon^{pr}) = \prod_{\varepsilon \in \Delta^+ \setminus \{1\}} L_p(1-k, \varepsilon^{pr}) = \prod_{\varepsilon \in \Delta^+ \setminus \{1\}} (1 - \frac{\varepsilon^{pr}(p)}{p^{1-k}}) L(1-k, \varepsilon)$ puisque $p-1 | k$ implique $(1 - \frac{\varepsilon^{pr}(p)}{p^{1-k}}) L(1-k, \varepsilon) = L(1-k, \varepsilon^{pr} \omega^{-k})$. Le groupe Δ s'identifie au groupe de Galois $Gal(K_o/\mathbb{Q})$ et $\hat{\Delta}$ s'identifie au groupe des caractères de $Gal(K_o/\mathbb{Q})$; le groupe $\hat{\Delta}^+$ s'identifie au groupe des caractères de $Gal(K_o^+/\mathbb{Q})$ si K_o^+ désigne le sous-corps réel maximal de K_o. On a donc (§0, résultat 0.4) $\prod_{\varepsilon \in \Delta^+} L(1-k, \varepsilon) = \zeta_{K_o^+}(1-k)$ et donc $\prod_{\varepsilon \in \Delta^+ \setminus \{1\}} L(1-k, \varepsilon) = \frac{\zeta_{K_o^+}(1-k)}{\zeta_{\mathbb{Q}}(1-k)}$; les fonctions ζ étant les fonctions L associées au caractère unité modulo 1, leurs valeurs aux entiers négatifs sont dans $\mathbb{Q}$, donc $\prod_{\varepsilon \in \Delta^+ \setminus \{1\}} L(1-k, \varepsilon)$ est dans $\mathbb{Q}$. Enfin, rappelons que $K_o = \mathbb{Q}(\mu_{mp})$ avec $(m,p) = 1$; les caractères ε de $\hat{\Delta}$ dont le conducteur n'est pas divisible par p i.e. ceux tels que $\varepsilon^{pr}(p) \neq 0$ sont donc ceux dont le noyau contient $Gal(K_o/\mathbb{Q}(\mu_p))$; ces caractères s'identifient donc avec les caractères de $Gal(\mathbb{Q}(\mu_m)/\mathbb{Q})$. Les caractères ε de $\hat{\Delta}^+$ tels que $\varepsilon^{pr}(p) \neq 0$ correspondent donc aux caractères de $Gal(\mathbb{Q}(\mu_m)^+/\mathbb{Q})$ si $\mathbb{Q}(\mu_m)^+$ est le sous-corps réel maximal de $\mathbb{Q}(\mu_m)$. De cela résulte que, pour un $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, l'ensemble des $\sigma(\varepsilon^{pr}(p))$ coïncide avec l'ensemble des $\varepsilon^{pr}(p)$ lorsque ε décrit $\hat{\Delta}^+ \setminus \{1\}$; le produit $\prod_{\varepsilon \in \hat{\Delta}^+ \setminus \{1\}} \left(1 - \frac{\varepsilon^{pr}(p)}{p^{1-k}}\right)$ est donc dans $\mathbb{Q}$. On a donc montré que, pour tout $k \geqslant 1$ tel que $p-1$ divise k, $g(\gamma^{k-1}-1)$ est dans $\mathbb{Q}$;

comme il est aussi dans R , il est dans $\mathbb{Z}_p$. Pour terminer la démonstration notons, pour tout $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$, par $g^{\tau}(T)$ la série formelle dont les coefficients sont les images par τ des coefficients de $g(T)$. On a clairement $g^{\tau}(\gamma^{-s}-1) = \tau(g(\gamma^{-s}-1))$ pour tout s de $\mathbb{Z}_p$; mais $\tau(g(\gamma^{-s}-1)) = g(\gamma^{-s}-1)$ puisque $g(\gamma^{-s}-1) \in \mathbb{Z}_p$, donc on a $g^{\tau}(\gamma^{-s}-1) = g(\gamma^{-s}-1)$ pour tout s de $\mathbb{Z}_p$ et donc (I, §2, remarque 5.3) $g^{\tau}(T) = g(T)$. Cette dernière égalité montre que $g(T) \in \mathbb{Q}_p[[T]]$; comme $g(T) \in R[[T]]$, il en résulte que $g(T) \in \mathbb{Z}_p[[T]]$. C.Q.F.D.

REMARQUE 1.7. Supposons dans les données de ce chapitre que $m=1$; le groupe $\hat{\Delta}$ est alors formé des puissances de ω_n ; l'ensemble $\hat{\Delta}^-$ est alors l'ensemble des ω_n^{k-1} pour $k=2,4,\ldots,p-1$. Pour $k=2,4,\ldots,p-3$ le conducteur de ω_n^k est p , donc $L_p(0,(\omega_n^k)^{pr}) = L(0,\omega_n^{k-1})$. On a donc, dans ce cas,
$\prod_{\varepsilon\in\hat{\Delta}^-\setminus\{\omega_n^{-1}\}} L(0,\varepsilon) = \prod_{\varepsilon\in\hat{\Delta}^+\setminus\{1\}} L_p(0,\varepsilon^{pr})$. En incorporant cela dans ce qui a été fait dans les démonstrations de la proposition 1.4 et du théorème 1.5, on obtient $e_n^- = \mathrm{ord}_p\left(\prod_{\zeta\in\mu_{p^n}} g(\zeta-1)\right)$ avec $g(T) = \prod_{k=2,4,\ldots,p-3} g(T,\omega^k)$.
Faisons $n=0$; on obtient l'équivalence $e_0^-=0$ si et seulement si $g(0)$ est premier à p . Mais $g(0)$ premier à p est équivalent à $g(\zeta-1)$ premier à p pour tout $\zeta\in\mu_{p^n}$ donc à
$e_n^- = \mathrm{ord}_p\left(\prod_{\zeta\in\mu_{p^n}} g(\zeta-1)\right) = 0$.

D'autre part $g(0) = \prod_{k=2,4,\ldots p-3} g(0,\omega^k)$; pour ces valeurs de k , on a $L_p(1-k,\omega^k) = L(1-k,\omega^k\omega^{-k}) = (1-\frac{1}{p^{1-k}})\zeta(1-k) = -(1-p^{k-1})\frac{B_k}{k}$ et donc $\mathrm{ord}_p(L_p(1-k,\omega^k) = \mathrm{ord}_p(B_k)$. Mais $L_p(1-k,\omega^k) = g(\gamma^{k-1}-1,\omega^k)$; pour $k\neq 0$ modulo $p-1$, la série $g(T,\omega^k)$ est dans $R[[T]]$, donc $g(\gamma^{k-1}-1,\omega^k) = g(0,\omega^k)$ modulo $(\gamma^{k-1}-1)R$. Pour $k=2,4,\ldots,p-3$ on a donc $\mathrm{ord}_p(g(0,\omega^k)) = 0$ si et seulement si $\mathrm{ord}_p(B_k) = 0$. Ainsi on retrouve le résultat classique suivant : $e_o^- = 0$ i.e. p ne divise pas h_o^- si et seulement si p ne divise aucun des B_k (dans $\mathbb{Z}_p$) pour $k = 2,4,\dots,p-3$.

§2. CLASSES RÉELLES ET UNITÉS CYCLOTOMIQUES.

Nous rappelons dans ce paragraphe des résultats classiques que l'on peut trouver par exemple dans [7]. On reprend les notations du §1 et on suppose que $m=1$; on a donc $q_n = p^{n+1}$ si $p \neq 2$, $q_n = 2^{n+2}$ si $p=2$, $K_n = \mathbb{Q}(\mu_{q_n})$ où μ_{q_n} est le groupe des racines $q_n^{\underline{\text{ièmes}}}$ de l'unité et $G_n = \mathrm{Gal}(K_n/\mathbb{Q})$. On va s'intéresser au nombre de classes h_n^+ du sous-corps réel maximal K_n^+ de K_n . Nous montrons l'existence d'un sous-groupe Cycl_n du groupe E_n des unités de K_n dont l'indice dans E_n est h_n^+ ; ce groupe Cycl_n est appelé le groupe des unités cyclotomiques de K_n .

Comme on l'a vu au §1, le groupe G_n s'identifie canoniquement à $(\mathbb{Z}/q_n\mathbb{Z})^*$; dans cette identification, le quotient $G_n^+ = \mathrm{Gal}(K_n^+/\mathbb{Q})$ de G_n apparait comme le quotient $(\mathbb{Z}/q_n\mathbb{Z})^*/\{\pm 1\}$ que nous noterons A_n dans ce §2. Si ε est un élément du groupe $\widehat{G_n^+}$ des caractères de G_n^+ et si $a \in A_n$, nous notons $\varepsilon(a)$ l'image par ε de l'élément de G_n^+ qui s'identifie à a . Avec ce vocabulaire on a :

PROPOSITION 2.1. <u>Soient</u> h_n^+ <u>et</u> R_n^+ <u>le nombre de classes et le régulateur de</u> K_n^+ ; <u>si</u> ζ_n <u>est une racine de l'unité d'ordre</u> q_n <u>et si</u> $\bar{\varepsilon}$ <u>est le caractère conjugué de</u> ε , <u>on a</u>

$$h_n^+ = \frac{1}{R_n^+} \prod_{\varepsilon \in \hat{G}_n^+ \setminus \{1\}} \left(\sum_{a \in A_n} \bar{\varepsilon}(a) \operatorname{Log}\left(\frac{1}{|1-\zeta_n^a|}\right)\right) .$$

<u>Démonstration</u>. Notons r_n le degré de $K_n^+/\mathbb{Q}$ i.e. $r_n = \frac{1}{2}\varphi(q_n)$ et D_n^+ la valeur absolue du discriminant de K_n^+. On a (§0 résultats 0.1 et 0.4) les égalités $\operatorname{Res}_{s=1} \zeta_{K_n^+}(s) = \dfrac{2^{r_n} h_n^+ R_n^+}{2\sqrt{D_n^+}} = \prod_{\varepsilon\in\widehat{G_n^+}\setminus\{1\}} L(1,\varepsilon)$.

Pour tout ε de $\widehat{G_n^+}$, on note ε^{pr} le caractère primitif associé à ε et $f(\varepsilon)$ son conducteur ; par définition $L(1,\varepsilon) = L(1,\varepsilon^{pr})$.

Posons $\zeta_\varepsilon = \zeta_n^{q_n/f(\varepsilon)}$ et $\tau(\varepsilon) = \sum_{t=1}^{f(\varepsilon)} \varepsilon^{pr}(t)\,\zeta_\varepsilon^t$; on a alors (I, §8, remarque 8.25) $L(1,\varepsilon^{pr}) = -\dfrac{\tau(\varepsilon)}{f(\varepsilon)} \sum_{b\in(\mathbb{Z}/f(\varepsilon)\mathbb{Z})^*} \overline{\varepsilon^{pr}}(b)\operatorname{Log}(1-\zeta_\varepsilon^{-b})$.

Compte-tenu de ce que $\varepsilon^{pr}(-b) = \varepsilon^{pr}(b)$ pour tout $b\in(\mathbb{Z}/f(\varepsilon)\mathbb{Z})^*$ et de ce que $\operatorname{Log}(1-\zeta^b)+\operatorname{Log}(1-\zeta^{-b}) = \operatorname{Log}|1-\zeta^b|^2$, on a (notations évidentes) $L(1,\varepsilon) = -\dfrac{\tau(\varepsilon)}{f(\varepsilon)} \sum_{b\in(\mathbb{Z}/f(\varepsilon)\mathbb{Z})^*\setminus\{\pm1\}} 2\,\overline{\varepsilon^{pr}}(b)\operatorname{Log}(|1-\zeta_\varepsilon^b|)$.

On a donc $\dfrac{2^{r_n} h_n^+ R_n^+}{2\sqrt{D_n^+}} = \prod_{\varepsilon\in\widehat{G_n^+}\setminus\{1\}} \left[\dfrac{\tau(\varepsilon)}{f(\varepsilon)} \sum_{b\in(\mathbb{Z}/f(\varepsilon)\mathbb{Z})^*/\{\pm1\}} 2\,\overline{\varepsilon^{pr}}(b)\operatorname{Log}\left(\dfrac{1}{|1-\zeta_\varepsilon^b|}\right)\right]$

qui, compte-tenu de la proposition 0.6 du §0, donne

$h_n^+ = \dfrac{1}{R_n^+} \prod_{\varepsilon\in\widehat{G_n^+}\setminus\{1\}} \left[\sum_{b\in(\mathbb{Z}/f(\varepsilon)\mathbb{Z})^*/\{\pm1\}} \overline{\varepsilon^{pr}}(b)\operatorname{Log}\left(\dfrac{1}{|1-\zeta_\varepsilon^b|}\right)\right]$. Soient maintenant a un élément de $(\mathbb{Z}/q_n\mathbb{Z})^*$ et b l'image de a dans $(\mathbb{Z}/f(\varepsilon)\mathbb{Z})^*$ par la projection canonique de $(\mathbb{Z}/q_n\mathbb{Z})^*$ sur $(\mathbb{Z}/f(\varepsilon)\mathbb{Z})^*$; on a $(\zeta_n^a)^{q_n/f(\varepsilon)} = \zeta_\varepsilon^b$. En conséquence, si X est une indéterminée, on a $\prod_{\substack{a\in(\mathbb{Z}/p^{n+1}\mathbb{Z})^*\\ a\to b}} (X-\zeta_n^a) = (X^{q_n/f(\varepsilon)} - \zeta_\varepsilon^b)$ où $a\to b$ signifie que l'image de a par la projection de $(\mathbb{Z}/q_n\mathbb{Z})^*$ sur $(\mathbb{Z}/f(\varepsilon)\mathbb{Z})^*$ est b ; en faisant $X=1$ il vient $\prod_{\substack{a\in(\mathbb{Z}/p^{n+1}\mathbb{Z})^*\\ a\to b}} (1-\zeta_n^a) = 1-\zeta_\varepsilon^b$ d'où l'on tire, pour tout b appartient $(\mathbb{Z}/f(\varepsilon)\mathbb{Z})^*\{\pm1\}$, l'égalité

$\prod_{\begin{cases} a\in A_n \\ a\to b\end{cases}} |1-\zeta_n^a| = |1-\zeta_\varepsilon^b|$ avec des notations évidentes. En remplaçant $|1-\zeta_\varepsilon^b|$ par ce produit dans l'expression de h_n^+ donnée ci-dessus, on conclut en remarquant que $\overline{\varepsilon}^{pr}(b) = \overline{\varepsilon}(a)$ si $a\to b$.

Rappelons deux lemmes :

LEMME 2.2 (Frobenius). Soient G un groupe abélien fini et f une application de G dans $\mathbb{C}$; on note $\hat{G}$ le groupe des caractères de G et $x_1,\dots,x_n$ les éléments de G. On a $\prod_{\varepsilon\in\hat{G}} (\sum_{a\in G} \varepsilon(a)f(a)) = \det(f(x_jx_i^{-1}))_{\substack{i=1,\dots,n\\ j=1,\dots,n}}$; ce déterminant ne dépend donc pas de l'ordre $x_1,\dots,x_n$ dans lequel on a rangé les éléments de G, nous le noterons $\det_{\left\{\substack{a\in G\\ b\in G}\right.}(f(ba^{-1}))$.

Démonstration. Notons V l'espace vectoriel des fonctions de G dans $\mathbb{C}$; pour tout $i=1,\dots,n$, notons $[x_i]$ l'élément de V qui vaut 1 sur x_i et 0 sur x_j si $i\neq j$; il est clair que la famille des $\{[x_i]\}_{i=1,\dots n}$ est une base de V sur $\mathbb{C}$. Désignons par T l'application linéaire de V dans lui-même définie par $T([x_j]) = \sum_{c\in G} f(c^{-1})[cx_j]$ pour $j=1,\dots,n$; on a $T([x_j]) = \sum_{i=1}^{n} f(x_jx_i^{-1})[x_i]$ donc le déterminant de l'application T est $\det(f(x_jx_i^{-1}))_{\substack{i=1,\dots,n\\ j=1,\dots,n}}$.

D'autre part, la famille des caractères $\{\varepsilon\}_{\varepsilon\in\hat{G}}$ est une autre base de V ; pour chacun de ces ε, on a $\varepsilon = \sum_{g\in G} \varepsilon(g)[g]$; on en tire $T(\varepsilon) = (\sum_{a\in G} \varepsilon(a)f(a))\varepsilon$ qui montre que le déterminant de T est $\prod_{\varepsilon\in\hat{G}} (\sum_{a\in G} \varepsilon(a)f(a))$ et montre que $\det(f(x_jx_i^{-1}))_{\substack{i=1,\dots,n\\ j=1,\dots,n}} = \prod_{\varepsilon\in\hat{G}} (\sum_{a\in G} \varepsilon(a)f(a))$. C.Q.F.D.

LEMME 2.3. On garde les notations du lemme 2.2 ; on a $\prod_{\varepsilon\in\hat{G}\setminus\{1\}} (\sum_{a\in G} \varepsilon(a)f(a)) = \det(f(x_jx_i^{-1}) - f(x_i^{-1}))_{\substack{i=1,\dots,n\\ j=1,\dots,n}}$; comme dans le lemme 2.2, nous notons $\det_{\left\{\substack{a\in G\setminus\{1\}\\ b\in G\setminus\{1\}}\right.}(f(ba^{-1}) - f(a^{-1}))$ ce déterminant.

Démonstration. Supposons que x_1 est l'élément neutre. Considérons la matrice $M = (f(x_jx_i^{-1}))_{\substack{i=1,\dots,n\\ j=1,\dots,n}}$ où i est l'indice de colonne et j l'indice de ligne. A partir de M formons M_1 en remplaçant la première colonne de M par la somme de toutes ses colonnes et en conservant les autres. Les déterminants de M et de M_1 sont égaux. Les termes de la première colonne de M_1 sont tous égaux à $\sum_{a\in G} f(a)$; en conséquence, le déterminant de M_1 est égal au déterminant de la matrice M_2 obtenue à partir de M_1 de la manière suivante : on conserve la première colonne et, pour $i \geqslant 2$, on soustrait de la $i^{\text{ème}}$ colonne de M_1 la colonne dont tous les termes sont égaux à $f(x_i^{-1})$. Le premier terme de la première ligne de M_2 est $\sum_{a\in G} f(a)$ et les autres termes de cette première ligne sont 0 ; en développant par rapport à cette ligne, on voit que le déterminant de M_2 est $\left(\sum_{a\in G} f(a)\right) \det_{\substack{a\in G\setminus\{1\}\\ b\in G\setminus\{1\}}} (f(ba^{-1}) - f(a^{-1}))$. Ce déterminant est égal au déterminant de M qui, d'après le lemme 2.2, est $\prod_{\varepsilon\in\hat{G}} (\sum_{a\in G} \varepsilon(a)f(a))$; notre lemme résulte de la comparaison de ces deux valeurs.

PROPOSITION 2.4. <u>On a</u> $h_n^+ = \dfrac{1}{R_n^+} \det_{\substack{a\in A_n\setminus\{1\}\\ b\in A_n\setminus\{1\}}} \left(\mathrm{Log}\left(\dfrac{|1-\zeta_n^{a^{-1}}|}{|1-\zeta_n^{ba^{-1}}|} \right)\right)$.

<u>Démonstration</u>. On utilise le lemme 2.3 dans l'expression de h_n^+ donnée dans la proposition 2.1.

Pour tout $b \in (\mathbb{Z}/q_n\mathbb{Z})^*$, le quotient $u_b = \dfrac{1-\zeta_n}{1-\zeta_n^b}$ est une unité de K_n ; l'égalité $\dfrac{1-\zeta_n^r}{1-\zeta_n^{rb}} = \left(\dfrac{1-\zeta_n}{1-\zeta_n^r}\right)^{-1} \cdot \left(\dfrac{1-\zeta_n}{1-\zeta_n^{rb}}\right)$ montre que le groupe engendré par les u_b lorsque b décrit $(\mathbb{Z}/q_n\mathbb{Z})^*$ ne dépend pas de la racine de l'unité ζ_n d'ordre q_n que nous avons choisie. On pose la définition suivante :

DEFINITION 2.5. <u>Le groupe des unités cyclotomiques du corps</u> K_n <u>est le sous-groupe du groupe des unités de</u> K_n <u>engendré par les</u> u_b <u>pour</u> b <u>parcourant</u> $(\mathbb{Z}/q_n\mathbb{Z})^*$. <u>Nous notons</u> Cycl_n <u>ce groupe (il contient le groupe des racines de l'unité de</u> A_n <u>puisque</u> $u_{-1} = -\zeta_n$).

2) <u>Le groupe des unités cyclotomiques du corps</u> K_n^+ <u>est</u>

l'intersection de Cycl_n *et de* K_n^+ *; nous le noterons* Cycl_n^+.

LEMME 2.6. *Soient* E_n *et* E_n^+ *les groupes des unités des corps* K_n *et* K_n^+ *; on a* $[E_n : \mathrm{Cycl}_n] = [E_n^+ : \mathrm{Cycl}_n^+]$.

Démonstration. La définition de Cycl_n^+ implique l'injectivité de l'homomorphisme de E_n^+/Cycl_n^+ dans E_n/Cycl_n induit par l'injection de E_n^+ dans E_n. D'autre part on sait (§0, propositions 0.9 et 0.12) que toute unité de E_n est le produit d'une unité de E_n^+ par une racine de l'unité de K_n. Ces racines de l'unité étant dans Cycl_n, notre homomorphisme est surjectif et le lemme est démontré.

LEMME 2.7. *Posons* $r_n = \frac{1}{2}\varphi(q_n) = [K_n^+:\mathbb{Q}]$. *Soient* $b_1,\ldots,b_{r_n-1}$ *une famille de* r_n-1 *éléments de* $(\mathbb{Z}/q_n\mathbb{Z})^*$ *dont l'image dans* A_n *est* $A_n\setminus\{1\}$ *; le groupe* Cycl_n *est engendré par les* u_{b_i} *pour* $i=1,\ldots,b_{r_n-1}$ *et par* $\mu(K_n)$.

Démonstration. Cela résulte clairement de l'égalité $\dfrac{1-\zeta_n}{1-\zeta_n^{-b}} = -\zeta_n^b\,\dfrac{1-\zeta_n}{1-\zeta_n^b}$ pour tout $b \in (\mathbb{Z}/q_n\mathbb{Z})^*$.

PROPOSITION 2.8. *On a* $h_n^+ = [E_n^+ : \mathrm{Cycl}_n^+]$.

Démonstration. Les propositions 0.9 et 0.12 du §0 montrent que toute unité de K_n s'écrit comme le produit d'une unité de K_n^+ par un élément de $\mu(K_n)$; nous emploierons plusieurs fois ce fait sans le rejustifier. Soient $b_1,\ldots b_{r_n-1}$ comme dans le lemme 2.7 ; pour tout i, on a $u_{b_i} = \eta_i\, v_{b_i}$ avec $\eta_i \in \mu(K_n)$ et $v_{b_i} \in E_n^+$; les v_{b_i} sont définis au signe près puisque $+1$ et -1 sont les seules racines de l'unité contenues dans K_n^+ ; montrons que Cycl_n^+ est engendré par les v_{b_i} et par ± 1 : tout d'abord $v_{b_i} = \eta_i^{-1} u_{b_i}$ donc $v_{b_i} \in \mathrm{Cycl}_n^+$; d'autre part, soit $v \in \mathrm{Cycl}_n^+$; on a $v \in \mathrm{Cycl}_n$ donc $v = \eta \prod_{i=1}^{r_n-1} u_{b_i}^{n(i)}$ pour des $n(i) \in \mathbb{Z}$; on a donc $v = (\eta \prod_{j=1}^{r_n-1} \eta_i^{n(i)}) \prod_{i=1}^{r_n-1} v_{b_i}^{n(i)}$; la quantité entre parenthèses est une racine de l'unité et est égale à $\left(\prod_{j=1}^{r_n-1} v_{b_i}^{n(i)}\right)^{-1} v$ qui est un réel, c'est donc $+1$ ou -1 et notre assertion est démontrée. Nous allons montrer que le régulateur du groupe d'unité engendré par les v_{b_i} est $\det_{\begin{cases} a\in A_n\setminus\{1\} \\ b\in A_n\setminus\{1\}\end{cases}}\left(\operatorname{Log}\left(\frac{|1-\zeta_n^{a^{-1}}|}{|1-\zeta_n^{ba^{-1}}|}\right)\right)$; en vertu de la proposition 2.4 cela impliquera que h_n^+ est l'indice dans $E_n^+/\{\pm 1\}$ du groupe engendré par les classes des v_{b_i} dans $E_n^+/\{\pm 1\}$ et donc que $h_n^+ = [E_n^+ : \mathrm{Cycl}_n^+]$ ce qu'on veut. Pour chaque $i = 1,\dots,r_n-1$, notons σ_i l'automorphisme de K_n qui envoie ζ_n sur $\zeta_n^{b_i^{-1}}$; on a $\sigma_i(u_{b_j}) = \dfrac{1-\zeta_n^{b_i^{-1}}}{1-\zeta_n^{b_j b_i^{-1}}}$, donc $\sigma_i(v_{b_j}) = \sigma_i(\eta_j^{-1}).\dfrac{1-\zeta_n^{b_i^{-1}}}{1-\zeta_n^{b_j b_i^{-1}}}$ et $|\sigma_i(v_{b_j})| = \dfrac{|1-\zeta_n^{b_i^{-1}}|}{|1-\zeta_n^{b_j b_i^{-1}}|}$. Lorsque i décrit $1,\dots,r_n-1$ la restriction de σ_i à K_n^+ décrit tous les éléments de $\mathrm{Gal}(K_n^+/\mathbb{Q})$ distincts de l'identité ; le régulateur du groupe engendré par les v_{b_i} est donc la valeur absolue du déterminant $\det(\operatorname{Log}|\sigma_i(v_j)|)_{\substack{i=1,\dots,r_n-1\\ j=1,\dots,r_n-1}} =$

$$\det\left(\operatorname{Log}\left(\frac{|1-\zeta_n^{b_i^{-1}}|}{|1-\zeta_n^{b_j b_i^{-1}}|}\right)\right)_{\substack{i=1,\dots,r_n-1\\ j=1,\dots,r_n-1}}$$

; mais ce déterminant est $\det_{\begin{cases} a\in A_n\setminus\{1\} \\ b\in A_n\setminus\{1\}\end{cases}}\left(\operatorname{Log}\left(\frac{|1-\zeta_n^{a^{-1}}|}{|1-\zeta_n^{ba^{-1}}|}\right)\right)$, qui est positif comme le montre la proposition 2.4 et donc est le régulateur du groupe engendré par les v_{b_i} ; c'est ce qu'on voulait.

§3. UNITÉS CYCLOTOMIQUES ET Γ EXTENSIONS.

Ce paragraphe sert essentiellement à introduire le théorème 3.7 qui sera démontré dans les deux paragraphes suivants. Nous reprenons les notations du §1 et nous supposons que $m=1$ et que p est impair. On a donc $K_n = \mathbb{Q}(\mu_{p^{n+1}})$, $G_n = \mathrm{Gal}(K_n/\mathbb{Q})$ et G_n est canoniquement isomorphe à $(\mathbb{Z}/p^{n+1}\mathbb{Z})^*$. On pose $K_\infty = \bigcup_{n\geqslant 0} K_n$ et $G_\infty = \mathrm{Gal}(K_\infty/\mathbb{Q})$; on note $\varkappa$ l'isomorphisme de G_∞ sur $\varprojlim(\mathbb{Z}/p^{n+1}\mathbb{Z})^*$ qui est la limite projective des isomorphismes canoniques des G_n sur les $(\mathbb{Z}/p^{n+1}\mathbb{Z})^*$. On a $\varprojlim(\mathbb{Z}/p^{n+1}\mathbb{Z})^* = \mathbb{Z}_p^* = \mu_{p-1}\times(1+p\mathbb{Z}_p)$ donc $\varkappa$ identifie G_∞ et $\mu_{p-1}\times(1+p\mathbb{Z}_p)$. On note Δ et Γ les sous-groupes de G_∞ qui s'identifient respectivement à μ_{p-1} et à $1+p\mathbb{Z}_p$; on a donc $\Gamma = \mathrm{Gal}(K_\infty/K_o)$. Pour tout $n\geqslant 0$, on pose aussi $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$ de sorte que Γ_n s'identifie à $1+p^{n+1}\mathbb{Z}_p$, que $\mathrm{Gal}(K_n/K_o) = \Gamma/\Gamma_n$ et que $\Gamma=\Gamma_o$. Le groupe Γ s'identifie (non canoniquement) au groupe $\mathbb{Z}_p$; pour cette raison nous disons que K_∞/K_o est une Γ-extension (en général, lorsque une extension galoisienne L/K a un groupe de Galois isomorphe à $\mathbb{Z}_p$, on note Γ son groupe de Galois et on dit que L/K est une Γ-extension).

Pour tout entier $n\geqslant 0$, on note $\underline{\underline{p}}_n$ l'unique idéal premier de K_n contenant p ; on note C_n le sous-groupe du groupe Cycl_n des unités cyclotomiques de K_n (§2, définition 2.5) formé des éléments congrus à 1 modulo $\underline{\underline{p}}_n$. Enfin nous choisissons une clôture algébrique $\bar{\mathbb{Q}}_p$ de $\mathbb{Q}_p$ et un plongement de K_∞ dans $\bar{\mathbb{Q}}_p$ de sorte que l'on considère les K_n comme inclus dans $\bar{\mathbb{Q}}_p$; on désigne par Φ_n l'adhérence de K_n dans $\bar{\mathbb{Q}}_p$ (donc Φ_n est le complété de K en $\underline{p}_n$) et par U_n le groupe des unités principales de Φ_n (i.e. le groupe des unités de Φ_n congrues à 1 modulo l'idéal maximal de Φ_n). Le groupe C_n est inclus dans U_n qui est compact et nous notons $\bar{C}_n$ l'adhérence de C_n dans U_n. Le groupe $\bar{C}_n$ est donc un sous-$\mathbb{Z}_p$-module de U_n, nous allons nous intéresser au quotient $U_n/\bar{C}_n$. Rappelons le résultat suivant qui découle directement du travail de Brumer [3] (conjecture de Leopoldt pour le corps K_n).

PROPOSITION 3.1. <u>Le</u> $\mathbb{Z}_p$ <u>rang de</u> $\bar{C}_n$ <u>est</u> $\frac{1}{2}\varphi(q_n)-1$.

<u>Démonstration</u>. $\frac{1}{2}\varphi(q_n)-1$ est le $\mathbb{Z}$ rang du groupe E_n des unités de K_n ; Brumer [3] montre que, si $\varepsilon_1,\dots,\varepsilon_{\frac{1}{2}\varphi(q_n)-1}$ est une famille d'unités libre sur $\mathbb{Z}$, alors cette famille (considérée comme une famille d'éléments de Φ_n) est libre sur $\mathbb{Z}_p$. Le lemme 2.6 et la proposition 2.8 montrent que Cycl_n est d'indice fini dans E_n ; l'élévation à la puissance $p-1$ envoyant Cycl_n dans C_n, on en déduit qu'il existe une famille de $\frac{1}{2}\varphi(q_n)-1$ éléments de C_n libre sur $\mathbb{Z}$; le résultat de Brumer montre que cette famille reste libre sur $\mathbb{Z}_p$; on conclut en remarquant que, $\mathbb{Z}_p$ étant compact, $\bar{C}_n$ est le $\mathbb{Z}_p$-module engendré dans Φ_n par C_n.

Pour tout $n \geqslant 0$ le groupe $\mathrm{Gal}(\Phi_n/\mathbb{Q}_p)$ s'identifie à G_n puisque p est totalement ramifié dans K_n. Le groupe U_n est stable par $\mathrm{Gal}(\Phi_n/\mathbb{Q}_p)$ donc est un $\mathbb{Z}_p[G_n]$-module. En remarquant que Cycl_n est stable par G_n, on voit que $\bar{C}_n$ est aussi un $\mathbb{Z}_p[G_n]$-module. D'autre part, $\mathbb{Z}_p[G_n]$ est un $\mathbb{Z}_p$-module libre de dimension finie donc, en tant que tel, est canoniquement muni d'une topologie que nous appellerons sa topologie naturelle ; rappelons la définition :

DEFINITION 3.2. <u>Soient</u> M <u>un</u> $\mathbb{Z}_p$-<u>module libre de dimension finie et</u> φ <u>un isomorphisme</u> $\mathbb{Z}_p$-<u>linéaire de</u> M <u>sur</u> $\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$; <u>la topologie de</u> M <u>obtenue en transportant la topologie produit sur</u> $\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$ <u>par</u> φ <u>ne dépend pas de</u> φ <u>et est appelée la topologie naturelle de</u> M .

On vérifie que, pour sa topologie naturelle, $\mathbb{Z}_p[G_n]$ est un anneau topologique et que U_n et $\bar{C}_n$ sont des $\mathbb{Z}_p[G_n]$-modules topologiques. Par la restriction des automorphismes de K_∞ à K_n , le groupe Δ s'identifie au sous-groupe cyclique d'ordre $p-1$ de G_n et on a $G_n = \Delta \times \Gamma/\Gamma_n$. L'anneau $\mathbb{Z}_p[G_n]$ contient donc les deux sous-anneaux $\mathbb{Z}_p[\Delta]$ et $\mathbb{Z}_p[\Gamma/\Gamma_n]$; les topologies induites par la topologie de $\mathbb{Z}_p[G_n]$ sur ces deux sous-anneaux coïncident avec leurs topologies naturelles de $\mathbb{Z}_p$-modules libres de dimensions finies (définition 3.2) et donc tout $\mathbb{Z}_p[G_n]$-module N peut-être considéré comme un $\mathbb{Z}_p[\Delta]$ et comme un $\mathbb{Z}_p[\Gamma/\Gamma_n]$-module topologique, les topologies de $\mathbb{Z}_p[\Delta]$ et de $\mathbb{Z}_p[\Gamma/\Gamma_n]$ étant les topologies naturelles. On note χ la restriction de $\varkappa$ à Δ , c'est-à-dire que χ vérifie la propriété suivante : si $\tau \in \Delta$ et si ζ_1 est une racine de l'unité d'ordre p , alors $\chi(\tau)$ est la racine $p-1^{\underline{\text{ième}}}$ de l'unité de $\mathbb{Z}_p$ telle que $\tau(\zeta_1) = \zeta_1^{\chi(\tau)}$. Les $p-1$ caractères de Δ sont les χ^i pour $i = 1,\ldots,p-1$; on pose $e_i = \frac{1}{p-1} \sum_{\tau \in \Delta} \chi^i(\tau^{-1})\tau$; on vérifie facilement que $1 = \sum_{i=1}^{p-1} e_i$, que $e_i e_j = 0$ si $i \neq j$ et que $e_i^2 = e_i$. On en déduit que tout $\mathbb{Z}_p[\Delta]$-module N se décompose canoniquement en $N = \bigoplus_{i=1}^{p-1} N^{(i)}$ où $N^{(i)}$ est l'ensemble des éléments de N invariants par e_i . Pour chaque i on vérifie que $N^{(i)}$ est aussi l'ensemble des éléments de N sur lesquels l'action de $\tau \in \Delta$ est la multiplication par $\chi^i(\tau)$; de plus si $0 \to N_1 \to N_2 \to N_3 \to 0$ est une suite exacte de $\mathbb{Z}_p[\Delta]$-module, alors $0 \to N_1^{(i)} \to N_2^{(i)} \to N_3^{(i)} \to 0$ reste exacte. Enfin, si N est un $\mathbb{Z}_p[G_n]$-module topologique, les $N^{(i)}$

sont de $\mathbb{Z}_p[G_n]$-modules topologiques ; dans la suite nous nous intéresserons essentiellement aux $N^{(i)}$ en tant que $\mathbb{Z}_p[\Gamma/\Gamma_n]$-modules topologiques (on semble ainsi négliger l'information donnée par l'action de Δ ; en fait cette information a déjà été utilisée dans la définition des $N^{(i)}$). En résumé nous posons :

DEFINITION 3.3. <u>Soit</u> N <u>un</u> $\mathbb{Z}_p[G_n]$-<u>module topologique ; pour</u> $i=1,\dots,p-1$ <u>on note</u> $N^{(i)}$ <u>l'ensemble des éléments de</u> N <u>invariants par</u> $e_i = \frac{1}{p-1}\sum_{\tau\in\Delta}\chi^i(\tau^{-1})\tau$; <u>les</u> $N^{(i)}$ <u>sont des</u> $\mathbb{Z}_p[\Gamma/\Gamma_n]$-<u>modules topologiques et l'on a</u> $N = \bigoplus_{i=1}^{p-1} N^{(i)}$.

Dans la suite nous nous intéressons spécialement aux $\mathbb{Z}_p[G_n]$-modules topologiques U_n , $\bar{C}_n$ et $U_n/\bar{C}_n$; il est clair que l'on a $(U_n/\bar{C}_n)^{(i)} = U_n^{(i)}/\bar{C}_n^{(i)}$.

Pour tout couple (m,n) d'entiers tels que $m \geqslant n \geqslant 0$, on note $N_{m,n}$ la norme de Φ_m sur Φ_n ; c'est une application continue qui envoie U_m dans U_n . Notons ζ_m une racine de l'unité d'ordre p^{m+1} contenue dans Φ_m de sorte que $\zeta_n = \zeta_m^{p^{m-n}}$ est une racine de l'unité d'ordre p^{n+1} . Pour tout $c \in (\mathbb{Z}/p^{m+1}\mathbb{Z})^*$, le polynome minimal de $1-\zeta_m^c$ sur $\Phi_n = \mathbb{Q}_p(\zeta_n)$ est $(1-X)^{p^{m-n}} - \zeta_n^c$ donc $N_{m,n}(1-\zeta_m^c) = -(1-\zeta_n^c)$ et donc $N_{m,n}\left(\frac{1-\zeta_m}{1-\zeta_m^b}\right) = \frac{1-\zeta_n}{1-\zeta_n^b}$. Cela montre que l'image par $N_{m,n}$ de Cycl_m (considéré comme inclus dans Φ_m) est Cycl_n (considéré comme inclus dans Φ_n) ; l'image de $1+\underline{p}_m$ par $N_{m,n}$ étant $1+\underline{p}_n$ on a donc $N_{m,n}(C_m) \subset C_n$; la continuité de $N_{m,n}$ et la compacité de $\bar{C}_m$ et $\bar{C}_n$ montrent alors que $N_{m,n}(\bar{C}_m) \subset \bar{C}_n$. En conséquence $N_{m,n}$ induit une application continue du quotient $U_m/\bar{C}_m$ vers $U_n/\bar{C}_n$. De plus, la projection canonique de G_m sur G_n induit un homomorphisme continu de $\mathbb{Z}_p[G_m]$ sur $\mathbb{Z}_p[G_n]$ et $N_{m,n}$ est compatible avec cet homomorphisme (i.e. pour $u \in U_m$, $x \in \mathbb{Z}_p[G_m]$ on a $N_{m,n}(x.u) = \bar{x}N_{m,n}(u)$ en notant $\bar{x}$ l'image de x dans $\mathbb{Z}_p[G_n]$) ;

on en déduit que $N_{m.n}(U_m^{(i)})$ et $N_{m,n}(\bar{C}_m^{(i)})$ sont respectivement inclus dans $U_n^{(i)}$ et $\bar{C}_n^{(i)}$, donc que $N_{m,n}$ induit une application de $U_m^{(i)}/\bar{C}_m^{(i)}$ vers $U_n^{(i)}/\bar{C}_n^{(i)}$. Pour tout $i=1,\dots,p-1$, les systèmes $(U_n^{(i)},N_{m,n})_{m,n\in\mathbb{Z}}$, $(\bar{C}_n^{(i)},N_{m,n})_{m,n\in\mathbb{Z}}$ et $(U_n^{(i)}/\bar{C}_n^{(i)},N_{m,n})_{m,n\in\mathbb{Z}}$ sont des systèmes projectifs ; la compatibilité de $N_{m,n}$ avec la projection de $\mathbb{Z}_p[G_m]$ sur $\mathbb{Z}_p[G_n]$ implique la compatibilité de $N_{m,n}$ avec la projection de $\mathbb{Z}_p[\Gamma/\Gamma_m]$ sur $\mathbb{Z}_p[\Gamma/\Gamma_n]$ et permet de définir une structure de $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$-module sur $\varprojlim(U_n^{(i)})$, $\varprojlim(\bar{C}_n^{(i)})$ et $\varprojlim(U_n^{(i)}/\bar{C}_n^{(i)})$; de plus si l'on munit toutes ces $\varprojlim$ des topologies limites projectives, ces $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$-modules sont des modules topologiques. La proposition suivante est fondamentale dans la suite.

PROPOSITION 3.4. <u>Soit</u> γ <u>un</u> $\mathbb{Z}_p$ <u>générateur de</u> Γ $(\simeq 1+p\mathbb{Z}_p)$ <u>et, pour tout</u> n, <u>soit</u> γ_n <u>la classe de</u> γ <u>dans</u> Γ/Γ_n ; <u>on identifie</u> γ <u>avec l'élément</u> $(\gamma_n)_{n\geqslant 0}$ <u>de</u> $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$. <u>Il existe un isomorphisme d'anneaux de</u> $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$ <u>sur l'anneau des séries formelles</u> $\mathbb{Z}_p[[T]]$ <u>qui envoie</u> γ <u>sur</u> $1+T$. <u>On pose</u> $\Lambda=\mathbb{Z}_p[[T]]$ <u>et on note</u> $\mathfrak{m}=(p,T)$ <u>son idéal maximal</u> ; <u>l'isomorphe précédent est un isomorphisme topologique si</u> Λ <u>est muni de la topologie</u> $\mathfrak{m}$ <u>adique</u>.

<u>Démonstration</u>. Pour tout n, posons $\omega_n(T)=(1+T)^{p^n}-1$; la surjection de $\mathbb{Z}_p[T]$ sur $\mathbb{Z}_p[\Gamma/\Gamma_n]$ qui envoie T sur γ_n-1 induit un isomorphisme topologique de $\mathbb{Z}_p[T]/(\omega_n(T))$ muni de sa topologie naturelle (définition 3.2) sur $\mathbb{Z}_p[\Gamma/\Gamma_n]$ muni de sa topologie naturelle. Si $m\geqslant n$, le polynôme $\omega_n(T)$ divise $\omega_m(T)$ donc $\mathbb{Z}_p[T]/(\omega_m(T))$ se projette canoniquement sur $\mathbb{Z}_p[T]/(\omega_n(T))$; modulo les isomorphismes que l'on vient de décrire, ces projections correspondent aux applications de $\mathbb{Z}_p[\Gamma/\Gamma_m]$ sur $\mathbb{Z}_p[\Gamma/\Gamma_n]$ déduites des projections de Γ/Γ_m sur Γ/Γ_n ; donc $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$ est isomorphe à $\varprojlim(\mathbb{Z}_p[T]/(\omega_n(T)))$; toutes nos flèches étant continues, cet isomorphisme est un isomorphisme topologique. Pour conclure nous aurons

besoin du lemme de préparation de Weierstrass qui s'énonce ainsi (pour sa démonstration voir [14],[8]) :

PROPOSITION 3.5. Soit $g(T)$ un élément de $\Lambda = \mathbb{Z}_p[[T]]$ qui n'est pas divisible par p et soit n_o le plus petit entier tel que le coefficient de T^{n_o} n'est pas divisible par p. Alors, pour tout $f(T) \in \Lambda$, il existe un couple $(Q(T), r(T))$ unique avec $Q(T)$ dans Λ et $r(T)$ polynôme de degré strictement plus petit que n_o tel que $f(T) = g(T)Q(T) + r(T)$.

Appliquons ce résultat avec $g(T) = \omega_n(T)$; on a $n_o = p^n$ donc tout $f(T) \in \Lambda$ est congru modulo $\omega_n(T)\Lambda$ à un polynôme et un seul de degré strictement plus petit que p^n ; cela implique que l'injection de $\mathbb{Z}_p[T]$ dans $\mathbb{Z}_p[[T]] = \Lambda$ induit un isomorphisme de $\mathbb{Z}_p[T]/\omega_n(T)$ sur $\Lambda/\omega_n(T)\Lambda$. Munissons Λ de la topologie $\mathfrak{m}$ adique et $\Lambda/\omega_n(T)\Lambda$ de la topologie quotient ; l'isomorphisme précédent est un isomorphisme topologique $(\mathbb{Z}_p[T]/(\omega_n(T))$ étant bien sûr muni de sa topologie naturelle). C'est un exercice facile de montrer que Λ muni de la topologie $\mathfrak{m}$ adique est compact ; les $\omega_n(T)\Lambda$ sont donc des sous-groupes fermés de Λ (image du compact Λ par la multiplication par $\omega_n(T)$) de Λ ; enfin, en remarquant que $\omega_n(T) \in \mathfrak{m}^{n+1}$ pour tout n, on voit que $\bigcap_n (\omega_n(T)\Lambda) = 0$ et notre proposition résulte du lemme suivant :

LEMME 3.6. Soient G un groupe compact et $(H_i)_{i\in I}$ une famille filtrante décroissante de sous-groupes fermés distingués telle que $\bigcap_{i\in I} H_i = 0$; on a alors $G = \varprojlim (G/H_i)$.

Démonstration. Voir [2] par exemple.

La proposition 3.4 montre que $\varprojlim(U_n^{(i)}/\bar{C}_n^{(i)})$ est un Λ-module. Le théorème que nous démontrerons dans les deux paragraphes suivants s'énonce ainsi :

THEOREME 3.7 (Iwasawa). <u>Soit</u> $i = 2,4,\ldots,p-3$ (i.e. $i \in \{1,\ldots,p-1\}$, i <u>pair et</u> $i \neq p-1$) <u>et soit</u> $Y^{(i)} = \varprojlim(U_n^{(i)}/\bar{C}_n^{(i)})$; <u>on a</u> :

1) <u>Le</u> Λ-<u>module</u> $Y^{(i)}$ <u>est isomorphe à</u> $\Lambda/(F_i(T))$ <u>où</u> $F_i(T)$ <u>est la série définie de la manière suivante</u> : <u>on note</u> $g_i(T)$ <u>la série telle que</u> $g_i(\varkappa(\gamma)^{-s}-1) = L_p(s,\omega^i)$ <u>pour tout</u> $s \in \mathbb{Z}_p$ (<u>voir</u> I, §7) <u>et on pose</u> $F_i(T) = g_i(\frac{1+T}{\varkappa(\gamma)} - 1)$.

2) <u>Pour tout</u> $n \geqslant 0$, <u>la projection de</u> $Y^{(i)}$ <u>sur</u> $U_n^{(i)}/\bar{C}_n^{(i)}$ <u>induit un isomorphisme de</u> $\Lambda/(F_i(T),\omega_n(T))$ <u>sur</u> $U_n^{(i)}/\bar{C}_n^{(i)}$.

REMARQUE 3.8. Appliquons le 2) du théorème 3.7 avec $n = 0$; on a $\omega_o(T) = T$, donc $\Lambda/(\omega_o(T),F_i(T))$ est isomorphe à $\mathbb{Z}_p/F_i(0)\mathbb{Z}_p$. Mais on a $F_i(0) \equiv g_i(\varkappa(\gamma)^{-1}-1) \equiv g_i(\varkappa(\gamma)^{j}-1)$ modulo $p\mathbb{Z}_p$ pour tout $j \in \mathbb{Z}$; en particulier $F_i(0) \equiv g_i(\varkappa(\gamma)^{i-1}-1) = L_p(1-i,\omega^i) = L(1-i,\omega^i\omega^{-i}) = (1-p^{i-1})\zeta(1-i) = (p^{i-1}-1)\frac{B_i}{i}$ modulo $p\mathbb{Z}_p$. En conséquence, on a $U_o^{(i)} \neq \bar{C}_o^{(i)}$ si et seulement si p divise B_i ; ce résultat était (au langage près) connu de Kummer ; notre théorème apparait donc comme un approfondissement de ce résultat ancien.

REMARQUE 3.9. Si i est impair, les unités de K_n congrues à 1 modulo $\underline{\underline{p}}_n$ et invariantes par e_i sont réduites à 1 si $i \neq 1$ et à $\mu_{p^{n+1}}$ si $i = 1$ (en effet, si $\tau \in \Delta$ et si x est un élément d'un $\mathbb{Z}_p[\Delta]$-module invariant par e_i , on a $\tau(x) = \chi^i(\tau).x$; si τ est la conjugaison complexe et x une unité de K_n invariante par e_i , on a donc $\tau(x) = x^{-1}$ puisque $\chi^i(\tau) = -1$; cela montre (proposition 0.12) que x est dans $\mu_{p^{n+1}}$; enfin par définition de χ , tout $x \in \mu_{p^{n+1}}$ est invariant par e_1 et cela prouve notre assertion). En conséquence $\bar{C}_n^{(i)}$ est réduit à 1 si i est impair et $i \neq 1$ et à $\mu_{p^{n+1}}$ si $i = 1$; le quotient $U_n^{(i)}/\bar{C}_n^{(i)}$ est donc la partie libre de $U_n^{(i)}$.

Pour démontrer notre théorème on va reprendre, dans le cas cyclotomique, des arguments donnés par Coates-Wiles [5] dans le cas elliptique. Nous étudierons d'abord le Λ-module $U^{(i)} = \varprojlim(U_n^{(i)})$ et nous nous servirons du lemme suivant :

LEMME 3.10. <u>Soient</u> $U^{(i)} = \varprojlim(U_n^{(i)})$ <u>et</u> $\bar{C}^{(i)} = \varprojlim(\bar{C}_n^{(i)})$ <u>alors</u> $U^{(i)}/\bar{C}^{(i)}$ <u>est isomorphe en tant que</u> Λ-<u>module</u> <u>à</u> $\varprojlim(U_n^{(i)}/\bar{C}_n^{(i)})$.

<u>Démonstration</u>. Pour tout $n \geqslant 0$ on a une suite exacte de $\mathbb{Z}_p[\Gamma/\Gamma_n]$-module $0 \to \bar{C}_n^{(i)} \to U_n^{(i)} \to U_n^{(i)}/\bar{C}_n^{(i)} \to 0$; en passant à la limite projective, on en déduit une injection de $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n]) = \Lambda$ module de $U^{(i)}/\bar{C}^{(i)}$ dans $\varprojlim(U_n^{(i)}/\bar{C}_n^{(i)})$ et on sait que l'image de cette injection est dense. Les $U_n^{(i)}$ étant compacts, $U^{(i)}$ est compact donc notre image est compacte et donc est $\varprojlim(U_n^{(i)}/\bar{C}_n^{(i)})$ tout entier ce qui achève la démonstration.

Pour terminer ce paragraphe, rappelons que l'anneau Λ a été étudié par Iwasawa ; les résultats d'Iwasawa sont exposés dans [ ] par exemple. Rappelons ici (sans démonstrations) ceux de ces résultats dont nous aurons besoin. On pose tout d'abord une définition :

DEFINITION 3.11. <u>Soient</u> M <u>et</u> N <u>deux</u> Λ-<u>modules</u> <u>de type fini</u> ; <u>on dit que</u> M <u>est quasi-isomorphe à</u> N <u>si il existe une suite exacte de</u> Λ-<u>modules</u> $0 \to A \to M \to N \to B \to 0$ <u>avec</u> A <u>et</u> B <u>finis</u>.

REMARQUE 3.12. La relation "quasi-isomorphe" n'est pas réflexive comme le montre l'exemple suivant : on prend $M = \mathfrak{M} = (p,T)$ et $N = \Lambda$; on a $0 \to \mathfrak{M} \to \Lambda \to \Lambda/\mathfrak{M} = \mathbb{F}_p \to 0$ donc M est quasi-isomorphe à N . Par contre, si $\Lambda \to \mathfrak{M}$ est un homomorphisme de Λ-module et si a est l'image de 1 , le conoyau de cette flèche est $\mathfrak{M}/(a)$; il est facile de vérifier que (a) ne peut pas contenir à la fois une puissance de p et une puissance de T , donc que $\mathfrak{M}/(a)$ n'est pas fini ; cela signifie que N n'est pas quasi-isomorphe à M .

PROPOSITION 3.13. <u>Soit</u> M <u>un</u> Λ-<u>module</u> <u>de type fini</u>, <u>alors</u> M <u>est quasi-isomorphe à un</u> Λ-<u>module</u> N <u>du type</u>

$N = \Lambda^r \oplus (\bigoplus_{i=1}^{k} \Lambda/p^{n_i}\Lambda) \oplus (\bigoplus_{j=1}^{\ell} \Lambda/(f_j))$ <u>où</u> f_j <u>est un polynôme distingué</u> i.e. <u>du type</u> $T^n + \sum_{i=0}^{n-1} a_i T^i$ <u>avec tous les</u> a_i <u>divisibles par</u> p .

Pour se servir de la proposition précédente il faut savoir démontrer qu'un Λ-module est de type fini ; on a :

LEMME 3.14. <u>Soit</u> M <u>un</u> Λ-<u>module</u> <u>topologique compact tel que</u> $M/\mathfrak{m}M$ <u>est de dimension finie sur</u> $\Lambda/\mathfrak{m}\Lambda = F_p$, <u>alors</u> M <u>est de type fini sur</u> Λ

<u>Démonstration</u>. Soit $m_1,\ldots,m_n$ une famille finie d'éléments de M dont les classes modulo $\mathfrak{m}M$ engendrent le $\mathbb{F}_p$-espace vectoriel $M/\mathfrak{m}M$. Notons P le Λ-module engendré par $m_1,\ldots,m_n$; ce module est un sous-module de M et le quotient M/P est un Λ-module R tel que $R/\mathfrak{m}R = 0$; le lemme suivant montre que $R = 0$ i.e. que $M = P$ et achève donc notre démonstration.

LEMME (de Nakayama) 3.15. <u>Soit</u> R <u>un</u> Λ-<u>module</u> <u>compact tel que</u> $R/\mathfrak{m}R = 0$, <u>alors</u> $R = 0$.

<u>Démonstration</u>. Soit V un voisinage de 0 dans R ; pour tout $r \in R$, il existe un entier $n(r)$ et un voisinage ouvert V_r de r tel que $\lambda.s \in V$ pour tout $\lambda \in \mathfrak{m}^{n(r)}$ et tout $s \in V_r$. La famille $(V_r)_{r\in R}$ étant un recouvrement ouvert de R , on a $R = \bigcup_{i=1}^{n} V_{r_i}$. Soit alors $n = \sup(n(r_i) ; i=1,\ldots,n)$, on a $\mathfrak{m}^n R \subset V$. Mais $R/\mathfrak{m}R = 0$ implique $R = \mathfrak{m}R$ et donc $R = \mathfrak{m}^n R$; on a donc $R \subset V$. Le voisinage V de 0 étant arbitraire, il en résulte $R = 0$. C.Q.F.D.

§4. LE Λ-MODULE $U^{(i)}$.

On conserve les notations introduites au §3 et on étudie le Λ-module $U^{(i)}$. Pour cela nous commençons, pour tout $n \geqslant 0$, par interpréter $U_n^{(i)}$ comme le groupe de Galois d'une extension locale. Plus précisément introduisons, pour tout $n \geqslant 0$ la p-extension abélienne maximale M_n de Φ_n ; l'extension $M_n/\mathbb{Q}_p$ est galoisienne donc le groupe de Galois $G_n = \mathrm{Gal}(\Phi_n/\mathbb{Q}_p)$ agit par conjugaison sur le groupe abélien $\mathrm{Gal}(M_n/\Phi_n)$; celui-ci, étant en plus une limite projective de p-groupes finis, est canoniquement muni d'une structure de $\mathbb{Z}_p$-module ; $\mathrm{Gal}(M_n/\Phi_n)$ est donc un $\mathbb{Z}_p[G_n]$-module. Le corps Φ_∞ est inclus dans M_n , donc le groupe $\mathrm{Gal}(M_n/\Phi_\infty)$ est un sous-groupe de $\mathrm{Gal}(M_n/\Phi_n)$; nous le noterons $\mathfrak{X}_n$. On vérifie que $\mathfrak{X}_n$ est un sous-$\mathbb{Z}_p[G_n]$-module de $\mathrm{Gal}(M_n/\Phi_n)$. On a donc (définition 3.3) $\mathfrak{X}_n = \prod_{i=1}^{p-1} \mathfrak{X}_n^{(i)}$ chaque $\mathfrak{X}_n^{(i)}$ étant un $\mathbb{Z}_p[\Gamma/\Gamma_n]$-module. Nous allons démontrer le résultat suivant :

PROPOSITION 4.1. <u>Pour</u> $i=1,\dots,p-2$ (i.e. $i \neq p-1$) <u>les</u> $\mathbb{Z}_p[\Gamma/\Gamma_n]$-<u>modules</u> $U_n^{(i)}$ <u>et</u> $\mathfrak{X}_n^{(i)}$ <u>sont isomorphes</u>.

<u>Démonstration</u>. Elle repose essentiellement sur la théorie du corps de classes local que nous supposons connue (voir [15] par exemple). La démonstration sera divisée en 4 points.

1) Pour tout entier $t \geqslant 0$, notons $A_{n,t}$ l'extension abélienne maximale de Φ_n d'exposant p^t (i.e. telle que $\mathrm{Gal}(A_{n,t}/\Phi_n)$ est t par p^t) ; on a $M_n = \bigcup_{t \geqslant 0} A_{n,t}$ et $A_{n,t} \cap \Phi_\infty = \Phi_{n+t}$; en consé-

quence, si t_1 et t_2 sont deux entiers tels que $t_1 \geqslant t_2 \geqslant 0$, la restriction des automorphismes de A_{n,t_1} à A_{n,t_2} induit une surjection de $Gal(A_{n,t_1}/\Phi_{n+t_1})$ sur $Gal(A_{n,t_2}/\Phi_{n+t_2})$. Pour ces surjections le système des $Gal(A_{n,t}/\Phi_{n+t})$ est un système projectif dont la limite est isomorphe à $Gal(M_n/\Phi_\infty) = \mathfrak{X}_n$. D'autre part, $A_{n,t}$ est une extension finie de Φ_n et l'application de réciprocité induit un isomorphisme de $\Phi_n^*/(\Phi_n^*)^{p^t}$ sur $Gal(A_{n,t}/\Phi_n)$. Posons $\Phi'_{n,t} = N_{n+t,n}(\Phi_{n+t}^*)$; l'isomorphisme de réciprocité identifie $\Phi'_{n,t}/(\Phi_n^*)^{p^t}$ à $Gal(A_{n,t}/\Phi_{n+t})$. De plus, si t_1 et t_2 sont deux entiers tels que $t_1 \geqslant t_2 \geqslant 0$, on a $\Phi'_{n,t_1} \subset \Phi'_{n,t_2}$ et $(\Phi_n^*)^{p^{t_1}} \subset (\Phi_n^*)^{p^{t_2}}$ donc on a une flèche de $\Phi'_{n,t_1}/(\Phi_n^*)^{p^{t_1}}$ vers $\Phi'_{n,t_2}/(\Phi_n^*)^{p^{t_2}}$. On sait que celle-ci correspond à travers l'isomorphisme de réciprocité à la restriction des automorphismes de A_{n,t_1} à A_{n,t_2}, donc le système projectif des $\Phi'_{n,t}/(\Phi_n^*)^{p^t}$ pour ces flèches est isomorphe au système projectif des $Gal(A_{n,t}/\Phi_{n+t})$ défini ci-dessus ; en conséquence $\mathfrak{X}_n$ est isomorphe à $\varprojlim(\Phi'_{n,t}/(\Phi_n^*)^{p^t})$. Le sous-groupe $\Phi'_{n,t}$ de Φ_n^* est stable par G_n, donc $\Phi'_{n,t}/(\Phi_n^*)^{p^t}$ est un $\mathbb{Z}_p[G_n]$-module ; de même, le sous-groupe $Gal(A_{n,t}/\Phi_{n+t})$ de $Gal(A_{n,t}/\Phi_n)$ est stable par l'action de G_n (par conjugaison) donc $Gal(A_{n,t}/\Phi_{n+t})$ est un $\mathbb{Z}_p[G_n]$-module ; on vérifie sans difficulté que toutes les flèches que l'on a introduites sont ~~des~~ $\mathbb{Z}_p[G_n]$ linéaires ; il en résulte que que l'isomorphisme entre $\mathfrak{X}_n$ et $\varprojlim(\Phi'_{n,t}/(\Phi_n^*)^{p^t})$ est un isomorphisme de $\mathbb{Z}_p[G_n]$-modules.

2) Introduisons $\Phi'_n = \bigcap_{t \geqslant 0} \Phi'_{n,t}$; un élément x de Φ_n^* est dans Φ'_n si et seulement si on a $(x,\Phi_\infty/\Phi_n) = 1$ en désignant par $(x,\Phi_\infty/\Phi_n)$ l'image par l'application de réciprocité de x dans $Gal(\Phi_\infty/\Phi_n)$. Pour tout entier $t \geqslant 0$, l'inclusion $\Phi'_n \subset \Phi'_{n,t}$ induit une

application de $\Phi'_n/(\Phi'_n)^{p^t}$ vers $\Phi'_{n,t}/(\Phi^*_n)^{p^t}$; nous allons montrer que cette application est un isomorphisme. Montrons d'abord qu'elle est injective, c'est-à-dire que, si $x \in \Phi'_n$ et si $x = y^{p^t}$ avec $y \in \Phi_n$, alors $y \in \Phi'_n$: l'égalité $x = y^{p^t}$ implique $(x, \Phi_\infty/\Phi_n) = (y, \Phi_\infty/\Phi_n)^{p^t}$ donc on a $(y, \Phi_\infty/\Phi_n)^{p^t} = 1$; mais $\mathrm{Gal}(\Phi_\infty/\Phi_n)$ est isomorphe à $\mathbb{Z}_p$ donc est sans torsion ; on a donc $(y, \Phi_\infty/\Phi_n) = 1$ ce qui montre que $y \in \Phi'_n$ qui est le résultat cherché. Pour montrer la surjectivité remarquons tout d'abord que l'application de réciprocité de Φ^*_n vers $\mathrm{Gal}(\Phi_\infty/\Phi_n)$ est surjective : en effet, on sait que l'image de Φ^*_n par cette application est dense dans $\mathrm{Gal}(\Phi_\infty/\Phi_n)$; d'autre part, l'extension Φ_∞/Φ_n étant une p-extension totalement ramifiée, l'image de Φ^*_n coïncide avec l'image de son sous-groupe compact U_n ; cette image est donc compacte et donc est $\mathrm{Gal}(\Phi_\infty/\Phi_n)$ tout entier. D'autre part, $\mathrm{Gal}(\Phi_\infty/\Phi_n)$ étant isomorphe à $\mathbb{Z}_p$, son sous-groupe d'indice p^t qui est $\mathrm{Gal}(\Phi_\infty/\Phi_{n+t})$ est égal à $(\mathrm{Gal}(\Phi_\infty/\Phi_n))^{p^t}$. Considérons maintenant un élément x de $\Phi'_{n,t}$; pour démontrer la surjectivité de notre application, il faut montrer que $x = uz^{p^t}$ pour un $u \in \Phi'_n$ et un $z \in \Phi^*_n$. L'élément $(x, \Phi_\infty/\Phi_n)$ est dans $\mathrm{Gal}(\Phi_\infty/\Phi_{n+t})$ puisque $x \in \Phi'_{n,t} = N_{n+t,n}(\Phi^*_{n+t})$; comme on vient de le remarquer cela implique que $(x, \Phi_\infty/\Phi_n)$ est dans $(\mathrm{Gal}(\Phi_\infty/\Phi_n))^{p^t}$ i.e. $(x, \Phi_\infty/\Phi_n) = \sigma^{p^t}$ pour un $\sigma \in \mathrm{Gal}(\Phi_\infty/\Phi_n)$. On a vu ci-dessus que $\sigma = (z, \Phi_\infty/\Phi_n)$ pour un $z \in \Phi^*_n$; posons $u = xz^{-p^t}$. On a $(u, \Phi_\infty/\Phi_n) = (x, \Phi_\infty/\Phi_n)(z, \Phi_\infty/\Phi_n)^{-p^t} = 1$ donc $u \in \Phi'_n$; on a donc $x = uz^{p^t}$ avec $u \in \Phi'_n$ et $z \in \Phi^*_n$, c'est ce qu'on cherchait. Le groupe Φ'_n est stable par l'action de $G_n = \mathrm{Gal}(\Phi_n/\mathbb{Q}_p)$ donc $\Phi'_n/(\Phi'_n)^{p^t}$ est un $\mathbb{Z}_p[G_n]$-module ; il est clair que l'isomorphisme de $\Phi'_n/(\Phi'_n)^{p^t}$ sur $\Phi'_{n,t}/(\Phi^*_n)^{p^t}$ que l'on vient de décrire est un isomorphisme de $\mathbb{Z}_p[G_n]$-module.

3) En juxtaposant les résultats de 1) et 2) on voit que $\mathfrak{X}_n$ est isomorphe en tant que $\mathbb{Z}_p[G_n]$-module à $\varprojlim(\Phi'_n/(\Phi'_n)^{p^t})$. En conséquence (définition 3.3), pour tout $i=1,\dots,p-1$, le $\mathbb{Z}_p[\Gamma/\Gamma_n]$-module $\mathfrak{X}_n^{(i)}$ est isomorphe au $\mathbb{Z}_p[\Gamma/\Gamma_n]$-module $\left[\varprojlim(\Phi'_n/(\Phi'_n)^{p^t})\right]^{(i)} = \varprojlim\left[(\Phi'_n/(\Phi'_n)^{p^t})^{(i)}\right]$. Notons $\mathrm{ord}_{\underline{\underline{p}}_n}$ la valuation de Φ_n dont l'image est $\mathbb{Z}$ et posons $U'_n = U_n \cap \Phi'_n$. La restriction de $\mathrm{ord}_{\underline{\underline{p}}_n}$ à Φ'_n est un homomorphisme de groupe de Φ'_n vers $\mathbb{Z}$ dont le noyau est le groupe V'_n engendré par U'_n et par μ_{p-1} ; en remarquant que, pour tout entier $t \geqslant 0$, on a $V'_n/(V'_n)^{p^t} = U'_n/(U'_n)^{p^t}$ on en déduit une suite exacte $0 \to U'_n/(U'_n)^{p^t} \to \Phi'_n/(\Phi'_n)^{p^t} \to \mathbb{Z}/p^t\mathbb{Z}$; le groupe U'_n est stable par l'action de G_n donc $U'_n/(U'_n)^{p^t}$ est un $\mathbb{Z}_p[G_n]$-module ; on définit aussi une structure de $\mathbb{Z}_p[G_n]$-module sur $\mathbb{Z}/p^t\mathbb{Z}$ en faisant agir G_n trivialement ; on vérifie sans difficulté que notre suite exacte est une suite exacte de $\mathbb{Z}_p[G_n]$-module. Pour chaque $i=1,\dots,p-1$ on a donc une suite exacte $0 \to \left[U'_n/(U'_n)^{p^t}\right]^{(i)} \to \left[\Phi'_n/(\Phi'_n)^{p^t}\right]^{(i)} \to (\mathbb{Z}/p^t\mathbb{Z})^{(i)}$ de $\mathbb{Z}_p[\Gamma/\Gamma_n]$-module ; comme $(\mathbb{Z}/p^t\mathbb{Z})^{(i)} = 0$ pour $i \neq p-1$, les $\mathbb{Z}_p[\Gamma/\Gamma_n]$-modules $[U'_n/(U'_n)^{p^t}]^{(i)}$ et $[\Phi'_n/(\Phi'_n)^{p^t}]^{(i)}$ sont isomorphes si $i \neq p-1$. En passant à la limite projective, on en déduit que le $\mathbb{Z}_p[\Gamma/\Gamma_n]$-module $\mathfrak{X}_n^{(i)}$ est isomorphe au $\mathbb{Z}_p[\Gamma/\Gamma_n]$-module $\varprojlim\left[(U'_n/(U'_n)^{p^t})\right]^{(i)}$. Mais U'_n est un sous-groupe fermé de U_n donc est un groupe compact et les $(U'_n)^{p^t}$ sont une famille filtrante décroissante de sous-groupes fermés dont l'intersection est nulle donc le lemme 3.6 montre que $\varprojlim(U'_n/(U'_n)^{p^t}) = U'_n$; il en résulte que, pour $i \neq p-1$, les $\mathbb{Z}_p[\Gamma/\Gamma_n]$-modules $(U'_n)^{(i)}$ et $\mathfrak{X}_n^{(i)}$ sont isomorphes.

4) Compte tenu de ce qui a été démontré en 3) il suffit, pour achever notre démonstration, de voir que les $\mathbb{Z}_p[\Gamma/\Gamma_n]$-modules $(U'_n)^{(i)}$ et $U_n^{(i)}$ sont isomorphes si $i \neq p-1$. Pour cela, notons, pour tout $k \geqslant 0$, par N_k la norme de Φ_k sur $\mathbb{Q}_p$; remarquons tout d'abord que Φ'_n est l'ensemble des éléments de Φ_n^* dont l'image par N_n est dans le sous-groupe de $\mathbb{Q}_p^*$ engendré par p : en effet, un élément x de Φ_n^* est dans Φ'_n si et seulement si $N_n(x)$ est, pour tout $k \geqslant 0$ dans $N_k(\Phi_k^*)$; mais $N_k(\Phi_k^*)$ est un sous-groupe de $\mathbb{Q}_p^*$ d'indice $(p-1)p^k$ qui contient $1+p^{k+1}\mathbb{Z}_p$ puisque le conducteur de Φ_k est p^{k+1} ; de plus $N_k(\Phi_k^*)$ contient p puisque $N_k(1-\zeta_k) = p$ si ζ_k est une racine de l'unité d'ordre p^{k+1} ; le sous-groupe de $\mathbb{Q}_p^*$ engendré par p et par $1+p^{k+1}\mathbb{Z}_p$ étant d'indice $(p-1)p^k$, c'est le groupe $N_k(\Phi_k^*)$; en conséquence un élément de $\mathbb{Q}_p^*$ est dans tous les $N_k(\Phi_k^*)$ si et seulement si il est dans le groupe engendré par p et notre assertion est prouvée. Les éléments de $U'_n = U_n \cap \Phi'_n$ sont donc les éléments de U_n dont l'image par N_n est 1, c'est-à-dire que l'on a une suite exacte $0 \to U'_n \to U_n \xrightarrow{N_n} 1+p\mathbb{Z}_p$. On munit $1+p\mathbb{Z}_p$ d'une structure de $\mathbb{Z}_p[G_n]$-module en faisant agir G_n trivialement ; il est alors clair que notre suite exacte est une suite exacte de $\mathbb{Z}_p[G_n]$-module ; on en déduit donc pour chaque $i = 1,\dots,p-1$ une suite exacte $0 \to (U'_n)^{(i)} \to U_n^{(i)} \to (1+p\mathbb{Z}_p)^{(i)}$; on conclut alors en remarquant que $(1+p\mathbb{Z}_p)^{(i)}$ est réduit à l'élément neutre si $i \neq p-1$.

Pour tout couple (m,n) d'entiers tel que $m \geqslant n \geqslant 0$, le corps M_m contient le corps M_n donc la restriction des automorphismes de M_m à M_n induit une surjection de $\mathfrak{X}_m = \mathrm{Gal}(M_m/\Phi_\infty)$ sur $\mathfrak{X}_n = \mathrm{Gal}(M_n/\Phi_\infty)$. Ces surjections sont clairement compatibles avec les structures de $\mathbb{Z}_p[G_m]$ et $\mathbb{Z}_p[G_n]$-module de $\mathfrak{X}_m$ et $\mathfrak{X}_n$ donc elles induisent pour chaque $i = 1,\dots,p-1$ des surjections de $\mathfrak{X}_m^{(i)}$ sur

$\mathfrak{X}_n^{(i)}$. Pour $i \neq p-1$, notons $\psi_n^{(i)}$ l'isomorphisme de $\mathbb{Z}_p[\Gamma/\Gamma_n]$-module de $\mathfrak{X}_n^{(i)}$ sur $U_n^{(i)}$ construit dans la démonstration de la proposition 4.1. En reprenant les quatre étapes de cette démonstration on vérifie le corollaire suivant :

COROLLAIRE 4.2. _Pour_ $i \neq p-1$, _la famille des isomorphismes_ $\psi_n^{(i)}$ _définis ci-dessus est un isomorphisme du système projectif des_ $\mathfrak{X}_n^{(i)}$ _pour les flèches induites par les restrictions des automorphismes sur le système projectif des_ $U_n^{(i)}$ _pour les flèches induites par la norme_.

Ce corollaire permet de remplacer l'étude de $\varprojlim(U_n^{(i)})$ qui nous intéresse par celle de $\varprojlim(\mathfrak{X}_n^{(i)})$. Posons $M_\infty = \bigcup_{n\geq 0} M_n$ et $\mathfrak{X} = \varprojlim(\mathfrak{X}_n)$ de sorte que $\mathfrak{X}$ s'identifie à $Gal(M_\infty/\Phi_\infty)$. Chaque M_n étant galoisien sur $\mathbb{Q}_p$, il en est de même de M_∞ et donc $G_\infty = Gal(\Phi_\infty/\mathbb{Q}_p)$ agit par conjugaison sur $\mathfrak{X}$; le sous-groupe Δ de G_∞ agit donc sur $\mathfrak{X}$ ce qui permet de munir $\mathfrak{X}$ d'une structure de $\mathbb{Z}_p[\Delta]$-module ; en tant que tel il se décompose canoniquement en $\mathfrak{X} = \prod_{i=1}^{p-1} \mathfrak{X}^{(i)}$ où $\mathfrak{X}^{(i)}$ est l'ensemble des éléments de $\mathfrak{X}$ invariants par $e_i = \frac{1}{p-1} \sum_{\tau\in\Delta} \chi^i(\tau^{-1})\tau$. Il est clair que $\mathfrak{X}^{(i)}$ est isomorphe à $\varprojlim(\mathfrak{X}_n^{(i)})$. D'autre part, chaque $\mathfrak{X}_n$ étant un $\mathbb{Z}_p[\Gamma/\Gamma_n]$-module topologique et les flèches du système projectif des $\mathfrak{X}_n$ étant continues et compatibles avec les structures de $\mathbb{Z}_p[\Gamma/\Gamma_n]$-module, la limite projective $\mathfrak{X}$ est munie d'une structure de $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$-module topologique donc (proposition 3.4) de Λ-module topologique. La proposition suivante sera fondamentale dans la suite :

PROPOSITION 4.3. _On considère_ $\mathfrak{X}$ _muni de sa structure de_ Λ-_module ; la projection de_ $\mathfrak{X}$ _sur_ $\mathfrak{X}_n$ _est surjective et son noyau est_ $\omega_n(T)$, _c'est-à-dire que l'on a une suite exacte_

$$0 \to \omega_n(T)\mathfrak{X} \to \mathfrak{X} \to \mathfrak{X}_n \to 0 .$$

Avant de démontrer cette proposition, tirons-en le corollaire qui nous intéressera dans la suite :

COROLLAIRE 4.4. *Si* $i \neq p-1$, *la projection du* Λ*-module* $U^{(i)}$ *sur* $U_n^{(i)}$ *est surjective et son noyau est* $\omega_n(T)U^{(i)}$; *le quotient* $U^{(i)}/(\omega_n(T)U^{(i)})$ *est donc isomorphe à* $U_n^{(i)}$.

Démonstration. De la suite exacte $0 \to \omega_n(T)\mathfrak{X} \to \mathfrak{X} \to \mathfrak{X}_n \to 0$ on tire, pour chaque $i=1,\dots,p-1$, une suite exacte $0 \to \omega_n(T)\mathfrak{X}^{(i)} \to \mathfrak{X}^{(i)} \to \mathfrak{X}_n^{(i)} \to 0$; notre corollaire résulte donc du corollaire 4.2.

Démontrons la proposition 4.3. Pour cela choisissons un générateur γ de Γ et identifions (proposition 3.4) $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$ et Λ par l'isomorphisme qui envoie γ sur $1+T$; dans cette identification $\gamma^{p^n}-1$ correspond à $\omega_n(T) = (1+T)^{p^n}-1$. Identifions aussi $\mathfrak{X}$ et $Gal(M_\infty/\Phi_\infty)$; la projection de $\mathfrak{X}$ sur $\mathfrak{X}_n$ est alors la restriction des automorphismes de M_∞ à M_n , elle est donc surjective et son noyau est $Gal(M_\infty/M_n)$. En conséquence, la première assertion de notre proposition est démontrée et la seconde est équivalence à l'égalité $Gal(M_\infty/M_n) = (\gamma^{p^n}-1)Gal(M_\infty/\Phi_\infty)$. Pour démontrer cette égalité commençons par montrer l'inclusion $(\gamma^{p^n}-1)Gal(M_\infty/\Phi_\infty) \subset Gal(M_\infty/M_n)$: le corps M_n étant le plus grand sous-corps de M_∞ abélien sur Φ_n (puisque, par définition, M_n est la p-extension abélienne maximale de Φ_n), le groupe $Gal(M_\infty/M_n)$ est l'adhérence du groupe des commutateurs de $Gal(M_\infty/\Phi_n)$; mais γ^{p^n} est dans $Gal(\Phi_\infty/\Phi_n)$, donc $(\gamma^{p^n}-1)Gal(M_\infty/\Phi_\infty)$ est inclus dans le groupe des commutateurs de $Gal(M_\infty/\Phi_n)$ et notre inclusion est démontrée. Pour achever la démonstration il ne reste plus qu'à voir l'inclusion inverse, soit $Gal(M_\infty/M_n) \subset (\gamma^{p^n}-1)Gal(M_\infty/\Phi_\infty)$. Pour cela remarquons que $(\gamma^{p^n}-1)Gal(M_\infty/\Phi_\infty)$ est l'image du compact $Gal(M_\infty/\Phi_\infty)$ par la multiplication par $\gamma^{p^n}-1$ qui est continue ; en conséquence

$(\gamma^{p^n}-1)\mathrm{Gal}(M_\infty/\Phi_\infty)$ est un groupe fermé et, si M'_n désigne le sous-corps de M_∞ fixé par $(\gamma^{p^n}-1)\mathrm{Gal}(M_\infty/\Phi_\infty)$, l'inclusion entre groupes que nous voulons démontrer est équivalente à l'inclusion entre corps $M'_n \subset M_n$. Enfin, par définition de M_n, il suffit pour montrer cette dernière inclusion de montrer que le corps M'_n est abélien sur Φ_n. Le groupe $(\gamma^{p^n}-1)\mathrm{Gal}(M_\infty/\Phi_\infty)$ est clairement distingué dans $\mathrm{Gal}(M_\infty/\Phi_n)$, donc M'_n est galoisien sur Φ_n ; pour voir qu'il est abélien il suffit de voir que toute extension galoisienne finie de Φ_n inclue dans M'_n est abélienne sur Φ_n. Soit donc F une extension galoisienne finie de Φ_n contenue dans M'_n ; posons $E = F \cap \Phi_\infty$. Le sous-groupe $\mathrm{Gal}(F/E)$ s'identifie à $\mathrm{Gal}(F\Phi_\infty/\Phi_\infty)$ qui est abélien (puisque $F\Phi_\infty$ est inclus dans M_∞ qui est abélien sur Φ_∞), donc $\mathrm{Gal}(F/E)$ est abélien. D'autre part $\mathrm{Gal}(E/\Phi_n)$ est cyclique et engendré par la restriction de γ^{p^n} à E ; le corps F étant inclus dans M'_n, l'action par conjugaison de γ^{p^n} sur $\mathrm{Gal}(F/E)$ est triviale ; on en déduit facilement que $\mathrm{Gal}(F/\Phi_n)$ est abélien, ce qu'on voulait.

Rappelons le résultat suivant dont nous aurons besoin plus loin :

LEMME 4.5. <u>Soit</u> $n \geqslant 0$ <u>un entier ; si</u> $i \neq 1$ <u>le</u> $\mathbb{Z}_p$<u>-module</u> $U_n^{(i)}$ <u>est libre de dimension</u> p^n. <u>D'autre part</u> $\mu_{p^{n+1}}$ <u>est inclus dans</u> $U_n^{(1)}$ <u>et</u> $U_n^{(1)}/\mu_{p^{n+1}}$ <u>est un</u> $\mathbb{Z}_p$<u>-module libre de dimension</u> p^n.

<u>Démonstration</u>. On sait que $\mu_{p^{n+1}}$ est le sous-groupe de torsion de U_n ; par définition de χ, il est clair que $\mu_{p^{n+1}}$ est inclus dans $U_n^{(1)}$; en conséquence $U_n^{(1)}/\mu_{p^{n+1}}$ et $U_n^{(i)}$ pour $i \neq 1$ sont des $\mathbb{Z}_p$-modules sans torsion ; U_n étant de type fini sur $\mathbb{Z}_p$, on en déduit que $U_n^{(1)}/\mu_{p^{n+1}}$ et $U_n^{(i)}$ pour $i \neq 1$ sont des $\mathbb{Z}_p$-modules libres de dimension finie. D'autre part on sait ([15] par exemple) qu'il existe un entier x de Φ_n dont les conjugués sont linéaire-

ment indépendants sur $\mathbb{Z}_p$; quitte à multiplier x par une puissance de p, on peut supposer que x est dans le domaine de convergence de l'exponentielle p-adique. Notons alors u l'image de x par l'exponentielle p-adique ; il est clair que le sous-$\mathbb{Z}_p[G_n]$-module de U_n engendré par u est isomorphe à $\mathbb{Z}_p[G_n]$. En conséquence, pour chaque $i = 1,\ldots,p-1$, le $\mathbb{Z}_p$-module $U_n^{(i)}$ contient un sous-module isomorphe au $\mathbb{Z}_p$-module $(\mathbb{Z}_p[G_n])^{(i)}$. Mais $(\mathbb{Z}_p[G_n])^{(i)}$ est le $\mathbb{Z}_p$-module engendré par les $(e_i.\sigma)_{\sigma\in\Gamma/\Gamma_n}$ et ces p^n générateurs sont libres sur $\mathbb{Z}_p$, donc chaque $U_n^{(i)}$ contient un $\mathbb{Z}_p$-module libre de dimension p^n. Il en résulte que les dimensions de $U_n^{(1)}/\mu_{p^{n+1}}$ et des $U_n^{(i)}$ pour $i \neq 1$ sont supérieures ou égales à p^n. Si l'une de ces dimensions était strictement plus grande que p^n, alors la dimension du $\mathbb{Z}_p$-module libre $U_n/\mu_{p^{n+1}}$ serait strictement plus grande que $(p-1)p^n$. On sait que la dimension sur $\mathbb{Z}_p$ de $U_n/\mu_{p^{n+1}}$ est le degré de $\Phi_n/\mathbb{Q}_p$; celui-ci est $(p-1)p^n$ et donc notre lemme est démontré.

Nous pouvons maintenant démontrer le théorème suivant :

THEOREME 4.6. <u>Si</u> $i \neq 1$, $p-1$ <u>alors le</u> Λ-<u>module</u> $U^{(i)}$ <u>est isomorphe à</u> Λ.

<u>Démonstration</u>. Pour tout i, on a $U^{(i)}/(\mathfrak{m}U^{(i)}) = U^{(i)}/(p,T)U^{(i)}$ puisque $\mathfrak{m} = (p,T)$. Mais $\omega_o(T) = T$, donc le corollaire 4.4 montre que $U^{(i)}/TU^{(i)} = U_o^{(i)}$ si $i \neq p-1$; dans ce cas on a donc $U^{(i)}/\mathfrak{m}U^{(i)} = U_o^{(i)}/(U_o^{(i)})^p$. Le quotient $U_o^{(i)}/(U_o^{(i)})^p$ est un $\Lambda/\mathfrak{m} = \mathbb{F}_p$-espace vectoriel de dimension finie et $U^{(i)}$ est compact (puisque $U^{(i)}$ est une limite projective de compact) donc, si $i \neq p-1$, le lemme 3.14 montre que $U^{(i)}$ est un Λ-module de type fini. La proposition 3.13 montre qu'alors $U^{(i)}$ s'insère dans une suite exacte de Λ-modules

(1) $$0 \to C \to U^{(i)} \to N \to D \to 0$$

dans laquelle C et D sont deux Λ-modules finis et N est un Λ-module de la forme $\Lambda^r \oplus \left[\bigoplus_{i=1}^{k} (\Lambda/p^{n_i}\Lambda)\right] \oplus \left[\bigoplus_{j=1}^{\ell} (\Lambda/f_j\Lambda)\right]$ avec f_j polynôme distingué. Chaque $U_n^{(i)}$ est sans torsion puisque $i \neq 1$, donc $U^{(i)}$ est sans torsion donc $C = 0$ et (1) devient

(2) $$0 \to U^{(i)} \to N \to D \to 0 .$$

Le Λ-module D étant un Λ-module topologique, on a $\mathfrak{m}^n D = 0$ pour n assez grand ; comme $\omega_n = (1+T)^{p^n} - 1$ est inclus dans $\mathfrak{m}^{n+1}$, on a $\omega_n D = 0$ pour n assez grand. Notons Y_n le noyau de la multiplication par ω_n sur N ; dès que n est assez grand pour que $\omega_n D = 0$, on a le diagramme suivant :

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & & Y_n \arrow[d] & D \arrow[d] & \\
0 \arrow[r] & U^{(i)} \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & D \arrow[r] \arrow[d, "\omega_n"] & 0 \\
0 \arrow[r] & U^{(i)} \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & D \arrow[r] \arrow[d] & 0 \\
 & U^{(i)}/\omega_n U^{(i)} \arrow[d] & N/\omega_n N \arrow[d] & D \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

dans lequel les lignes et les colonnes sont exactes. Le lemme du serpent permet d'en déduire une suite exacte $Y_n \to D \to U^{(i)}/\omega_n U^{(i)} \to N/\omega_n N \to D \to 0$. Par hypothèse $i \neq p-1$, donc (corollaire 4.4) le quotient $U^{(i)}/\omega_n U^{(i)}$ est isomorphe à $U_n^{(i)}$; comme $i \neq 1$, celui-ci est sans torsion, donc la flèche de D dans $U_n^{(i)}$ est la flèche 0 ; notre suite exacte donne donc les deux suites exactes suivantes :

(3) $$0 \to U_n^{(i)} \to N/\omega_n N \to D \to 0$$

(4) $$Y_n \to D \to 0 .$$

Nous allons maintenant montrer que $N = \Lambda$, c'est-à-dire que $r = 1$, $k = 0$ et $\ell = 0$. Commençons par $k = 0$ et raisonnons par l'absurde : si $k \neq 0$, le quotient $N/\omega_n N$ contient des facteurs du type $\Lambda/(p^{n_i}, \omega_n)\Lambda$ avec $n_i \neq 0$; la proposition 3.5 montre que $\Lambda/\omega_n\Lambda$ est isomorphe à $\mathbb{Z}_p[T]/\omega_n\mathbb{Z}_p[T]$ donc que $\Lambda/\omega_n\Lambda$ est un $\mathbb{Z}_p$-module libre de rang p^n ; le quotient $\Lambda/(p^{n_i}, \omega_n)\Lambda$ est donc fini et son cardinal est $p^n p^{n_i}$; on en déduit que, lorsque n tend vers l'infini, le cardinal du sous-groupe de torsion de $N/\omega_n N$ tend vers l'infini ; dans la suite exacte (3) la surjection de $N/\omega_n N$ sur D a pour noyau $U_n^{(i)}$ qui est sans torsion puisque $i \neq 1$; la restriction de cette surjection au sous-groupe de torsion de $N/\omega_n N$ est donc injective ce qui implique que le cardinal de ce groupe de torsion est majoré par le cardinal de D ; cela contredit le fait que ce cardinal tend vers l'infini avec n et donc prouve que $k = 0$.

Montrons maintenant que $r = 1$. Compte-tenu de ce que l'on vient de voir, on a $N = \Lambda^r \oplus \left[\bigoplus_{j=1}^{\ell} (\Lambda/f_j\Lambda)\right]$; on a donc $N/\omega_n N =$ $(\Lambda/\omega_n\Lambda)^r \oplus \left[\bigoplus_{j=1}^{\ell} \Lambda/(f_j, \omega_n)\Lambda\right]$. Les polynômes ω_n et f_j étant distingués on déduit de la proposition 3.5 que $\Lambda/\omega_n\Lambda$ et $\Lambda/f_j\Lambda$ sont respectivement des $\mathbb{Z}_p$-modules libres de rang p^n et d_j si d_j désigne le degré de f_j . Le $\mathbb{Z}_p$-rang de $(\Lambda/\omega_n\Lambda)^r$ est donc rp^n tandis que le $\mathbb{Z}_p$-rang de $\bigoplus_{j=1}^{k} (\Lambda/(f_j, \omega_n)\Lambda)$ est plus petit ou égal à $d = \sum_{j=1}^{k} d_j$. D'autre part la suite exacte (3) montre que le $\mathbb{Z}_p$-rang de $N/\omega_n N$ est égal au $\mathbb{Z}_p$-rang de $U_n^{(i)}$ donc (lemme 4.5) à p^n . En conséquence, dès que n est assez grand, on a $p^n = rp^n + d_n$ où d_n est un entier borné par $d = \sum_{j=1}^{k} d_j$; en faisant tendre n vers l'infini, on en tire $r = 1$ ce qu'on voulait.

Montrons enfin que $\ell = 0$. Compte-tenu de ce qu'on vient de voir, on a $N = \Lambda \oplus \left[\bigoplus_{j=1}^{\ell} (\Lambda/f_j\Lambda) \right]$; on a donc $N/\omega_n N = \Lambda/\omega_n\Lambda \oplus \left[\bigoplus_{j=1}^{\ell} (\Lambda/(f_j,\omega_n)\Lambda) \right]$. Comme on l'a vu en démontrant que $r = 1$, les $\mathbb{Z}_p$-rangs de $N/\omega_n N$ et $\Lambda/\omega_n\Lambda$ sont tous les deux égaux à p^n ; le $\mathbb{Z}_p$-rang de chaque $\Lambda/(f_j,\omega_n)\Lambda$ est donc nul, ce qui implique que chaque $\Lambda/(f_j,\omega_n)\Lambda$ est fini. Mais on a vu (en démontrant que $k = 0$) que le cardinal du sous-groupe de torsion de $N/\omega_n N$ est majoré par le cardinal de D , donc l'assertion $\ell = 0$ résulte du lemme suivant :

LEMME 4.7. <u>Soit</u> f <u>un polynôme distingué tel que le quotient</u> $\Lambda/(f,\omega_n)\Lambda$ <u>est fini dès que</u> n <u>est assez grand</u>. <u>Si le cardinal du quotient</u> $\Lambda/(f,\omega_n)\Lambda$ <u>reste borné lorsque</u> n <u>tend vers l'infini</u>, <u>alors</u> $f = 1$.

Avant de démontrer ce lemme, montrons comment on achève la démonstration du théorème 4.6. On sait maintenant que $N = \Lambda$; le noyau Y_n de la multiplication par ω_n sur N est donc 0 ; la suite exacte (4) montre alors que $D = 0$ et la suite exacte (2) que $U^{(i)}$ est isomorphe à $N = \Lambda$, c'est l'assertion du théorème.

Démontrons le lemme 4.7. Notons d le degré de f et choisissons un entier n_o tel que $p^{n_o} \geqslant d$; les polynômes ω_n et f étant distingués, la différence $\omega_{n_o} - T^{(p^{n_o}-d)}f$ est divisible par p et donc ω_{n_o} est dans l'idéal $(f,p)\Lambda$ engendré par f et p . Posons $\alpha = 1+T$; pour tout n , on a $\omega_{n+1} = \omega_n\left(\sum_{i=0}^{p-1} \alpha^{ip^n}\right)$ et, pour chaque $i = 1,\dots,p-1$, on a $\alpha^{ip^n} \equiv 1+T^{ip^n}$ modulo $p\Lambda$; si $n \geqslant n_o$, alors T^{ip^n} appartient à l'idéal $(f,p)\Lambda$ et donc α^{ip^n} est congru à 1 modulo $(f,p)\Lambda$. En conséquence, si $n \geqslant n_o$, la somme $\sum_{i=0}^{p-1} \alpha^{ip^n}$ est contenue dans l'idéal $(f,p)\Lambda$; cela montre, par récurrence sur n , que ω_n est dans l'idéal $(f,p^{n-n_o+1})\Lambda$. En conséquence le cardinal de $\Lambda/(f,\omega_n)\Lambda$ est supérieur ou égal au cardinal de $\Lambda/(f,p^{n-n_o+1})\Lambda$;

ce dernier est égal à dp^{n-n_o+1} puisque $\Lambda/f\Lambda$ est un $\mathbb{Z}_p$-module libre de dimension d (proposition 3.5) ; l'hypothèse de notre lemme implique donc que dp^{n-n_o+1} reste borné lorsque n tend vers l'infini ; cela impose $d=0$ donc $f=1$. C.Q.F.D.

Choisissons maintenant pour chaque $n \in \mathbb{N}$ une racine de l'unité ζ_n d'ordre p^{n+1} de telle sorte que $\zeta_{n+1}^p = \zeta_n$ pour tout $n \in \mathbb{N}$; nous posons $\pi_n = \zeta_n - 1$ et donnons la définition suivante :

DEFINITION 4.8. <u>Un élément</u> $u = (u_n)_{n\in\mathbb{N}}$ <u>de</u> $U = \varprojlim(U_n)$ <u>est dit admissible si il existe une série</u> $f(T) \in \mathbb{Z}_p[[T]]$ <u>telle que</u> $u_n = f(\pi_n)$ <u>pour tout</u> $n \in \mathbb{N}$. <u>Nous notons</u> $\mathfrak{a}$ <u>le sous-ensemble de</u> U <u>formé des éléments admissibles</u>.

Nous allons montrer que, si $i \neq 1, p-1$, alors tous les éléments de $U^{(i)}$ sont admissibles i.e. $U^{(i)} \subset \mathfrak{a}$ (en fait on sait que $\mathfrak{a} = U$ mais nous n'aurons pas besoin de ce résultat pour ce que nous avons en vue qui est la démonstration du théorème 3.7). Nous aurons besoin tout d'abord d'étudier U_o . Pour chaque $k=1,\dots,p-1$ définissons l'application ψ_k de U_o dans $\mathbb{Z}/p\mathbb{Z}$ de la manière suivante : chaque $u_o \in U_o$ s'écrit de manière unique $u_o = \sum_{j=0}^{\infty} c_j \pi_o^j$ avec $c_j \in \{1,\dots,p-1\}$; notons $f_{u_o}(T)$ la série $\sum_{j=0}^{\infty} c_j T^j$ et D l'opérateur $(1+T)\frac{d}{dT}$; la série $f_{u_o}(T)$ est inversible dans $\mathbb{Z}[[T]]$ puisque $c_o = 1$ pour tout u_o , donc $\frac{Df_{u_o}}{f_{u_o}}(T)$ est dans $\mathbb{Z}[[T]]$; pour chaque $k=1,\dots,p-1$ la série $D^{k-1}\frac{Df_{u_o}}{f_{u_o}}(T)$ est donc aussi dans $\mathbb{Z}[[T]]$ et nous définissons $\psi_k(u_o)$ comme la classe dans $\mathbb{Z}/p\mathbb{Z}$ de l'entier $\left[D^k \frac{Df_{u_o}}{f_{u_o}}\right](0)$. On a alors :

PROPOSITION 4.9. <u>Pour tout</u> $k=1,\dots,p-1$ <u>on a</u> :

1) ψ_k <u>est un homomorphisme du groupe</u> U_o <u>vers le groupe</u> $\mathbb{Z}/p\mathbb{Z}$.

2) <u>Soient</u> $\tau\in\Delta$ <u>et</u> $\widetilde{\chi(\tau)}$ <u>la classe de</u> $\chi(\tau)$ <u>dans</u> $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$; <u>on a</u> $\psi_k(\tau(u_o)) = \widetilde{\chi(\tau)}^k\psi_k(u_o)$ <u>pour tout</u> $u_o\in U_o$.

<u>Démonstration</u>. 1) Notons ord_p la valuation de Φ_o normalisée par $\mathrm{ord}_p(p)=1$. Soient u_o et v_o dans U_o et $w_o = u_o v_o$; considérons la série $(f_{u_o}f_{v_o}-f_{w_o})(T) = \sum_{i=0}^{\infty} a_i T^i$. On a $a_o=0$ puisque les termes constants de f_{u_o} , f_{v_o} et f_{w_o} sont égaux à 1 ; de plus $(f_{u_o}f_{v_o}-f_{w_o})(\pi_o) = u_o v_o - w_o = 0$ donc $\sum_{i=1}^{\infty} a_i\pi_o^{i-1} = 0$. On en déduit que $\mathrm{ord}_p(\sum_{i=1}^{p-1} a_i\pi_o^{i-1}) = \mathrm{ord}_p(\sum_{i=p}^{\infty} a_i\pi_o^{i-1})$; mais $\mathrm{ord}_p(\pi_o) = \frac{1}{p-1}$ donc, d'une part $\mathrm{ord}_p(\sum_{i=p}^{\infty} a_i\pi_o^{i-1}) \geqslant 1$ et, d'autre part les $\mathrm{ord}_p(a_i\pi_o^{i-1})$ pour $i=1,\dots,p-1$ sont distincts deux à deux. Pour chaque $i=1,\dots,p-1$, on a donc $\mathrm{ord}_p(a_i\pi_o^{i-1})\geqslant 1$ ce qui implique que p divise a_i pour chacun de ces i . On en déduit que, pour $k=1,\dots,p-1$, les entiers $\left[D^{k-1}\dfrac{D(f_{u_o}f_{v_o})}{(f_{u_o}f_{v_o})}\right](0)$ et $\left[D^{k-1}\dfrac{Df_{w_o}}{f_{w_o}}\right](0)$ sont congrus modulo p et notre assertion résulte alors de l'égalité

$$\frac{D(f_{u_o}f_{v_o})}{(f_{u_o}f_{v_o})}(T) = \frac{Df_{u_o}}{f_{u_o}}(T) + \frac{Df_{v_o}}{f_{v_o}}(T).$$

2) Soit $a(\tau)$ un entier congru à $\chi(\tau)$ modulo $p\mathbb{Z}_p$. Comme dans la démonstration du point 1), on vérifie que les p premiers coefficients de la série $f_{\tau(u_o)}(T) - f_{u_o}((1+T)^{a(\tau)}-1)$ sont divisibles par p ; en conséquence les entiers $\left[D^{k-1}\dfrac{Df_{\tau(u_o)}}{f_{\tau(u_o)}}\right](0)$ et

$$D^{k-1}\left.\frac{Df_{u_o}((1+T)^{a(\tau)}-1)}{f_{u_o}((1+T)^{a(\tau)}-1)}\right|_{T=0}$$

sont congrus modulo p . Notre assertion résulte alors du lemme général suivant :

LEMME 4.10. <u>Soient</u> $f(T)$ <u>une série inversible de</u> $\mathbb{Z}_p[[T]]$ <u>et</u> x <u>un élément de</u> $\mathbb{Z}_p$. <u>Si</u> $g(T)$ <u>est la série</u> $f((1+T)^x-1)$, <u>alors on a</u> $D^{k-1}\frac{Dg}{g}(T) = x^k \frac{Df}{f}((1+T)^x-1)$.

<u>Démonstration</u>. Montrons tout d'abord le résultat suivant : soient $h(T) \in \mathbb{Z}_p[[T]]$ et $x \in \mathbb{Z}_p$; si $j(T) = h((1+T)^x-1)$ on a $Dj(T) = x(Dh)((1+T)^x-1)$. En effet $Dj(T) = (1+T)\frac{d}{dT}j(T) = (1+T)\left[x(1+T)^{x-1}(\frac{d}{dT}h)((1+T)^x-1)\right] = x[1+((1+T)^x-1)](\frac{d}{dT}h)((1+T)^x-1) = x(Dh)((1+T)^x-1)$. En appliquant cette identité avec $h=f$, il vient $Dg(T) = x(Df)((1+T)^x-1)$ et donc $\frac{Dg}{g}(T) = x\frac{Df}{f}((1+T)^x-1)$. On obtient alors le lemme en réappliquant notre identité successivement avec $h = \frac{Df}{f},\ldots,h = D^{k-2}\frac{Df}{f}$.

La proposition 4.9 admet le corollaire suivant :

COROLLAIRE 4.11. <u>Pour tout</u> $k=1,\ldots,p-1$ <u>on a</u> :

1) <u>Si</u> $x \in \mathbb{Z}_p$ <u>et si</u> $\tilde{x}$ <u>est la classe de</u> x <u>dans</u> $\mathbb{Z}_p/p\mathbb{Z}_p$, <u>alors</u> $\psi_k(u_o^x) = \tilde{x}\psi_k(u_o)$ <u>pour tout</u> $u_o \in U_o$.

2) <u>La restriction de</u> ψ_k <u>à</u> $U_o^{(i)}$ <u>est nulle si</u> $i \neq k$.

3) <u>Si</u> $u_o \in U_o$ <u>et si</u> $u_o = \prod_{i=1}^{p-1} u_o^{(i)}$ <u>est la décomposition de</u> u_o <u>dans</u> $U_o = \prod_{i=1}^{p-1} U_o^{(i)}$, <u>on a</u> $\psi_k(u_o) = \psi_k(u_o^{(k)})$.

<u>Démonstration</u>. 1) Notons $\bar{x}$ un élément de $\mathbb{N}$ tel que $\bar{x} \equiv x$ modulo $p\mathbb{Z}_p$ et posons $y = \frac{x-\bar{x}}{p}$; on a $\psi_k(u_o^x) = \psi_k(u_o^{\bar{x}}.(u_o^y)^p) = \bar{x}\psi_k(u_o) + p\psi_k(u_o^y)$ puisque ψ_k est un homomorphisme de groupe. Mais $\bar{x}\psi_k(u_o) = \tilde{x}\psi_k(u_o)$ et $p\psi_k(u_o) = 0$, donc notre assertion est démontrée.

2) Si $u_o \in U_o^{(i)}$ on a $\tau(u_o) = u_o^{\chi^i(\tau)}$ pour tout $\tau \in \Delta$; le 1) de ce corollaire montre donc que $\psi_k(\tau(u_o)) = \widetilde{\chi(\tau)}^i\,\psi_k(u_o)$. D'autre part, le 2) de la proposition 4.9 montre que $\psi_k(\tau(u_o)) = \widetilde{\chi(\tau)}^k\,\psi_k(u_o)$. On a donc $(\widetilde{\chi(\tau)}^i - \widetilde{\chi(\tau)}^k)\psi_k(u_o) = 0$ et on conclut en remarquant que $\widetilde{\chi(\tau)}^i \neq \widetilde{\chi(\tau)}^k$ si $\tau \neq 1$ et $k \neq i$.

3) Résulte de 2) et du fait que ψ_k est un homomorphisme de groupe.

Revenons maintenant à $U = \varprojlim U_n$; on a :

PROPOSITION 4.12. Soient $k \neq 1, p-1$ et $w = (w_n)_{n \in \mathbb{N}}$ un élément de U. Si $\psi_k(w_o) \neq 0$, alors $w^{(k)}$ est une base du Λ-module $U^{(k)}$.

Démonstration. Puisque $k \neq 1, p-1$, le théorème 4.6 montre que le Λ-module $U^{(k)}$ est isomorphe à Λ ; pour montrer que $w^{(k)}$ est une base de $U^{(k)}$, il suffit donc de démontrer que $w^{(k)}$ engendre le Λ-module $U^{(k)}$. Le lemme 3.15 (lemme de Nakayama) montre que $w^{(k)}$ engendre le Λ-module $U^{(k)}$ si sa classe dans $U^{(k)}/\mathfrak{m}U^{(k)}$ engendre ce $\Lambda/\mathfrak{m} = \mathbb{F}_p$-espace vectoriel. Mais, k étant différent de $p-1$, le corollaire 4.4 montre que la projection de $U^{(k)}$ sur $U_o^{(k)}$ induit un isomorphisme de $U^{(k)}/TU^{(k)}$ sur $U_o^{(k)}$; comme $\mathfrak{m} = (p,T)$ on en déduit que la classe de $w^{(k)}$ dans $U^{(k)}/\mathfrak{m}U^{(k)}$ engendre ce $\mathbb{F}_p$-espace vectoriel si et seulement si la classe de $w_o^{(k)}$ dans $U_o^{(k)}/(U_o^{(k)})^p$ engendre ce $\mathbb{F}_p$-espace vectoriel. Si $\psi_k(w_o) \neq 0$, on a $\psi_k(w_o^{(k)}) \neq 0$ d'après le 3) du corollaire 4.11 et donc $w_o^{(k)}$ n'est pas dans $(U_o^{(k)})^p$; puisque $k \neq 1$, il en résulte que la classe de $w_o^{(k)}$ dans $U_o^{(k)}/(U_o^{(k)})^p$ engendre ce $\mathbb{F}_p$-espace vectoriel ce qui termine la démonstration.

Nous pouvons maintenant démontrer la proposition suivante :

PROPOSITION 4.13. Soit λ une racine $p-1^{\underline{\text{ième}}}$ de l'unité de $\mathbb{Z}_p$ qui est différente de 1 ; pour chaque $n \in \mathbb{N}$ nous posons $w_{\lambda,n} = \frac{\lambda-1-\pi_n}{\omega(\lambda-1)}$ où $\omega(\lambda-1)$ est la racine $p-1^{\underline{\text{ième}}}$ de l'unité de $\mathbb{Z}_p$ congrue à $\lambda-1$ modulo $p\mathbb{Z}_p$; on a :

1) $w_\lambda = (w_{\lambda,n})_{n \in \mathbb{N}}$ est dans $\mathfrak{A}$

2) pour chaque $i \neq 1, p-1$, il existe au moins un λ (dépendant de i) tel que $w_{\lambda-1}^{(i)}$ est une base du Λ-module $U^{(i)}$.

Démonstration. 1) Il est clair que $w_{\lambda,n}$ est dans U_n pour tout $n \in \mathbb{N}$. Pour $n \geqslant 1$, le polynôme minimal de $\lambda-1-\pi_n$ sur Φ_{n-1} est

$(X-\lambda)^p+\zeta_{n-1}$ donc $N_{n,n-1}(\lambda-1-\pi_n) = \lambda^p-\zeta_{n-1} = \lambda-1-\pi_{n-1}$; comme d'autre part $N_{n,n-1}(\omega(\lambda-1)) = \omega(\lambda-1)^p = \omega(\lambda-1)$, on a $N_{n,n-1}(w_{\lambda,n}) = w_{\lambda,n-1}$ et donc w_λ est dans $U = \varprojlim U_n$. Enfin, si $f(T) = \frac{\lambda-1-T}{\omega(\lambda-1)}$, on a $w_{\lambda,n} = f(\pi_n)$ pour chaque n ce qui montre que w_λ est dans $\mathfrak{a}$.

2) Soit toujours $f(T) = \frac{\lambda-1-T}{\omega(\lambda-1)}$; on a $f(\pi_o) = w_o$. Un raisonnement analogue à celui fait dans la démonstration du 1) de la proposition 4.9 montre que, pour $i=1,\ldots,p-2$, la classe modulo $p\mathbb{Z}_p$ de $[D^{i-1}\frac{Df}{f}](0)$ est $\psi_i(w_o)$ (le terme constant de f n'étant pas 1 , on ne peut rien dire pour $i=p-1$). On a $\frac{Df}{f}(T) = -\frac{1+T}{\lambda-(1+T)}$; on vérifie facilement que le changement de variable $1+T=e^Z$ transforme l'opérateur D en $\frac{d}{dZ}$ et donc $D^{i-1}\left(-\frac{1+T}{\lambda-(1+T)}\right)\Big|_{T=0} = \frac{d^{i-1}}{dZ^{i-1}}\left(-\frac{e^Z}{\lambda-e^Z}\right)\Big|_{Z=0}$. Par récurrence sur i , on voit que $\frac{d^{i-1}}{dZ^{i-1}}\left(-\frac{e^Z}{\lambda-e^Z}\right)$ est de la forme $\frac{\lambda^{i-1}e^Z+Q(\lambda)}{(\lambda-e^Z)^i}$ où Q est un polynôme à coefficient dans $\mathbb{Z}[e^Z]$ dont le degré est strictement inférieur à $i-1$. En conséquence $\psi_i(w_o)$ est la classe modulo $p\mathbb{Z}_p$ de $\frac{\lambda^{i-1}+q(\lambda)}{(\lambda-1)^i}$ où q est un polynôme à coefficient dans $\mathbb{Z}$ dont le degré est strictement inférieur à $i-1$. Désignons par $\tilde{\lambda}$ la classe de λ modulo $p\mathbb{Z}_p$ et par $\tilde{q}$ le polynôme obtenu en réduisant q modulo $p\mathbb{Z}$, on a $\psi_i(w_o) = \frac{\tilde{\lambda}^{i-1}+\tilde{q}(\lambda)}{(\tilde{\lambda}-1)^i}$. Mais $i \neq p-1$ donc $i-1 \leqslant p-3$ et donc le polynôme $X^{i-1}-\bar{q}(X)$ a au plus $p-3$ racines. Lorsque λ décrit les racines $p-1^{\text{ièmes}}$ de l'unité de $\mathbb{Z}_p$ différentes de 1 , les $\tilde{\lambda}$ prennent $p-2$ valeurs distinctes donc il existe au moins un λ tel que $\psi_i(w_o) \neq 0$. On conclut à l'aide de la proposition 4.12.

Revenons à l'étude de $\mathfrak{a}$; on a :

LEMME 4.14. <u>Soit</u> $u = (u_n)_{n\in\mathbb{N}}$ <u>un élément admissible de</u> $U = \varprojlim U_n$. <u>La série</u> $f(T) \in \mathbb{Z}_p[[T]]$ <u>telle que</u> $f(\pi_n) = u_n$ <u>pour tout</u>

$n \in \mathbb{N}$ <u>est unique ; de plus, son terme constant est congru à</u> 1 <u>modulo</u> $p\mathbb{Z}_p$.

<u>Démonstration</u>. Soient f_1 et f_2 deux séries tels que $f_1(\pi_n) = f_2(\pi_n) = u_n$ pour tout $n \in \mathbb{N}$. Si $g = f_1 - f_2$, on a $g(\pi_n) = 0$ pour tout $n \in \mathbb{N}$; montrons que cela implique $g = 0$ et donc $f_1 = f_2$ ce qui est la première assertion de notre lemme. Supposons $g \neq 0$ et notons p^α la plus grande puissance de p qui divise g ; on a $g = p^\alpha g_1$ avec g_1 non divisible par p ; notons n_o le plus petit entier tel que p ne divise pas le coefficient de T^{n_o} dans g_1 ; la proposition 3.5 montre qu'il existe un polynôme r de degré strictement plus petit que n_o et une série Q tels que $T^{n_o} = Q.g_1 + r$; pour tout n , on a $\pi_n^{n_o} = r(\pi_n)$ puisque $g_1(\pi_n) = 0$, donc le polynôme $T^{n_o}-r$ a une infinité de racines ; c'est impossible puisque $T^{n_o}-r$ n'est pas le polynôme 0 , donc $g = 0$.

Pour la deuxième assertion du lemme on écrit $u_o = f(\pi_o)$ qui montre que le terme constant de f est congru à 1 modulo l'idéal maximal de Φ_o ; ce terme constant étant dans $\mathbb{Z}_p$, il est dans $1+p\mathbb{Z}_p$.

PROPOSITION 4.15. <u>Pour tout</u> u <u>de</u> $\mathfrak{G}$, <u>nous notons</u> $f_r(u)$ <u>le coefficient de</u> T^r <u>dans la série associée à</u> u ; <u>pour tout</u> $r \in \mathbb{N}$, <u>l'application qui à</u> u <u>associe</u> $f_r(u)$ <u>est une application continue de</u> $\mathfrak{G}$ <u>munie de la topologie induite par la topologie de</u> U <u>vers</u> $\mathbb{Z}_p$.

<u>Démonstration</u>. Notons ord_p la valuation de $\bar{\mathbb{Q}}_p$ normalisée par $\mathrm{ord}_p(p) = 1$. Pour tout $u = (u_n)_{n\in\mathbb{N}} \in U = \varprojlim U_n$ et tout couple (M,N) d'entiers positifs, on note $V_u(M,N)$ le sous-ensemble de U formé des $v = (v_n)_{n\in\mathbb{N}}$ tels que $\mathrm{ord}_p(u_n - v_n) \geqslant M$ pour $n = 1,\dots,N$. Par définition de la topologie limite projective, les $V_u(M,N)$ décrivent un système fondamental de voisinages de u dans U lorsque M et N tendent vers $+\infty$. En conséquence, l'assertion de notre proposition est équivalente à l'assertion suivante : soient $u \in \mathfrak{G}$ et $r \in \mathbb{N}$; pour

tout entier $a > 0$, il existe deux entiers M et N tels que $v \in \mathfrak{A} \cap V_u(M,N)$ implique $\mathrm{ord}_p(f_r(u)-f_r(v)) \geqslant a$. Pour prouver cette dernière assertion, montrons qu'il suffit de prendre $M = a$ et N tels que $\varphi(p^{N-a+2}) \geqslant r+1$ (φ désignant l'indicateur d'Euler). Soient donc N tel que $\varphi(p^{N-a+2}) \geqslant r+1$ et $v \in \mathfrak{A} \cap V_u(a,N)$; pour tout $i \in \mathbb{N}$, posons $g_i = f_i(u)-f_i(v)$ de sorte que $u_n - v_n = \sum_{i=0}^{\infty} g_i \pi_n^i$ pour tout $n \in \mathbb{N}$. En particulier, pour $n = N$, il vient $u_N - v_N = \sum_{i=0}^{\infty} g_i \pi_N^i$ ce qui implique $\mathrm{ord}_p\left(\sum_{i=0}^{\infty} g_i \pi_N^i\right) \geqslant a$. On a $\mathrm{ord}_p(\pi_N) = \dfrac{1}{\varphi(p^{N+1})}$; on en déduit d'une part que $\mathrm{ord}_p\left(\sum_{i=\varphi(p^{N+1})}^{\infty} g_i \pi_N^i\right) \geqslant 1$ et d'autre part que les $\mathrm{ord}_p(g_i \pi_N^i)$ pour $i = 1,\dots,\varphi(p^{N+1})-1$ sont distincts deux à deux (puisque $\mathrm{ord}_p(g_i) \in \mathbb{N}$). De ces deux derniers points on déduit que, pour chaque $i = 0,1,\dots,\varphi(p^{N+1})-1$, on a $\mathrm{ord}_p(g_i \pi_N^i) \geqslant 1$; pour ces i, on a donc $\mathrm{ord}_p(g_i) > 0$, ce qui implique que p divise g_i. Si $a = 1$, cela termine la démonstration puisque $r \leqslant \varphi(p^{N+1})-1$ par définition de N. Si $a \geqslant 2$, l'égalité $u_{N-1} - v_{N-1} = \sum_{i=0}^{\infty} g_i \pi_{N-1}^i$ implique $\mathrm{ord}_p\left(\sum_{i=0}^{\infty} g_i \pi_{N-1}^i\right) \geqslant 2$. Si $i \geqslant \varphi(p^{N+1})$, on a $\mathrm{ord}_p(g_i \pi_{N-1}^i) \geqslant \dfrac{i}{\varphi(p^N)} \geqslant 2$; si $\varphi(p^N) \leqslant i \leqslant \varphi(p^{N+1})-1$, on a $\mathrm{ord}_p(g_i \pi_{N-1}^i) = \mathrm{ord}_p(g_i) + \dfrac{i}{\varphi(p^N)} \geqslant 2$ puisque, comme nous venons de le voir, p divise g_i pour ces i. On a donc $\mathrm{ord}_p\left(\sum_{i=\varphi(p^N)}^{\infty} g_i \pi_{N-1}^i\right) \geqslant 2$ d'où l'on tire $\mathrm{ord}_p\left(\sum_{i=0}^{\varphi(p^N)-1} g_i \pi_{N-1}^i\right) \geqslant 2$. Mais, pour $i = 0,\dots,\varphi(p^N)-1$, les $\mathrm{ord}_p(g_i \pi_{N-1}^i)$ sont distincts (puisque $\mathrm{ord}_p(g_i) \in \mathbb{N}$) donc on a $\mathrm{ord}_p(g_i \pi_{N-1}^i) \geqslant 2$ pour chaque $i = 0,\dots,\varphi(p^N)-1$. On en déduit $\mathrm{ord}_p(g_i) > 1$ pour ces i, donc p^2 divise g_i pour $i = 0,\dots,\varphi(p^N)-1$. En itérant ce procédé, on montre p^a divise g_i pour $i = 0,\dots,\varphi(p^{N-a+2})-1$ ce qui prouve p^a divise g_r puisque $r \leqslant \varphi(p^{N-a+2})-1$ par définition de N ; cela achève notre démonstration.

COROLLAIRE 4.16. <u>Le sous-ensemble</u> $\mathfrak{a}$ <u>de</u> U <u>est complet</u> (<u>donc fermé, donc compact</u>).

<u>Démonstration</u>. Soit $(u^j)_{j\in\mathbb{N}}$ une suite d'élément de $\mathfrak{a}$ convergeant vers un élément $u = (u_n)_{n\in\mathbb{N}} \in U$. La proposition 4.15 montre que, pour tout $r \in \mathbb{N}$, la suite $f_r(u^j)$ est une suite de Cauchy dans $\mathbb{Z}_p$ donc converge dans $\mathbb{Z}_p$; notons f_r sa limite et posons $f(T) = \sum_{r=0}^{\infty} f_r T^r$. On vérifie facilement que $f(\pi_n) = u_n$ pour tout $n \in \mathbb{N}$ donc que u est dans $\mathfrak{a}$, C.Q.F.D.

PROPOSITION 4.17. 1) <u>Si</u> u <u>et</u> v <u>sont dans</u> $\mathfrak{a}$, <u>alors le produit</u> uv <u>est dans</u> $\mathfrak{a}$.

2) <u>Si</u> u <u>est dans</u> $\mathfrak{a}$ <u>et si</u> $a \in \mathbb{Z}_p$, <u>alors</u> u^a <u>est dans</u> $\mathfrak{a}$.

3) <u>Si</u> u <u>est dans</u> $\mathfrak{a}$ <u>et si</u> $\sigma \in G_\infty = \mathrm{Gal}(\Phi_\infty/\mathbb{Q}_p)$, <u>alors</u> $\sigma(u)$ <u>est dans</u> $\mathfrak{a}$.

<u>Démonstration</u>. 1) Si f et g sont les séries telles que $f(\pi_n) = u_n$ et $g(\pi_n) = v_n$ pour tout $n \in \mathbb{N}$, alors on a $(fg)(\pi_n) = u_n v_n$ pour tout $n \in \mathbb{N}$ ce qui montre que $uv \in \mathfrak{a}$.

2) Soit $f(T) = \sum_{i\geqslant 0} f_i T^i$ la série associée à u . D'après le lemme 4.14 on a $f_o \in 1+p\mathbb{Z}_p$ et donc f_o^a est bien défini ; d'autre part $\frac{1}{f_o} f(T) \in 1+p\mathbb{Z}_p[[T]]$ donc $(\frac{1}{f_o} f(T))^a$ est bien défini ; on pose $f^a(T) = f_o^a(\frac{1}{f_o} f(T))^a$. En combinant le lemme 7.4 du §7 de la partie I de ce cours et le théorème 2 du §5 du chap. IV de [1] , on voit que $f^a(\pi_n) = (f(\pi_n))^a$ pour tout $n \in \mathbb{N}$ i.e. que $f^a(\pi_n) = u_n^a$ pour tout $n \in \mathbb{N}$; cela montre bien que u^a est dans $\mathfrak{a}$.

3) Désignons toujours par f(T) la série associée à u et posons $g(T) = f((1+T)^{\varkappa(\sigma)}-1)$. En raisonnant comme en 2) on voit que $g(\pi_n) = f(\zeta_n^{\varkappa(\sigma)}-1)$ pour tout $n \in \mathbb{N}$; mais $\zeta_n^{\varkappa(\sigma)}-1 = \sigma(\pi_n)$ donc $f(\zeta_n^{\varkappa(\sigma)}-1) = \sigma(f(\pi_n)) = \sigma(u_n)$ pour tout $n \in \mathbb{N}$ i.e. $g(\pi_n) = \sigma(u_n)$ pour tout $n \in \mathbb{N}$; cela montre que $\sigma(u)$ est dans $\mathfrak{a}$.

COROLLAIRE 4.18. *$\mathfrak{a}$ est un sous-Λ-module de U. De plus, si $u \in \mathfrak{a}$ et si $u = \prod_{i=1}^{p-1} u^{(i)}$ est la décomposition canonique de u dans $U = \prod_{i=1}^{p-1} U^{(i)}$, alors chaque $u^{(i)}$ est dans $\mathfrak{a}$.*

Démonstration. D'après le 2) et le 3) de la proposition précédente, $\mathfrak{a}$ est stable par $\mathbb{Z}_p$ et par Γ ; en conséquence $\mathfrak{a}$ est stable par le sous-anneau de Λ formé des combinaisons à coefficients dans $\mathbb{Z}_p$ des séries du type $(1+T)^a$ avec $a \in \mathbb{Z}_p$. Ce sous-anneau étant dense dans Λ le corollaire 4.16 montre que $\mathfrak{a}$ est stable par Λ tout entier. D'autre part $u^{(i)} = \prod_{\tau \in \Delta} \tau(u)^{\chi^i(\tau^{-1})}$ donc, $\mathfrak{a}$ étant stable par Δ et par $\mathbb{Z}_p$ d'après les 2) et 3) de la proposition précédente, $u^{(i)}$ est dans $\mathfrak{a}$ dès que u est dans $\mathfrak{a}$.

On peut enfin démontrer le résultat annoncé plus haut :

THEOREME 4.19. *Si $i \neq 1, p-1$, les éléments de $U^{(i)}$ sont admissibles* i.e. $U^{(i)} \subset \mathfrak{a}$.

Démonstration. Cela résulte directement de la juxtaposition de la proposition 4.13 et du corollaire 4.18.

Terminons ce chapitre en définissant, pour tout entier $k \geqslant 1$, une application φ_k du Λ-module $\mathfrak{a}$ vers $\mathbb{Z}_p$ qui, pour $k = 1,\dots,p-1$ est l'analogue de l'application ψ_k de U_o dans $\mathbb{F}_p$ définie ci-dessus. Pour tout $u = (u_n)_{n \in \mathbb{N}} \in \mathfrak{a}$, notons f_u la série de $\mathbb{Z}_p[[T]]$ telle que $u_n = f_u(\pi_n)$ pour tout $n \in \mathbb{N}$ (cette série est bien déterminée par u d'après le lemme 4.14) ; on définit $\varphi_k(u)$ par l'égalité $\varphi_k(u) = \left[D^{k-1} \frac{Df_u}{f_u}\right](0)$ (on rappelle que D est l'opérateur $(T+1)\frac{d}{dT}$). On a :

PROPOSITION 4.20. *Pour tout $k \geqslant 1$ on a :*

1) *φ_k est un homomorphisme continu du groupe $\mathfrak{a}$ (muni de la topologie induite par la topologie de U) vers $\mathbb{Z}_p$.*

2) <u>Pour tout</u> $\sigma \in G_\infty = \mathrm{Gal}(\Phi_\infty/\mathbb{Q}_p)$ <u>et tout</u> $u \in \mathcal{U}$ <u>on a</u> $\varphi_k(\sigma(u)) = \varkappa(\sigma)^k \varphi_k(u)$.

<u>Démonstration</u>. 1) Soit $u \in \mathcal{U}$; le lemme 4.14 montre que f_u est inversible dans $\mathbb{Z}_p[[T]]$ donc $\frac{Df}{f}$ est dans $\mathbb{Z}_p[[T]]$. En conséquence $D^{k-1}\frac{Df}{f}$ est dans $\mathbb{Z}_p[[T]]$ et donc $\varphi_k(u)$ est dans $\mathbb{Z}_p$. Si maintenant u et v sont dans $\mathcal{U}$, il est clair que uv est dans $\mathcal{U}$ et que $f_{uv} = f_u f_v$; on a donc $\frac{D(f_u f_v)}{f_u f_v} = \frac{Df_u}{f_u} + \frac{Df_v}{f_v}$ d'où l'on tire $\varphi_k(uv) = \varphi_k(u) + \varphi_k(v)$. Enfin la continuité de φ_k résulte clairement de la proposition 4.15.

2) Comme on l'a vu dans la démonstration du 3) de la proposition 4.17, on a $f_{\sigma(u)}(T) = f_u((1+T)^{\varkappa(\sigma)}-1)$. Le lemme 4.10 montre donc que $\left[D^{k-1}\frac{Df_{\sigma(u)}}{f_{\sigma(u)}}\right](0) = \varkappa(\sigma)^k\left[D^{k-1}\frac{Df_u}{f_u}\right](0)$ c'est-à-dire que $\varphi_k(\sigma(u)) = \varkappa(\sigma)^k\,\varphi_k(u)$, C.Q.F.D.

COROLLAIRE 4.21. 1) <u>Si</u> u <u>est un élément admissible de</u> $U^{(i)}$ <u>et si</u> $k \equiv i$ <u>modulo</u> $p-1$, <u>on a</u> $\varphi_k(u) = 0$.

2) <u>Si</u> u <u>est un élément admissible de</u> U <u>et si</u> $u = \prod_{i=1}^{p-1} u^{(i)}$ <u>est la décomposition de</u> u <u>dans</u> $U = \prod_{i=1}^{p-1} U^{(i)}$, <u>on a</u> $\varphi_k(u) = \varphi_k(u^{(i)})$ <u>pour chaque</u> $k \equiv i$ <u>modulo</u> $p-1$.

<u>Démonstration</u>. Si $\tau \in \Delta$, on a par définition $\varkappa(\tau) = \chi(\tau)$ et on raisonne comme dans les démonstrations des points 2) et 3) du corollaire 4.11.

Le point important est le théorème suivant :

THEOREME 4.22. <u>Soit</u> γ <u>le</u> $\mathbb{Z}_p$<u>-générateur du sous-groupe</u> $\Gamma = \mathrm{Gal}(\Phi_\infty/\Phi_0)$ <u>de</u> G_∞ <u>choisi pour identifier</u> $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$ <u>et</u> $\Lambda = \mathbb{Z}_p[[T]]$ (proposition 3.4). <u>Pour tout</u> $u \in \mathcal{U}$, <u>tout</u> $h \in \Lambda$ <u>et tout</u> $k \geqslant 1$, <u>on a</u> $\varphi_k(hu) = h(\varkappa(\gamma)^k-1)\varphi_k(u)$.

<u>Démonstration</u>. L'égalité du théorème est claire pour $h=1$; le 2) de la proposition 4.20 appliqué avec $\sigma=\gamma$ montre qu'elle est vraie pour $h=1+T$; on en déduit qu'elle est vraie pour $h=T$, puis pour $h=T^n$ si $n \geqslant 0$; en conséquence cette égalité est vraie pour tout $h \in \mathbb{Z}_p[T]$. Enfin, les φ_k étant continues et $\mathbb{Z}_p[T]$ étant dense dans $\mathbb{Z}_p[[T]]$, on en déduit que notre égalité est vraie pour tout $h \in \mathbb{Z}_p[[T]]$, C.Q.F.D.

§5. LA DÉMONSTRATION DU THÉORÈME 3.7.

Rappelons l'énoncé du théorème 3.7 : soit $i=2,4,\dots,p-3$ et soit $Y^{(i)} = \varprojlim(U_n^{(i)}/\bar{C}_n^{(i)})$; alors 1) le Λ-module $Y^{(i)}$ est isomorphe à $\Lambda/(F_i(T))$ où $F_i(T)$ est la série définie de la manière suivante : on note $g_i(T)$ la série telle que $g_i(\varkappa(\gamma)^{-s}-1) = L_p(s,\omega^i)$ pour tout $s \in \mathbb{Z}_p$ et on pose $F_i(T) = g_i(\frac{1+T}{\varkappa(\gamma)} - 1)$.

2) Pour tout $n \geqslant 0$, la projection de $Y^{(i)}$ sur $U_n^{(i)}/\bar{C}_n^{(i)}$ induit un isomorphisme de $\Lambda/(F_i(T),\omega_n(T))$ sur $U_n^{(i)}/\bar{C}_n^{(i)}$.

Dans ce paragraphe, on choisit un $c \in \mathbb{Z}_p$ qui vérifie la propriété suivante : pour tout $n \geqslant 0$, la classe de c modulo $p^{n+1}\mathbb{Z}_p$ engendre le groupe $(\mathbb{Z}_p/p^n\mathbb{Z}_p)^* = (\mathbb{Z}/p^n\mathbb{Z})^*$; on pose alors

$e_n = \dfrac{\zeta_n - 1}{\zeta_n^c - 1}$ (on rappelle que ζ_n est une racine de l'unité d'ordre p^{n+1} et que $\zeta_n^p = \zeta_{n-1}$ pour tout $n > 0$). On a :

LEMME 5.1. <u>Le groupe</u> Cycl_n <u>est le groupe engendré par la famille</u> $(\sigma(e_n))_{\sigma \in G_n}$.

<u>Démonstration</u>. On reprend les notations de la définition 2.5 et on note $c(n)$ l'image de c dans $(\mathbb{Z}/p^{n+1}\mathbb{Z})^*$. On a $e_n = u_{c(n)}$ donc $e_n \in \mathrm{Cycl}_n$ et donc le groupe engendré par la famille $(\sigma(e_n))_{\sigma\in G_n}$ est inclus dans Cycl_n. D'autre part, si $b \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^*$, il existe un entier t tel que $b = c(n)^t$. Notons σ l'élément de G_n défini

par $\sigma(\zeta_n)=\zeta_n^c$; on a $e_n.\sigma(e_n)\ldots\sigma^{t-1}(e_n) = \frac{\zeta_n-1}{\zeta_n^c-1}.\frac{\zeta_n^c-1}{\zeta_n^{c^2}-1}\ldots\frac{\zeta_n^{c^{t-1}}-1}{\zeta_n^{c^t}-1}$ $= \frac{\zeta_n-1}{\zeta_n^b-1} = u_b$, donc u_b appartient au groupe engendré par les $(\sigma(e_n))_{\sigma\in G_n}$ et donc Cycl_n est inclus dans ce groupe, ce qui achève notre démonstration.

On rappelle que l'on a plongé $K_\infty = \bigcup_n K_n$ dans $\bar{\mathbb{Q}}_p$ et que l'on a noté Φ_n l'adhérence de K_n dans $\bar{\mathbb{Q}}_p$; en conséquence on peut considérer e_n comme un élément de Φ_n . Notons $\omega(c)$ la racine $p-1$ième de l'unité de $\mathbb{Z}_p$ qui est congrue à c modulo $p\mathbb{Z}_p$ et posons $v_n = \omega(c)e_n \in \Phi_n$. On a

LEMME 5.2. <u>L'élément</u> v_n <u>défini ci-dessus est dans</u> U_n .

<u>Démonstration</u>. On a $\frac{\zeta_n^c-1}{\zeta_n-1} = \frac{\zeta_n^d-1}{\zeta_n-1}$ si d est un entier positif congru à c modulo $p^{n+1}\mathbb{Z}_p$; on a donc $\frac{\zeta_n^c-1}{\zeta_n-1} = \zeta_n^{d-1}+\zeta_n^{d-2}+\ldots+1$ ce qui montre que $\frac{\zeta_n^c-1}{\zeta_n-1}$ est congru à d modulo l'idéal maximal de Φ_n ; comme $\omega(c)$ est congru à d modulo $p\mathbb{Z}_p$, on a $v_n = \omega(c)\frac{\zeta_n-1}{\zeta_n^c-1} \in U_n$, C.Q.F.D.

Montrons maintenant la proposition suivante :

PROPOSITION 5.3. <u>Le</u> $Z_p[G_n]$<u>-module</u> $\bar{C}_n$ <u>est engendré par</u> v_n i.e. $\bar{C}_n = \mathbb{Z}_p[G_n]v_n$.

<u>Démonstration</u>. Montrons tout d'abord que C_n est inclus dans le groupe engendré par la famille $(\sigma(v_n))_{\sigma\in G_n}$, ce qui impliquera $\bar{C}_n \subset \mathbb{Z}_p[G_n]v_n$. Soit x un élément de C_n , alors (lemme 5.1) $x = \prod_{\sigma\in G_n} \sigma(e_n)^{x_\sigma}$ pour une famille $(x_\sigma)_{\sigma\in G_n}$ d'éléments de $\mathbb{Z}$; compte-tenu de $v_n = \omega(c)^{-1}e_n$ et du fait que $\omega(c)$ est dans $\mathbb{Z}_p$,

on en déduit $x = \omega(c)^{-\sum_\sigma x_\sigma} \prod_{\sigma \in G_n} \sigma(v_n)$; comme x et chacun des $\sigma(v_n)$ est dans U_n, cette dernière égalité implique que $\omega(c)^{\sum_\sigma x_\sigma}$ est dans U_n ; mais $\omega(c)$ étant une racine $p-1^{\text{ième}}$ de l'unité on en déduit que $\omega(c)^{\sum_\sigma x_\sigma} = 1$ et donc que $x = \prod_{\sigma \in G_n} \sigma(v_n)^{x_\sigma}$, ce qu'on voulait. Il reste, pour achever la démonstration, à voir que v_n est dans $\bar{C}_n$. Pour tout entier t, on a $\left(\frac{\zeta_n - 1}{\zeta_n^c - 1}\right)^{1-p^t} \in C_n$ puisque $\left(\frac{\zeta_n - 1}{\zeta_n^c - 1}\right)^{1-p^t}$ est dans U_n et dans Cycl_n ; on a donc $\frac{\zeta_n - 1}{\zeta_n^c - 1} \cdot \left(\frac{\zeta_n - 1}{\zeta_n^c - 1}\right)^{-p^t} \in C_n$. Posons $\frac{\zeta_n - 1}{\zeta_n^c - 1} = x_1 x_2$ avec $x_1 = \omega(c)$ et x_2 congru à 1 modulo l'idéal maximal de Φ_n ; on a donc $x_1^{p^t} = \omega(c)$ pour tout $t \geqslant 0$ et $x_2^{p^t}$ tend vers 1 lorsque t tend vers l'infini. En conséquence, les $\frac{\zeta_n - 1}{\zeta_n^c - 1}\left(\frac{\zeta_n - 1}{\zeta_n^c - 1}\right)^{-p^t}$ forment une suite (indicée par t) d'éléments de C_n qui converge vers $\frac{\zeta_n - 1}{\zeta_n^c - 1}\,\omega(c)^{-1} = v_n$; cela montre que $v_n \in \bar{C}_n$ et achève la démonstration.

COROLLAIRE 5.4. <u>Pour tout</u> $i = 1, \dots, p-1$, <u>on a</u>
$\bar{C}_n^{(i)} = \mathbb{Z}_p[\Gamma/\Gamma_n] v_n^{(i)}$.

<u>Démonstration</u>. La proposition précédente montre que $\bar{C}_n^{(i)} = \mathbb{Z}_p[G_n] v_n^{(i)}$. Le groupe G_n s'identifie à $\Delta \times (\Gamma/\Gamma_n)$. On sait que, pour tout $\tau \in \Delta$, l'action de τ sur $U_n^{(i)}$ est l'élévation à la puissance $\chi^i(\tau)$, il en résulte que $\mathbb{Z}_p[G_n] v_n^{(i)} = \mathbb{Z}_p[\Gamma/\Gamma_n] v_n^{(i)}$ ce qui démontre notre corollaire.

Enfin on a

PROPOSITION 5.5. 1) <u>L'élément</u> $v = (v_n)_{n \in \mathbb{N}}$ <u>est dans</u> $U = \varprojlim U_n$.
2) $\bar{C}^{(i)} = \Lambda v^{(i)}$ <u>pour tout</u> $i = 1, \dots, p-1$.

<u>Démonstration</u>. 1) Le lemme 5.2 montre que $v_n \in U_n$ pour tout $n \in \mathbb{N}$, il reste à voir que $N_{n+1,n}(v_{n+1}) = v_n$ pour tout $n \in \mathbb{N}$. Le polynôme minimal de $\zeta_{n+1} - 1$ sur Φ_n étant $(X+1)^p - \zeta_n$, on a $N_{n+1,n}(\zeta_{n+1} - 1) = \zeta_n - 1$; de même on montre que $N_{n+1,n}(\zeta^c_{n+1} - 1) = \zeta^c_n - 1$. On conclut alors en remarquant que $N_{n+1,n}(\omega(c)) = \omega(c)^p = \omega(c)$.

2) On a vu que $v_n \in \bar{C}_n$, donc $v_n^{(i)} \in \bar{C}_n^{(i)}$ et $v^{(i)} \in \bar{C}^{(i)}$; il en résulte que $\Lambda v^{(i)} \subset \bar{C}^{(i)}$. D'autre part, le corollaire 5.4 montre que l'image de $\Lambda v^{(i)}$ par la projection de $\bar{C}^{(i)}$ sur $\bar{C}_n^{(i)}$ est $\bar{C}_n^{(i)}$ tout entier. En conséquence $\Lambda v^{(i)}$ est dense dans $\varprojlim \bar{C}_n^{(i)} = \bar{C}_i$; mais $\Lambda v^{(i)}$ est compact, donc $\Lambda v^{(i)} = \bar{C}^{(i)}$. C.Q.F.D.

Rappelons (proposition 4.13) que, si $i \neq 1, p-1$, alors il existe une racine $p-1^{\underline{\text{ième}}}$ de l'unité λ dans $\mathbb{Z}_p$ telle que $U^{(i)} = \Lambda w_\lambda^{(i)}$; en conséquence, il existe un $h \in \Lambda$ tel que $v^{(i)} = h w_\lambda^{(i)}$ et le Λ-module $U^{(i)}/\bar{C}^{(i)}$ est isomorphe à $\Lambda/\Lambda h$. Pour démontrer le 1) du théorème 3.7, il faut montrer que l'idéal Λh de Λ est égal à $\Lambda(F_i)$ où $F_i(T)$ est la série définie dans l'énoncé du théorème 3.7. Commençons par calculer, pour tout $k \geqslant 1$, les valeurs $\varphi_k(v)$ et $\varphi_k(w_\lambda)$.

PROPOSITION 5.6. <u>Pour tout</u> $k \geqslant 1$, <u>on a</u> $\varphi_k(v) = (c^k - 1)\zeta(1-k)$.

<u>Démonstration</u>. Pour tout $n \geqslant 0$, on a $v_n = \omega(c)\dfrac{\zeta_n - 1}{\zeta_n^c - 1}$ c'est-à-dire que $v_n = f(\pi_n)$ si $f(T) = \omega(c)\dfrac{T}{(T+1)^c - 1}$. D'autre part $\dfrac{Df}{f}(T) = \dfrac{1+T}{T} - c\,\dfrac{(1+T)^c}{(1+T)^c - 1}$; désignons alors par C un élément de $\hat{\mathbb{Z}}^*$ tel que $C_p = c$, on a vu (I, corollaire 8.11) que la série $F_{\nu_{C,1}}(T)$ attachée à la mesure $\nu_{C,1}$ est $C_p \dfrac{(1+T)^{C_p}}{(1+T)^{C_p} - 1} - \dfrac{1+T}{T}$; on a donc $\dfrac{Df}{f}(T) = -F_{\nu_{C,1}}(T)$. En conséquence $\varphi_k(v) = \left[D^{k-1}\dfrac{Df}{f}\right](0) = -\left[D^{k-1}F_{\nu_{C,1}}\right](0)$ est égal (I, corollaire 8.7) à $-\int_{\mathbb{Z}_p} x^{k-1} d\nu_{C,1}(x) = (C_p^k - 1)\zeta(1-k) =$

$(c^k-1)\zeta(1-k)$. C.Q.F.D.

PROPOSITION 5.7. <u>Soit</u> $\lambda \neq 1$ <u>une racine</u> $p-1^{\text{ième}}$ <u>de l'unité dans</u> $\mathbb{Z}_p$ <u>et</u> $i \in \{1,\dots,p-1\}$; <u>on a</u> :

1) <u>il existe une série</u> $u \in \Lambda$ <u>telle que</u> $(1-p^{k-1})\varphi_k(w_\lambda) = u(\varkappa(\gamma)^{k-1}-1)$ <u>pour tout entier</u> $k \geqslant 1$ <u>et</u> $k \equiv i$ <u>modulo</u> $p-1$;

2) <u>si</u> $i \neq 1, p-1$ <u>et</u> λ <u>est tel que</u> $w_\lambda^{(i)}$ <u>est une base du</u> Λ-<u>module</u> $U^{(i)}$, <u>alors</u> $u \in \Lambda^*$.

<u>Démonstration</u>. 1) Pour tout $n \geqslant 0$, on a $w_{\lambda,n} = f(\pi_n)$ si $f(T) = \frac{\lambda-1-T}{\omega(\lambda-1)}$; on a $\frac{Df}{f}(T) = \frac{T+1}{T+1-\lambda}$ que nous notons $F(T)$. Comme au §8 du I posons $\tilde{F}(T) = F(T) - \frac{1}{p}\sum_{\eta\in\mu_p} F(\eta(T+1)-1) = \frac{T+1}{T+1-\lambda} - \frac{1}{p}\sum_{\eta\in\mu_p}\frac{\eta(T+1)}{\eta(T+1)-\lambda}$ $= \frac{T+1}{T+1-\lambda} - \frac{(T+1)^p}{(T+1)^p-\lambda}$. On sait que le changement de variable $T+1 = e^Z$ transforme l'opérateur D en l'opérateur $\frac{d}{dZ}$; en conséquence, si $G(Z) = \frac{e^Z}{e^Z-\lambda}$, on a $D^{k-1}\left.\frac{T+1}{T+1-\lambda}\right|_{T=0} = \left.\frac{d^{k-1}}{dZ^{k-1}}G(Z)\right|_{Z=0}$; de même $G(pZ) = \frac{e^{pZ}}{e^{pZ}-\lambda}$, donc $D^{k-1}\left.\frac{(T+1)^p}{(T+1)^p-\lambda}\right|_{T=0} = \left.\frac{d^{k-1}}{dZ^{k-1}}G(pZ)\right|_{Z=0} =$ $p^{k-1}\left.\frac{d^{k-1}}{dZ^{k-1}}G(Z)\right|_{Z=0}$; en conséquence $D^{k-1}\tilde{F}(T)\Big|_{T=0} =$ $(1-p^{k-1})\,D^{k-1}\left.\frac{T+1}{T+1-\lambda}\right|_{T=0} = (1-p^{k-1})\varphi_k(w_\lambda)$ par définition de $\varphi_k(w_\lambda)$. Pour achever la démonstration de ce 1), il suffit donc de voir qu'il existe une série $u \in \Lambda$ telle que $u(\varkappa(\gamma)^{k-1}-1) = D^{k-1}\tilde{F}(T)\Big|_{T=0}$ pour tout entier $k \geqslant 1$ et $k \equiv i$ modulo $p-1$; comme $1-\lambda$ est inversible dans $\mathbb{Z}_p$, il est clair que $\tilde{F}(T)$ est dans Λ et donc le lemme suivant achève la démonstration du 1) :

LEMME 5.8. <u>Soient</u> $H(T)$ <u>un élément de</u> Λ <u>et</u> i <u>un entier compris entre</u> 1 <u>et</u> $p-1$; <u>il existe une série</u> $u \in \Lambda$ <u>telle que</u> $u(\varkappa(\gamma)^{k-1}-1) = D^{k-1}H(T)\Big|_{T=0}$ <u>pour tout entier</u> $k \geqslant 1$ <u>et</u> $k \equiv i$ <u>modulo</u> $p-1$.

Démonstration. Notons ν la mesure sur $\mathbb{Z}_p$ associée à la série $H(T)$ (i.e. telle que $H(T) = F_\nu(T)$ avec les notations du $\mathcal{I}$, proposition 4.4). On sait ($\mathcal{I}$, corollaire 8.7) que $D^{k-1}H(T)\big|_{T=0} = \int_{\mathbb{Z}_p} x^{k-1}\,d\nu(x) = \int_{\mathbb{Z}_p} \omega(x)^{k-1}\langle x\rangle^{k-1}\,d\nu(x)$ si $\omega(x)$ est la racine $p-1^{\text{ième}}$ de l'unité de $\mathbb{Z}_p$ congrue à x modulo $p\mathbb{Z}_p$. Mais $k \equiv i$ modulo $p-1$, donc $\omega^{k-1}(x) = \omega^{i-1}(x)$ et on a $D^{k-1}H(T)\big|_{T=0} = \int \langle x\rangle^{k-1} d(\omega^{i-1}\nu)(x)$ en désignant par $\omega^{i-1}\nu$ la mesure sur $\mathbb{Z}_p$ de densité ω^{i-1} par rapport à ν ($\mathcal{I}$, définition 2.5). En reprenant les notations du $\mathcal{I}$, cela signifie que $D^{k-1}H(T)\big|_{T=0} = \Gamma_{\omega^{i-1}\nu}(1-k)$ et notre lemme résulte du théorème 5.7 de I puisque $\varkappa(\gamma)$ est un générateur de $1+p\mathbb{Z}_p$.

2) Il découle des définitions de ψ_i et de φ_i que, pour $1 \leqslant i \leqslant p-2$ et $x = (x_n)_{n\in\mathbb{N}}$ élément admissible de $U = \varprojlim U_n$, la classe de $\varphi_i(x)$ modulo $p\mathbb{Z}_p$ est égale à $\psi_i(x)$. La proposition 4.12 montre donc que $\varphi_i(w_\lambda)$ est dans $\mathbb{Z}_p^*$ si λ est tel que $w_\lambda^{(i)}$ est une base de $U^{(i)}$. En conséquence, si $1 \not\leqslant i \not\leqslant p-1$, l'élément $(1-p^{i-1})\varphi_i(w_\lambda)$ est dans $\mathbb{Z}_p^*$ c'est-à-dire que $u(\varkappa(\gamma)^{i-1}-1)$ est dans $\mathbb{Z}_p^*$; comme $\varkappa(\gamma)^{i-1}-1$ est dans $p\mathbb{Z}_p$, il en résulte que u est dans Λ^*, ce qui est ce qu'on cherchait.

Nous sommes maintenant en mesure de démontrer le théorème 3.7. Soient $i \in \{1,\ldots,p-1\}$ et $i \neq 1, p-1$, soit λ une racine $p-1^{\text{ième}}$ de l'unité de $\mathbb{Z}_p$ telle que $\Lambda w_\lambda^{(i)} = U^{(i)}$ et soit $h \in \Lambda$ l'élément défini par $v^{(i)} = hw_\lambda^{(i)}$ de sorte que $U_n^{(i)}/\bar{C}_n^{(i)}$ est (comme nous l'avons remarqué plus haut) isomorphe en tant que Λ-module à $\Lambda/\Lambda h$. Le théorème 4.22 montre que $\varphi_k(v^{(i)}) = h(\varkappa(\gamma)^k-1)\varphi_k(w_\lambda^{(i)})$. Si $k \equiv i$ modulo $p-1$, le corollaire 4.18 montre que $\varphi_k(v^{(i)}) = \varphi_k(v)$ et $\varphi_k(w_\lambda^{(i)}) = \varphi_k(w_\lambda)$; les propositions 5.6 et 5.7 prouvent alors que $(c^k-1)(1-p^{k-1})\zeta(1-k) = h(\varkappa(\gamma)^k-1)u(\varkappa(\gamma)^{k-1}-1)$ avec $u \in \Lambda^*$, soit ($\mathcal{I}$, définition 6.4) $(c^k-1)L_p(1-k,\omega^i) = h(\varkappa(\gamma)^k-1)u(\varkappa(\gamma)^{k-1}-1)$.

Posons $u_1(T) = u(\frac{1+T}{\varkappa(\gamma)} - 1)$ et $r(T) = 1-\omega^i(c)(1+T)^\alpha$ où $\alpha \in \mathbb{Z}_p$ est défini par $\langle c \rangle = \varkappa(\gamma)^\alpha$; la série $u_1(T)$ est dans Λ^* puisque u est dans Λ^*, la série $r(T)$ est dans Λ^* puisque $\omega^i(c)$ n'est pas congru à 1 modulo p (car c a été choisi de telle sorte que sa classe modulo $p\mathbb{Z}_p$ engendre $(\mathbb{Z}_p/p\mathbb{Z}_p)^*$ et on a $u_1(\varkappa(\gamma)^k-1) = u(\varkappa(\gamma)^{k-1}-1)$ et $r(\varkappa(\gamma)^k-1) = c^k-1$ si $k \equiv i$ modulo $p-1$. En conséquence, si l'on pose $F_i = \frac{hu_1}{r}$, on a d'une part $\Lambda h = \Lambda F_i$ et d'autre part $F_i(\varkappa(\gamma)^k-1) = L_p(1-k,\omega^i)$ pour tout entier $k \geqslant 1$ et $k \equiv i$ modulo $p-1$. Enfin, si en plus i est pair et si on note g_i la série telle que $g_i(\varkappa(\gamma)^{-s}-1) = L_p(s,\omega^i)$ pour tout $s \in \mathbb{Z}_p$, les séries $F_i(T)$ et $g_i(\frac{1+T}{\varkappa(\gamma)} - 1)$ prennent toutes les deux la valeur $L_p(1-k,\omega^i)$ pour $T = \varkappa(\gamma)^k-1$ si $k \geqslant 1$ et $k \equiv i$ modulo $p-1$; un raisonnement analogue à celui fait dans la démonstration du lemme 4.14 montre que cela implique l'égalité $F_i(T) = g_i(\frac{1+T}{\varkappa(\gamma)} - 1)$ et cela achève la démonstration du 1) du théorème 3.7.

Il reste à démontrer l'assertion 2) du théorème 3.7. La proposition 5.5 et le corollaire 5.4 montrent que la projection de $\bar{C}^{(i)}$ vers $\bar{C}_n^{(i)}$ est surjective. Du corollaire 4.4, on déduit alors que la projection de $U^{(i)}$ vers $U_n^{(i)}$ induit une surjection de $U^{(i)}$ sur $U_n^{(i)}/\bar{C}_n^{(i)}$ dont le noyau est $\bar{C}^{(i)}.(\omega_n(T)U^{(i)})$. Le quotient $U_n^{(i)}/\bar{C}_n^{(i)}$ est donc isomorphe à $U^{(i)}/[\bar{C}^{(i)}.(\omega_n(T)U^{(i)})]$ qui, d'après le 1) du théorème 3.7, est isomorphe à $\Lambda/(F_i(T),\omega_n(T))$; cela démontre le 2) du théorème 3.7, et donc achève la démonstration de ce théorème.

§6. MODULES D'IWASAWA ET GROUPES DE CLASSES.

Nous revenons à l'étude globale. Comme précédemment p est un nombre premier impair, K_n est le corps $\mathbb{Q}(\mu_{p^{n+1}})$, G_n est le groupe de Galois de $K_n/\mathbb{Q}$ et $\underline{\underline{p}}_n$ est l'idéal premier de K_n au-dessus de p ; pour alléger l'écriture nous notons K le corps $K_\infty = \bigcup_{n \geqslant 0} K_n$. Nous désignons par M_n la p-extension abélienne maximale de K_n qui est non ramifiée en dehors de $\underline{\underline{p}}_n$; pour tout n, le corps M_n contient K et M_{n+1} contient M_n ; nous posons $X_n = \mathrm{Gal}(M_n/K)$ et $X = \varprojlim X_n$ (les flèches de X_{n+1} vers X_n étant les restrictions des automorphismes de M_{n+1} à M_n) de sorte que X s'identifie à $\mathrm{Gal}(M/K)$ si $M = \bigcup_{n \geqslant 0} M_n$. Le corps M est galoisien sur $\mathbb{Q}$, donc $\mathrm{Gal}(K/\mathbb{Q})$ agit par conjugaison sur $X = \mathrm{Gal}(M/K)$; cette action munit X d'une structure de $\mathrm{Gal}(K/\mathbb{Q})$-module (on dit que X est un module d'Iwasawa). D'autre part, pour chaque n, notons A_n le sous-groupe du groupe des classes de K_n formé des classes dont l'ordre est une puissance de p et posons $A = \varinjlim A_n$ (les flèches entre A_n et A_{n+1} étant celles qui envoient la classe d'un idéal $\underline{a}$ de K_n sur la classe de l'idéal de K_{n+1} engendré par $\underline{a}$). Le groupe $\mathrm{Gal}(K/\mathbb{Q})$ agit de façon naturelle sur chaque A_n et ces actions définissent une action de $\mathrm{Gal}(K/\mathbb{Q})$ sur A qui fait de A un $\mathrm{Gal}(K/\mathbb{Q})$-module. Dans ce paragraphe nous allons relier les $\mathrm{Gal}(K/\mathbb{Q})$-modules X et A.

Notons $\tilde{K}$ la p-extension abélienne maximale de K. Pour tout $n \geqslant 0$ et tout $\alpha \in K^*$ nous désignons par $\varphi_n(\alpha)$ l'homomorphisme de $\mathrm{Gal}(\tilde{K}/K)$ vers μ_n défini de la manière suivante : on choisit une racine p^{n+1} ième de α que l'on note $\sqrt[p^{n+1}]{\alpha}$; celle-ci est dans $\tilde{K}$ et, pour tout $\tau \in \mathrm{Gal}(\tilde{K}/K)$ on pose $[\varphi_n(\alpha)](\tau) = \dfrac{\tau(\sqrt[p^{n+1}]{\alpha})}{\sqrt[p^{n+1}]{\alpha}}$ (qui est clairement un élément de μ_n indépendant du choix de la racine p^{n+1} ième de α choisie). On sait (théorie de Kummer) que l'application qui à α associe $\varphi_n(\alpha)$ induit un isomorphisme de $K^*/(K^*)^{p^{n+1}}$ sur $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\tilde{K}/K),\mu_n)$. L'injection canonique de $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\tilde{K}/K),\mu_n)$ dans $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\tilde{K}/K),\mu_{n+1})$ correspond, à travers ces isomorphismes, à l'application de $K^*/(K^*)^{p^{n+1}}$ vers $K^*/(K^*)^{p^{n+2}}$ qui envoie la classe d'un x de K^* modulo $(K^*)^{p^{n+1}}$ sur la classe de x^p modulo $(K^*)^{p^{n+2}}$; enfin $K^*/(K^*)^{p^m}$ s'identifie canoniquement à $K^* \otimes (\frac{1}{p^m}\mathbb{Z}/\mathbb{Z})$ et, dans cette identification, l'homomorphisme de $K^*/(K^*)^{p^m}$ vers $K^*/(K^*)^{p^{m+1}}$ décrit ci-dessus correspond au produit tensoriel de l'identité de K^* par l'injection canonique de $\frac{1}{p^m}\mathbb{Z}/\mathbb{Z}$ dans $\frac{1}{p^{m+1}}\mathbb{Z}/\mathbb{Z}$. En conséquence on a un isomorphisme de $\varinjlim_m (K^* \otimes (\frac{1}{p^m}\mathbb{Z}/\mathbb{Z})) = K^* \otimes \mathbb{Q}_p/\mathbb{Z}_p$ vers $\varinjlim_n (\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\tilde{K}/K),\mu_n)) = \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\tilde{K}/K),\mu_\infty)$ si $\mu_\infty = \bigcup_{n \geqslant 0} \mu_n$ est muni de la topologie discrète ; nous notons φ cet isomorphisme. Introduisons maintenant le sous-groupe V de $K^* \otimes \mathbb{Q}_p/\mathbb{Z}_p$ dont l'image par φ est le sous-groupe $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(M/K),\mu_\infty)$ de $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\tilde{K}/K),\mu_\infty)$; on note ψ l'homomorphisme de groupe de $\mathrm{Gal}(M/K) = X$ vers $\mathrm{Hom}(V,\mu_\infty)$ défini par $[\psi(x)](v) = [\varphi(v)](x)$ pour tout $x \in \mathrm{Gal}(M/K)$ et $v \in V$. On a le résultat suivant :

PROPOSITION 6.1. <u>L'application</u> ψ <u>définie ci-dessus est un isomorphisme du groupe</u> X <u>sur le groupe</u> $\mathrm{Hom}(V,\mu_\infty)$.

<u>Démonstration</u>. L'extension M/K est une p-extension, donc le groupe $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(M/K),\mu_\infty)$ est égal au groupe $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(M/K),\mathbb{C}^*)$; ce dernier, muni de la topologie discrète, est le dual de Pontrjagin de $\mathrm{Gal}(M/K)$. L'application φ identifie donc V muni de la topologie discrète au dual de Pontrjagin de $\mathrm{Gal}(M/K)$. D'autre part, pour tout $v \in V$ il existe un entier n_v tel que $p^{n_v} v = 0$ (puisqu'il en est déjà ainsi pour tout $v \in K^* \otimes \mathbb{Q}_p/\mathbb{Z}_p$), donc $\mathrm{Hom}(V,\mu_\infty)$ est égal à $\mathrm{Hom}(V,\mathbb{C}^*)$; ce dernier est le dual de Pontrjagin du groupe V muni de la topologie discrète, donc $\mathrm{Hom}(V,\mu_\infty)$ s'identifie au bidual de $\mathrm{Gal}(M/K)$. Dans cette identification, l'application ψ correspond à l'application canonique de $\mathrm{Gal}(M/K)$ vers son bidual donc le théorème de Pontrjagin montre que ψ est un isomorphisme de groupe, C.Q.F.D.

Dans la suite, si R est un anneau et G un groupe et si $\mathcal{A}$ et $\mathcal{B}$ sont deux R-modules munis de structures de G-modules compatibles avec l'action de R (i.e. $\mathcal{A}$ et $\mathcal{B}$ sont des $R[G]$-modules), on munit le R-module $\mathcal{A} \otimes_R \mathcal{B}$ (resp. $\mathrm{Hom}_R(\mathcal{A},\mathcal{B})$) de la structure de G-module qui est telle que, pour tout $\sigma \in G$, on ait $\sigma.(a\otimes b) = (\sigma.a)\otimes(\sigma.b)$ (resp. $[\sigma.f](a) = \sigma(f(\sigma^{-1}.a))$) si $a \in \mathcal{A}$ et $b \in \mathcal{B}$ (resp. $a \in \mathcal{A}$ et $f \in \mathrm{Hom}_R(\mathcal{A},\mathcal{B})$) ; il est clair que les structures de R-modules et de G-modules de $\mathcal{A}\otimes_R\mathcal{B}$ (resp. $\mathrm{Hom}_R(\mathcal{A},\mathcal{B})$) sont compatibles. Dans la pratique $R = \mathbb{Z}$ ou $\mathbb{Z}_p$; dans le premier cas on note $\mathcal{A}\otimes\mathcal{B}$ et $\mathrm{Hom}(\mathcal{A}\otimes\mathcal{B})$ à la place de $\mathcal{A}\otimes_R\mathcal{B}$ et $\mathrm{Hom}_R(\mathcal{A}\otimes\mathcal{B})$. Le corps $\tilde{K}$ étant galoisien sur $\mathbb{Q}$, $\mathrm{Gal}(K/\mathbb{Q})$ agit par conjugaison sur $\mathrm{Gal}(\tilde{K}/K)$ et donc $\mathrm{Hom}(\mathrm{Gal}(\tilde{K}/K),\mu_\infty)$ est un $\mathrm{Gal}(K/\mathbb{Q})$-module ; on munit $\mathbb{Q}_p/\mathbb{Z}_p$ d'une structure de $\mathrm{Gal}(K/\mathbb{Q})$-module en faisant agir $\mathrm{Gal}(K/\mathbb{Q})$ trivialement, cela permet de munir $K^*\otimes(\mathbb{Q}_p/\mathbb{Z}_p)$ d'une structure de $\mathrm{Gal}(K/\mathbb{Q})$-module. On a :

PROPOSITION 6.2. <u>L'isomorphisme</u> φ <u>est un isomorphisme de</u> $\mathrm{Gal}(K/\mathbb{Q})$-module <u>de</u> $K^*\otimes(\mathbb{Q}_p/\mathbb{Z}_p)$ <u>sur</u> $\mathrm{Hom}_{cont}(\mathrm{Gal}(\tilde{K}/K),\mu_\infty)$.

<u>Démonstration</u>. Pour chaque $n\in\mathbb{N}$, l'isomorphisme φ_n de $K^*/(K^*)^{p^{n+1}}$ vers $\mathrm{Hom}_{cont}(\mathrm{Gal}(\tilde{K}/K),\mu_n)$ est un isomorphisme de $\mathrm{Gal}(K/\mathbb{Q})$-module : en effet, si $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$, $\tau\in\mathrm{Gal}(\tilde{K}/K)$ et $\alpha\in K^*$, on a $[\varphi_n(\sigma(\alpha))](\tau) = \dfrac{\tau\left(\sqrt[p^n]{\sigma(\alpha)}\right)}{\sqrt[p^{n+1}]{\sigma(\alpha)}} = \dfrac{\tau\tilde{\sigma}\left(\sqrt[p^{n+1}]{\alpha}\right)}{\tilde{\sigma}\left(\sqrt[p^{n+1}]{\alpha}\right)}$ si $\tilde{\sigma}$ est un prolongement de σ à $\tilde{K}$; on a donc $[\varphi_n(\sigma(\alpha))](\tau) = \tilde{\sigma}\,\dfrac{\tilde{\sigma}^{-1}\,\tau\,\tilde{\sigma}\left(\sqrt[p^{n+1}]{\alpha}\right)}{\sqrt[p^{n+1}]{\alpha}} = \tilde{\sigma}\left\{[\varphi_n(\alpha)](\sigma^{-1}.\tau)\right\}$ c'est-à-dire $\varphi_n(\sigma(\alpha)) = [\sigma.\varphi_n](\alpha)$, ce qui prouve notre assertion relative à φ_n. On conclut alors en remarquant que l'isomorphisme de $K^*/(K^*)^{p^m}$ sur $K^*\otimes(\frac{1}{p^m}\mathbb{Z}/\mathbb{Z})$ est un isomorphisme de $\mathrm{Gal}(K/\mathbb{Q})$-module et en passant à la limite inductive.

COROLLAIRE 6.3. 1) V <u>est un</u> <u>sous</u>-$\mathrm{Gal}(K/\mathbb{Q})$-<u>module</u> <u>de</u> $K^*\otimes\mathbb{Q}_p/\mathbb{Z}_p$.

2) <u>L'isomorphisme</u> ψ (proposition 6.1) <u>est un isomorphisme</u> <u>de</u> $\mathrm{Gal}(K/\mathbb{Q})$-module.

<u>Démonstration</u>. 1) Claire.

2) Pour tout $w\in K^*\otimes\mathbb{Q}_p/\mathbb{Z}_p$ et tout $\tau\in\mathrm{Gal}(\tilde{K}/K)$, posons $\langle w,\tau\rangle = [\varphi(w)](\tau)$; la proposition précédente montre que $\langle\ ,\ \rangle$ est une application bilinéaire de $(K^*\otimes\mathbb{Q}_p/\mathbb{Z}_p)\times\mathrm{Gal}(\tilde{K}/K)$ vers μ_∞ qui vérifie $\langle\sigma.w\,,\,\sigma.\tau\rangle = \sigma.\langle w,\tau\rangle$ pour tout $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$, $w\in K^*\otimes\mathbb{Q}_p/\mathbb{Z}_p$, $\tau\in\mathrm{Gal}(\tilde{K}/K)$. L'application $\langle\ ,\ \rangle$ induit donc une application de $V\times\mathrm{Gal}(M/K)$ vers μ_∞ qui vérifie $\langle\sigma.v\,,\,\sigma.\tau\rangle = \sigma.\langle v,\tau\rangle$ pour tout $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$, $v\in V$ et $\tau\in\mathrm{Gal}(M/K)$. Par définition de ψ, on a $[\psi(\tau)](v) = \langle v,\tau\rangle$, donc l'égalité précédente montre que ψ est un homomorphisme de $\mathrm{Gal}(K/\mathbb{Q})$-module de $\mathrm{Gal}(M/K)=X$ vers $\mathrm{Hom}(V,\mu_\infty)$; cela achève la démonstration puisque l'on a déjà vu (proposition 6.1) que ψ est un isomorphisme.

Introduisons le module de Tate :

DEFINITION 6.4. 1) <u>On appelle module de Tate et on note</u> T_p <u>le</u> $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-<u>module qui est la limite projective des</u> $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-<u>modules</u> μ_n, <u>les flèches des</u> μ_{n+1} <u>vers les</u> μ_n <u>étant l'élévation à la puissance</u> p.

2) <u>Si</u> $\mathfrak{a}$ <u>est un</u> $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-<u>module, on note</u> $\mathfrak{a}(1)$ (resp. $\mathfrak{a}(-1)$) <u>le</u> $\mathbb{Z}_p$-<u>module</u> $\mathfrak{a}\otimes_{\mathbb{Z}_p} T_p$ (resp. $\mathrm{Hom}_{\mathbb{Z}_p}(T_p,\mathfrak{a})$) <u>muni de la structure de</u> $\mathrm{Gal}(K/\mathbb{Q})$-<u>module défini ci-dessus</u>.

Rappelons que $\varkappa$ est l'isomorphisme de $\mathrm{Gal}(K/\mathbb{Q})$ sur $\mathbb{Z}_p^*$ défini de la manière suivante : pour tout $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$, $\varkappa(\sigma)$ est l'élément de $\mathbb{Z}_p^*$ tel que l'action de σ sur μ_∞ est l'élévation à la puissance $\varkappa(\sigma)$; on a :

LEMME 6.5. 1) <u>Soit</u> $\mathfrak{a}$ <u>un</u> $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-<u>module ; pour tout</u> $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$, <u>on note</u> $\sigma.a$ <u>le résultat de l'action de</u> σ <u>sur</u> a. <u>Le module</u> $\mathfrak{a}(1)$ (resp. $\mathfrak{a}(-1)$) <u>est isomorphe au</u> $\mathbb{Z}_p$-<u>module</u> $\mathfrak{a}$ <u>muni de l'action de</u> $\mathrm{Gal}(K/\mathbb{Q})$ <u>définie de la manière suivante : le résultat de l'action de</u> $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$ <u>sur</u> $a\in\mathfrak{a}$ <u>est</u> $\varkappa(\sigma)(\sigma.a)$ (resp. $\varkappa(\sigma)^{-1}(\sigma.a)$).

2) <u>Pour tout</u> $\mathbb{Z}_p[\mathrm{Gal}(K/Q)]$-<u>module</u> $\mathfrak{a}$, <u>les modules</u> $[\mathfrak{a}(1)](-1)$ <u>et</u> $[\mathfrak{a}(-1)](1)$ <u>sont isomorphes à</u> $\mathfrak{a}$ <u>en tant que</u> $\mathbb{Z}_p[\mathrm{Gal}(K/Q)]$-<u>modules</u>.

<u>Démonstration</u>. 1) Pour chaque $n\in\mathbb{N}$, on choisit une racine de l'unité ζ_n d'ordre p^n de sorte que $\zeta_n^p=\zeta_{n-1}$ si $n\geqslant 1$. Il est clair que $\zeta=(\zeta_n)_{n\in\mathbb{N}}$ est une base du $\mathbb{Z}_p$-module T_p. Désignons par φ l'application de $\mathfrak{a}\otimes_{\mathbb{Z}_p} T_p$ (resp. $\mathrm{Hom}_{\mathbb{Z}_p}(T_p,\mathfrak{a})$) qui à $a\otimes\zeta^x$ (resp. à f) associe $\varphi(a\otimes\zeta)=x.a$ (resp. $\varphi(f)=f(\zeta)$) ; il est clair que φ est un isomorphisme de $\mathbb{Z}_p$-module et que l'action de $\mathrm{Gal}(K/\mathbb{Q})$ sur $\mathfrak{a}$ image de l'action de $\mathrm{Gal}(K/\mathbb{Q})$ sur $\mathfrak{a}\otimes_{\mathbb{Z}_p} T_p=\mathfrak{a}(1)$ (resp. $\mathrm{Hom}_{\mathbb{Z}_p}(T_p,\mathfrak{a})=\mathfrak{a}(-1)$) est l'action décrite dans l'énoncé du lemme ; cela prouve notre première assertion.

2) Résulte clairement de 1).

Les structures de $\mathbb{Z}_p$-modules de $\mathbb{Q}_p/\mathbb{Z}_p$ et de μ_∞ permettent de munir les groupes $\mathrm{Hom}(V,\mu_\infty)$ et $\mathrm{Hom}(V,\mathbb{Q}_p/\mathbb{Z}_p)$ de structures de $\mathbb{Z}_p$-modules ; ces structures sont compatibles avec les actions du groupe $\mathrm{Gal}(K/\mathbb{Q})$ sur chacun de ces groupes et on a :

PROPOSITION 6.6. <u>Les</u> $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-<u>modules</u> $[\mathrm{Hom}(V,\mathbb{Q}_p/\mathbb{Z}_p)](1)$ <u>et</u> $\mathrm{Hom}(V,\mu_\infty)$ <u>sont isomorphes</u>.

<u>Démonstration</u>. Soit φ l'application de $\mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}_p} T_p$ vers μ_∞ définie de la manière suivante : si $\frac{i}{p^n} \in \mathbb{Q}_p/\mathbb{Z}_p = \bigcup_{k\in\mathbb{N}} \frac{1}{p^k}\mathbb{Z}_p$ et si $\eta = (\eta_k)_{k\in\mathbb{N}} \in T_p$, on pose $\varphi(\frac{i}{p^n}\otimes\eta) = \eta_n^i$ (qui ne dépend pas du n choisi pour représenter l'élément $\frac{i}{p^n}$ de $\mathbb{Q}_p/\mathbb{Z}_p$) ; il est clair que φ est un isomorphisme de $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-module. On définit alors l'application Φ de $\mathrm{Hom}(V,\mathbb{Q}_p/\mathbb{Z}_p)(1)$ vers $\mathrm{Hom}(V,\mu_\infty)$ de la manière suivante : si $f\in\mathrm{Hom}(V,\mathbb{Q}_p/\mathbb{Z}_p)$ et $\eta\in T_p$, alors $\Phi(f\otimes\eta)$ est l'élément de $\mathrm{Hom}(V,\mu_\infty)$ qui à $v\in V$ associe $[\Phi(f\otimes\eta)](v) = \varphi(f(v)\otimes\eta)$. Il est clair que Φ est un isomorphisme de $\mathbb{Z}_p$-module. Enfin, pour tout $v\in V$, on a $\{\sigma.[\Phi(f\otimes\eta)\}(v) = \sigma.\varphi(f(\sigma^{-1}(v))\otimes\eta) = \varphi(f(\sigma^{-1}(v))\otimes\sigma(\eta)) = [\Phi(\sigma.f\otimes\sigma(\eta))](v)$ ce qui montre que Φ est compatible avec l'action de $\mathrm{Gal}(K/\mathbb{Q})$ et achève la démonstration.

Rappelons que Δ désigne l'unique sous-groupe cyclique d'ordre p-1 de $\mathrm{Gal}(K/\mathbb{Q})$ et que χ désigne le caractère de Δ égal à la restriction de $\varkappa$. Tout $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-module $\mathfrak{a}$ est un $\mathbb{Z}_p[\Delta]$-module ; si $\mathfrak{a}$ est un tel module et si $i\in\mathbb{Z}$, on rappelle que $\mathfrak{a}^{(i)} = e_i\mathfrak{a}$ où $e_i = \frac{1}{p-1}\sum_{\tau\in\Delta}\chi^i(\tau)\tau^{-1}$ de sorte que $\mathfrak{a} = \bigoplus_{i=1}^{p-1}\mathfrak{a}^{(i)}$; on vérifie sans mal que chaque $\mathfrak{a}^{(i)}$ est un sous $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-module de $\mathfrak{a}$. Nous aurons besoin du lemme suivant :

LEMME 6.7. <u>Soit</u> $\mathfrak{a}$ <u>un</u> $\mathbb{Z}_p[\mathrm{Gal}(K/Q)]$-<u>module</u> ; <u>pour tout</u> $i\in\mathbb{Z}$, <u>les</u> $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-<u>modules</u> $[\mathfrak{a}(1)]^{(i)}$ <u>et</u> $\mathfrak{a}^{(i-1)}(1)$ <u>sont isomorphes</u>.

Démonstration. Le lemme 6.5 montre que $\mathcal{A}(1)$ est le $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-module dont le $\mathbb{Z}_p$-module sous-jacent est $\mathcal{A}$ et qui est muni de l'action de $\mathrm{Gal}(K/\mathbb{Q})$ suivante : si $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ et si $a \in \mathcal{A}$, le résultat de l'action de σ sur a est $\kappa(\sigma)(\sigma.a)$ si $\sigma.a$ est le résultat de l'action de σ sur a dans $\mathcal{A}$. On sait que $[\mathcal{A}(1)]^{(i)}$ est l'ensemble des éléments de $\mathcal{A}(1)$ sur lesquels l'action d'un $\tau \in \Delta$ est l'élévation à la puissance $\chi^i(\tau) = \kappa^i(\tau)$; en conséquence le sous-$\mathbb{Z}_p$-module de $\mathcal{A}$ sous-jacent à $[\mathcal{A}(1)]^{(i)}$ est $\mathcal{A}^{(i-1)}$ et l'action d'un $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ sur $\mathcal{A}^{(i-1)}$ est celle décrite ci-dessus ; le lemme 6.5 montre donc que $[\mathcal{A}(1)]^{(i)}$ est le $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-module $[\mathcal{A}^{(i-1)}](1)$, C.Q.F.D.

On a :

PROPOSITION 6.8. <u>Pour tout</u> $i \in \mathbb{Z}$, <u>les</u> $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-<u>modules</u> $X^{(i)}(-1)$ <u>et</u> $\mathrm{Hom}(V^{(1-i)}, \mathbb{Q}_p/\mathbb{Z}_p)$ <u>sont isomorphes</u>.

Démonstration. L'isomorphisme ψ étant un isomorphisme de $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-module (corollaire 6.3, 2)), il induit pour chaque $i \in \mathbb{Z}$ un isomorphisme de $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-module de $X^{(i)}$ sur $(\mathrm{Hom}(V,\mu_\infty))^{(i)}$. La proposition 6.6 montre que $(\mathrm{Hom}(V,\mu_\infty))^{(i)}$ est isomorphe à $\left\{[\mathrm{Hom}(V,\mathbb{Q}_p/\mathbb{Z}_p)](1)\right\}^{(i)}$ donc (lemme 6.7) à $\left[\mathrm{Hom}(V,\mathbb{Q}_p/\mathbb{Z}_p)^{(i-1)}\right](1)$. Mais $\mathrm{Hom}(V,\mathbb{Q}_p/\mathbb{Z}_p)^{(i-1)}$ est, comme on le vérifie facilement, isomorphe à $\mathrm{Hom}(V^{(1-i)},\mathbb{Q}_p/\mathbb{Z}_p)$ en tant que $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-module, donc $X^{(i)}$ est isomorphe à $\left[\mathrm{Hom}(V^{(i-1)},\mathbb{Q}_p/\mathbb{Z}_p)\right](1)$; on conclut alors à l'aide du lemme 6.5, 2).

Nous allons maintenant relier V et A. Pour cela nous adoptons les notations suivantes : pour tout $n \in \mathbb{N}$ et tout $\alpha \in K_n$, nous notons $(\alpha)'_n$ l'idéal $\prod_{\underline{\underline{q}} \neq \underline{\underline{p}}_n} \underline{\underline{q}}^{\mathrm{ord}_{\underline{\underline{q}}}(\alpha)}$ où $\underline{\underline{q}}$ décrit les idéaux premiers de K_n différents de $\underline{\underline{p}}_n$ (on rappelle que $\underline{\underline{p}}_n$ est l'idéal premier de K_n qui contient p) et où $\mathrm{ord}_{\underline{\underline{q}}}$ désigne la valuation de K_n associée à $\underline{q}$ et normalisée par $\mathrm{ord}_{\underline{q}}(K_n^*) = \mathbb{Z}$. De plus, si $\underline{a}$ est un idéal de K_n dont la classe a pour ordre une puissance de p, nous notons $Cl_n(\underline{a})$ cette classe ; $Cl_n(\underline{a})$ est donc un élément de A_n. Avec ces notations on a :

LEMME 6.9. 1) <u>Tout élément de</u> $K^* \otimes \mathbb{Q}_p/\mathbb{Z}_p$ <u>peut s'écrire sous la forme</u> $\alpha \otimes \frac{1}{p^n}$ <u>pour un</u> $\alpha \in K^*$; <u>de plus l'égalité</u> $\alpha \otimes \frac{1}{p^n} = \beta \otimes \frac{1}{p^m}$ <u>avec</u> $m \geqslant n$ <u>implique l'existence d'un</u> $\gamma \in K^*$ <u>tel que</u> $\alpha^{p^{m-n}} = \beta \gamma^{p^m}$.

2) <u>L'élément</u> $\alpha \otimes \frac{1}{p^n}$ <u>de</u> $K^* \otimes \mathbb{Q}_p/\mathbb{Z}_p$ <u>est dans</u> V <u>si et seulement si, pour tout entier</u> m <u>tel que</u> $\alpha \in K_m$ <u>et</u> $m \geqslant n-1$, <u>l'idéal</u> $(\alpha)'_m$ <u>est de la forme</u> $\underline{a}^{p^n}$ <u>pour un idéal</u> $\underline{a}$ <u>de</u> K_m.

<u>Démonstration</u>. Les éléments de $K^* \otimes \mathbb{Q}_p/\mathbb{Z}_p$ sont de la forme $\sum_{k=1}^{t} \alpha_k \otimes \frac{i(k)}{p^{n(k)}}$ avec $\alpha_k \in K^*$, $i(k) \in \mathbb{Z}$ et $n(k) \in \mathbb{N}$ pour $k = 1,\dots,t$; soit n un majorant de tous les $n(k)$ et soit $\alpha = \prod_{k=1}^{t} \alpha_k^{i(k)p^{n-n(k)}}$ on a $\alpha \otimes \frac{1}{p^n} = \sum_{k=1}^{t} \alpha_k \otimes \frac{i(k)}{p^{n(k)}}$, ce qui prouve notre première assertion. Pour la seconde, remarquons que $\alpha \otimes \frac{1}{p^n} = \alpha^{p^{m-n}} \otimes \frac{1}{p^m}$, donc il suffit de prouver notre assertion dans le cas où $m = n$. L'application de $K^*/(K^*)^{p^i}$ vers $K^*/(K^*)^{p^{i+1}}$ induite par l'élévation à la puissance p dans K^* est injective pour tout entier i : en effet, si $x^p = y^{p^{i+1}}$ pour x et y dans K^*, on a $x = \zeta\, y^{p^i}$ pour un ζ tel que $\zeta^p = 1$; dans K un tel ζ est une puissance p^i <u>ème</u>, donc x est dans $(K^*)^{p^i}$ ce qui prouve l'injectivité cherchée. On en déduit que, pour tout $n \geqslant 0$, l'application de $K^*/(K^*)^{p^n}$ dans $\varinjlim K^*/(K^*)^{p^i}$ est injective, i.e. que l'application de $K^* \otimes (\frac{1}{p^n} \mathbb{Z}/\mathbb{Z})$ dans $K^* \otimes Q_p/Z_p$ est injective. En conséquence $\alpha \otimes \frac{1}{p^n} = \beta \otimes \frac{1}{p^n}$ dans $K^* \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$ implique $\alpha \otimes \frac{1}{p^n} = \beta \otimes \frac{1}{p^n}$ dans $K^* \otimes (\frac{1}{p^n} \mathbb{Z}/\mathbb{Z})$. Enfin, cette dernière égalité implique que α et β ont la même image dans $K^*/(K^*)^{p^n}$ i.e. que $\alpha = \beta \gamma^{p^n}$ pour un $\gamma \in K^*$, cela achève notre démonstration.

2) Par définition de V, l'élément $\alpha\otimes\frac{1}{p^n}$ de $K^*\otimes(\mathbb{Q}_p/\mathbb{Z}_p)$ est dans V si et seulement si le corps $K(\sqrt[p^n]{\alpha})$ est inclus dans M. Soit m un entier positif ; l'extension K/K_m étant non ramifiée en dehors de $\underline{p}_m$, le corps $K(\sqrt[p^n]{\alpha})$ est inclus dans M si et seulement si l'extension $K_m(\sqrt[p^n]{\alpha})/K_m$ est non ramifiée en dehors de $\underline{p}_m$. Si m est tel que $\alpha\in K_m$ et $m \geqslant n-1$, cette dernière extension est une extension de Kummer ; elle est donc non ramifiée en dehors de $\underline{p}_m$ si et seulement si l'idéal $(\alpha)'_m$ est la puissance p^n $\underline{\text{ième}}$ d'un idéal de K_m, cela prouve notre assertion.

Soit v un élément de V et soient α et β deux éléments de K^* et n et m deux entiers tels que $v=\alpha\otimes\frac{1}{p^n}=\beta\otimes\frac{1}{p^m}$. Soient r et s deux entiers tels que $r\geqslant n$, $s\geqslant m$ et $\alpha\in K_r^*$, $\beta\in K_s^*$; le lemme 6.9, 2) montre que $(\alpha)'_r=\underline{a}^{p^n}$ et $(\beta)'_s=\underline{b}^{p^m}$ où $\underline{a}$ est un idéal de K_r et $\underline{b}$ un idéal de K_s. Du lemme 6.9, 1) on déduit que les deux éléments $cl_r(\underline{a})\in A_r$ et $cl_s(\underline{b})\in A_s$ définissent le même élément de $A=\varinjlim A_n$; en associant à v cet élément de A, on définit donc une application de V dans A que nous notons θ. Il est clair que θ est un morphisme de $\mathbb{Z}_p[\mathrm{Gal}(K/Q)]$-module ; de plus on a :

PROPOSITION 6.10. <u>Soit</u> $E=\bigcup_n E_n$ <u>où</u> E_n <u>est le groupe des unités de</u> K_n. <u>L'application</u> θ <u>définie ci-dessus s'insère dans la suite exacte de</u> $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-<u>module</u> <u>suivante</u> :

$$0\to E\otimes\mathbb{Q}_p/\mathbb{Z}_p\to V\xrightarrow{\theta} A\to 0,$$

<u>l'injection de</u> $E\otimes\mathbb{Q}_p/\mathbb{Z}_p$ <u>dans</u> V <u>étant le produit tensoriel de l'injection de</u> E <u>dans</u> K^* <u>par l'identité de</u> $\mathbb{Q}_p/\mathbb{Z}_p$.

<u>Démonstration</u>. En raisonnant comme dans la démonstration du lemme 6.9, 1), on voit que tout élément de $E\otimes\mathbb{Q}_p/\mathbb{Z}_p$ peut s'écrire sous

la forme $\alpha \otimes \frac{1}{p^n}$ pour un $\alpha \in E$ et un $n \in \mathbb{N}$; si l'image de $\alpha \otimes \frac{1}{p^n}$ dans $K^* \otimes \mathbb{Q}_p/\mathbb{Z}_p$ est l'élément neutre de ce groupe, le lemme 6.9, 1) montre que $\alpha = \beta^{p^n}$ pour un β de K^* ; cette égalité implique que $\beta \in E$, donc que $\alpha \otimes \frac{1}{p^n}$ est l'élément neutre de $E \otimes \mathbb{Q}_p/\mathbb{Z}_p$ ce qui prouve que l'application de $E \otimes \mathbb{Q}_p/\mathbb{Z}_p$ dans $K^* \otimes \mathbb{Q}_p/\mathbb{Z}_p$ est injective. De plus, si m est un entier tel que $m \geqslant n-1$ et $\alpha \in E_m$, alors l'idéal $(\alpha)'_m$ est l'élément neutre du groupe des idéaux de K_m donc est la puissance p^n $\underline{\text{ième}}$ d'un idéal ; le lemme 6.9, 2) montre donc que $\alpha \otimes \frac{1}{p^n}$ est dans V i.e. que notre injection envoie $E \otimes \mathbb{Q}_p/\mathbb{Z}_p$ dans V . Soient maintenant $v = \beta \otimes \frac{1}{p^n}$ un élément de V et m un entier tel que $m \geqslant n$ et $\beta \in K_m$; d'après le lemme 6.9, 2) l'idéal $(\beta)'_m$ est de la forme $\underline{b}^{p^n}$ pour un idéal $\underline{b}$ de K_m ; l'idéal $(\beta)_m$ engendré par β dans K_m est donc de la forme $\underline{\underline{p}}_m^x\, \underline{b}^{p^n}$ pour un $x \in \mathbb{Z}$. Par définition de θ , l'élément v est dans le noyau de θ si et seulement si $Cl_m(\underline{b}) \in A_m$ représente l'élément neutre de A i.e. si il existe un $r \geqslant m$ tel que l'idéal de K_r engendré par $\underline{b}$ est principal. Mais, l'idéal de K_r engendré par $\underline{\underline{p}}_m$ est $\underline{\underline{p}}_r^{p^{r-m}}$, donc en prenant $r \geqslant m+n$ et en se rappelant que $\underline{\underline{p}}_r$ est principal, on voit que v est dans le noyau de θ si et seulement si l'idéal de K_r engendré par β dans K_r est la puissance p^n $\underline{\text{ième}}$ d'un idéal principal de K_r ; il en est ainsi si et seulement si $\beta = u\gamma^{p^n}$ pour une unité u de K_r et un γ de K_r c'est-à-dire (lemme 6.9, 1)) si et seulement si $v = \beta \otimes \frac{1}{p^n} = u \otimes \frac{1}{p^n}$ i.e. si et seulement si v est dans l'image de $E \otimes \mathbb{Q}_p/\mathbb{Z}_p$ dans V . Pour achever la démonstration, il reste à voir que θ est surjectif : soient x un élément de A et n un entier tel que x est la classe dans A d'un $x_n \in A_n$; soit $\underline{a}$ un idéal de K_n premier à $\underline{\underline{p}}_n$ qui appartient à x_n et soit p^t l'ordre de x_n dans A_n ; l'idéal $\underline{a}^{p^t}$ est un idéal principal de K_n ; si α est un de ses générateurs on a

$\alpha\otimes\frac{1}{p^t}\in V$ par le lemme 6.9, 2) et $\theta(\alpha\otimes\frac{1}{p^t})=x$ par définition de θ ce qui prouve la surjectivité cherchée.

COROLLAIRE 6.11. <u>Si</u> $i\notin 2\mathbb{Z}$, <u>alors les</u> $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-<u>modules</u> $V^{(i)}$ <u>et</u> $A^{(i)}$ <u>sont isomorphes</u>.

<u>Démonstration</u>. Compte-tenu de la proposition précédente, il suffit de voir que $(E\otimes\mathbb{Q}_p/\mathbb{Z}_p)^{(i)}$ est trivial si $i\notin 2\mathbb{Z}$. Pour cela, désignons par σ la conjugaison complexe ; σ est dans Δ. Soit $e\otimes\frac{1}{p^n}$ un élément de $E\otimes\mathbb{Q}_p/\mathbb{Z}_p$; on a $\sigma(e\otimes\frac{1}{p^n}) = \sigma(e)\otimes\frac{1}{p^n}$. Il existe un entier $m\geqslant 0$ tel que e est une unité de K_m, donc (§0, propositions 0.9 et 0.12) $e=\eta f$ où η est dans μ_m et où f est une unité du sous-corps réel maximal de K_m. On a $e\otimes\frac{1}{p^n} = f\otimes\frac{1}{p^n}$ (puisque $\eta\otimes\frac{1}{p^n} = \eta^{p^m}\otimes\frac{1}{p^{n+m}} = 1\otimes\frac{1}{p^{n+m}}$ est l'élément neutre de $E\otimes\mathbb{Q}_p/\mathbb{Z}_p$) et donc $\sigma.(e\otimes\frac{1}{p^n}) = \sigma(f)\otimes\frac{1}{p^n} = f\otimes\frac{1}{p^n} = e\otimes\frac{1}{p^n}$. Si $i\notin 2\mathbb{Z}$, on a $\chi^i(\sigma)=-1$, donc pour que $e\otimes\frac{1}{p^n}$ appartienne à $(E\otimes\mathbb{Q}_p/\mathbb{Z}_p)^{(i)}$ il est nécessaire que $e\otimes\frac{1}{p^n}$ soit égal à son inverse ; comme p est supposé impair, cela implique que $e\otimes\frac{1}{p^n}$ est l'élément neutre ce qui achève la démonstration.

La juxtaposition de ce corollaire 6.11 et de la proposition 6.8 donne le théorème suivant :

THEOREME 6.12. <u>Si</u> $i\in 2\mathbb{Z}$, <u>les</u> $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-<u>modules</u> $X^{(i)}(-1)$ <u>et</u> $\mathrm{Hom}(A^{(1-i)},\mathbb{Q}_p/\mathbb{Z}_p)$ <u>sont isomorphes</u>.

§7. UNE CONJECTURE.

Pour chaque entier $n \in \mathbb{N}$, la surjection canonique de $\Gamma = \mathrm{Gal}(K/K_o)$ sur Γ/Γ_n induit un homomorphisme surjectif de $\mathbb{Z}_p[\Gamma]$ sur $\mathbb{Z}_p[\Gamma/\Gamma_n]$; on a donc un homomorphisme canonique de $\mathbb{Z}_p[\Gamma]$ dans $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$ dont l'image est dense ; on vérifie que cet homomorphisme est injectif. Choisissons un $\mathbb{Z}_p$-générateur γ de Γ ; on sait (proposition 3.4) que cela permet d'identifier $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$ avec Λ et donc de définir un homomorphisme injectif de $\mathbb{Z}_p[\Gamma]$ dans Λ dont l'image est dense. Ainsi, tout Λ-module peut être regardé comme un $\mathbb{Z}_p[\Gamma]$-module. Dans l'autre sens on vérifie facilement que, si $\mathfrak{a}$ est un $\mathbb{Z}_p[\Gamma]$-module muni d'une topologie de groupe complet telle que l'application de $\Gamma \times \mathfrak{a}$ vers $\mathfrak{a}$ est continue, alors on peut prolonger par continuité l'action de $\mathbb{Z}_p[\Gamma]$ sur $\mathfrak{a}$ en une action de Λ sur $\mathfrak{a}$ qui fait de $\mathfrak{a}$ un Λ-module. En particulier on munit ainsi $\mathrm{Hom}(A^{(1-i)}, \mathbb{Q}_p/\mathbb{Z}_p)$ ($A^{(1-i)}$ est muni de la topologie discrète et $\mathrm{Hom}(A^{(1-i)}, \mathbb{Q}_p/\mathbb{Z}_p) \simeq \mathrm{Hom}(A^{(1-i)}, \mu_\infty)$ de la topologie duale au sens de Pontrjagin qui est compacte) et $X^{(i)}$ d'une structure de Λ-module. Enfin on rappelle que, pour $i = 2, 4, \ldots, p-3$, on a noté $g_i(T)$ la série de Λ telle que $g_i(\kappa(\gamma)^{-s}-1) = L_p(s, \omega^i)$ pour tout $s \in \mathbb{Z}_p$.

Dans une situation plus générale que celle étudiée ici, Iwasawa d'abord puis Coates [4] ont conjecturé l'existence de liens entre les "modules d'Iwasawa" (attachés à des classes d'idéaux) et des fonctions L p-adiques. Dans le cas qui nous intéresse, une forme forte de ces conjectures est la suivante :

CONJECTURE 7.1. Pour $i=2,4,\dots,p-3$, le Λ-module $\mathrm{Hom}(A^{(1-i)},\mathbb{Q}_p/\mathbb{Z}_p)$ est isomorphe au Λ-module $\Lambda/(g_i(T))$.

Posons $F_i(T) = g_i\left(\frac{1+T}{\kappa(\gamma)} - 1\right)$. L'application qui à T associe $\frac{1+T}{\kappa(\gamma)} - 1$ induit un isomorphisme de $\mathbb{Z}_p$-module de $\Lambda/(g_i(T))$ sur $\Lambda/(F_i(T))$; à travers cet isomorphisme la multiplication par $\kappa(\gamma)(1+T)$ dans $\Lambda/(g_i(T))$ correspond à la multiplication par $1+T$ dans $\Lambda/(F_i(T))$. Ceci joint au lemme 6.5 montre que la conjecture 7.1 est équivalente à l'assertion suivante : pour $i=2,4,\dots,p-3$, les $\mathbb{Z}_p[\Gamma]$-modules $[\mathrm{Hom}(A^{(1-i)},\mathbb{Q}_p/\mathbb{Z}_p)](1)$ et $\Lambda/(F_i(T))$ sont isomorphes. Mais alors le théorème 6.12 montre que la conjecture 7.1 est équivalente à :

CONJECTURE 7.2. Pour $i=2,4,\dots,p-3$, le Λ-module $X^{(i)}$ est isomorphe au Λ-module $\Lambda/F_i(T)$.

Enfin, le théorème 3.7 montre que cette conjecture est équivalente à la suivante :

CONJECTURE 7.3. Pour $i=2,4,\dots,p-3$, le Λ-module $X^{(i)}$ est isomorphe à $\varprojlim(U_n^{(i)}/\bar{C}_n^{(i)})$.

Nous allons montrer un résultat qui se rapproche de la conjecture 7.3. Pour chaque entier $n\in\mathbb{N}$, notons L_n la p-extension abélienne maximale non ramifiée de K_n ; posons $Z_n = \mathrm{Gal}(M_n/L_n)$, $Z = \varprojlim \mathrm{Gal}(M_n/L_n)$ (les flèches étant les restrictions des automorphismes) et $L = \bigcup_n L_n$ de sorte que Z s'identifie à $\mathrm{Gal}(M/L)$. De plus désignons par $E_{n,1}$ le sous-groupe du groupe des unités de K_n formé des unités congrues à 1 modulo $\underline{p}_n$ et par $\bar{E}_{n,1}$ l'adhérence de $E_{n,1}$ dans U_n . Si $m\geqslant n$ l'application $N_{m,n}$ de U_m vers U_n (on rappelle que $N_{m,n}$ désigne la norme dans l'extension locale Φ_m/Φ_n où Φ_j est le complété de K_j en $\underline{p}_j$) envoie $\bar{E}_{m,1}$ dans

$\bar{E}_{n,1}$ donc induit une application de $U_m/\bar{E}_{m,1}$ vers $U_n/\bar{E}_{n,1}$. On note $\varprojlim(U_n/\bar{E}_{n,1})$ la limite projective des $U_n/\bar{E}_{n,1}$ pour les flèches induites par les $N_{m,n}$; il est clair que cette limite projective est un $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-module et on a :

PROPOSITION 7.4. Les $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-module Z et $\varprojlim(U_n/\bar{E}_{n,1})$ sont isomorphes.

Avant de démontrer cette proposition, donnons le corollaire évident suivant qui se rapproche de la conjecture 7.3 (nous verrons plus loin que, si $p \nmid h_o^+$, ce corollaire implique la conjecture 7.3).

COROLLAIRE 7.5. Pour tout $i \in \mathbb{Z}$, les Λ-modules $Z^{(i)}$ et $\varprojlim(U_n^{(i)}/\bar{E}_{n,1}^{(i)})$ sont isomorphes.

Démonstration de la proposition 7.4. Pour chaque entier $n \in \mathbb{N}$ on note $\mathfrak{J}_n$ le groupe des idèles de K_n et j_n l'injection canonique de Φ_n^* (on rappelle que Φ_n est le complété de K_n en $\underline{p}_n$) dans $\mathfrak{J}_n$. Le groupe d'inertie de $\underline{p}_n$ dans M_n/K_n étant $\mathrm{Gal}(M_n/L_n)$, l'application d'Artin de $\mathfrak{J}_n$ vers $\mathrm{Gal}(M_n/K_n)$ induit une surjection θ_n de $j_n(U_n)$ sur $\mathrm{Gal}(M_n/L_n)$; nous allons montrer que le noyau de θ_n est $j_n(\bar{E}_{n,1})$. Pour cela notons, pour chaque entier $i > 0$, par $K_n(\underline{p}_n^i)$ le corps de rayon $\underline{p}_n^i$ sur K_n et posons $M_n' = \bigcup_{i>0} K_n(\underline{p}_n^i)$. Il est clair que M_n est la plus grande p-extension de K_n contenue dans M_n ; en conséquence, le groupe $j_n(U_n)$ étant un p-groupe, l'image d'un élément de $j_n(U_n)$ par l'application d'Artin dans $\mathrm{Gal}(M_n'/K_n)$ est triviale si et seulement si son image par l'application d'Artin dans $\mathrm{Gal}(M_n/K_n)$ est triviale. Pour chaque entier $i > 0$, posons $W_n^i = U_n^i . \prod_{v \neq \underline{p}_n} U_{n,v}$ où U_n^i est le sous-groupe de U_n formé des éléments congrus à 1 modulo $\hat{\underline{p}}_n^i$ ($\hat{\underline{p}}_n$ étant l'idéal maximal de Φ_n), où v décrit les places de K_n différentes de $\underline{p}_n$ et où, pour chaque v, le groupe $U_{n,v}$ est le groupe des unités du complété de K_n en v. On sait que $K_n^* W_n^i$ est le noyau de l'application d'Artin de $\mathfrak{J}_n$ vers $\mathrm{Gal}(K_n(\underline{p}_n^i)/K_n)$, donc $\bigcap_{i>0} (K^* W_n^i)$ est le noyau de l'application d'Artin vers $\mathrm{Gal}(M_n'/K_n)$. Il en résulte que le noyau de θ_n est $j_n(U_n) \cap (\bigcap_{i>0} (K^* W_n^i)$; nous allons montrer le lemme suivant :

LEMME 7.6. <u>On a</u> $j_n(\bar{E}_{n,1}) = j_n(U_n) \cap (\bigcap_{i>0} K^* W_n^i)$.

Avant de démontrer ce lemme, voyons comment il permet d'achever la démonstration de notre proposition. Le groupe U_n étant compact, l'injection continue j_n induit un isomorphisme de $U_n/\bar{E}_{n,1}$ sur $j_n(U_n)/j_n(\bar{E}_{n,1})$; le lemme 7.6 montre alors que la surjection θ_n induit un isomorphisme de $U_n/\bar{E}_{n,1}$ sur $\mathrm{Gal}(M_n/L_n)$. Les propriétés de l'application d'Artin montrent que ces isomorphismes entre les $U_n/\bar{E}_{n,1}$ et les $\mathrm{Gal}(M_n/L_n)$ sont des isomorphismes de $\mathrm{Gal}(K/\mathbb{Q})$-modules et qu'ils définissent un isomorphisme entre le système projectif des $U_n/\bar{E}_{n,1}$ et celui des $\mathrm{Gal}(M_n/L_n)$; notre proposition est donc démontrée à condition de démontrer le lemme 7.6.

<u>Démonstration du lemme</u> 7.6. Montrons d'abord que $j_n(\bar{E}_{n,1}) \subset j_n(U_n) \cap (\bigcap_{i>0} (K^* W_n^i))$. Soit $e \in E_{n,1}$, alors $j_n(e) = (e)x$ où (e) est l'idèle principale image de e et où x est l'idèle définie par $x_v = e^{-1}$ pour toute place v de K_n différente de $\underline{p}_n$ et $x_{\underline{p}_n} = 1$; l'idèle x est dans W_n^i pour tout i, donc $j_n(e)$ est dans $\bigcap_{i>0} (K^* W_n^i)$ ce qui montre que $j_n(E_{n,1}) \subset j_n(U_n) \cap (\bigcap_{i>0} (K^* W_n^i))$; mais $j_n(U_n) \cap (\bigcap_{i>0} K^* W_n^i)$ est fermé puisque c'est le noyau de θ_n, donc notre inclusion implique $j_n(\bar{E}_{n,1}) \subset j_n(U_n) \cap (\bigcap_{i>0} K^* W_n^i)$. Montrons maintenant $j_n(U_n) \cap (\bigcap_{i>0} (K^* W_n^i)) \subset j(\bar{E}_{n,1})$. Soit $u \in U_n$ tel que $j_n(u) \in \bigcap_{i>0} (K^* W_n^i)$; pour chaque i, il existe un $\alpha_i \in K^*$ et un $x_i \in W_n^i$ tels que $j_n(u) = (\alpha_i)x_i$ si (α_i) désigne l'idèle principale image de α_i ; une telle égalité implique d'une part que α_i est une v unité pour toute place finie v de K_n donc que α_i est une

unité de K_n et, d'autre part, que u est congrue à α_i modulo $\hat{\underline{\underline{p}}}_n^i$. Cela signifie que, dans U_n , l'élément u est la limite des α_i et donc prouve que $u \in \bar{E}_{n,1}$. Il en résulte que $j(U_n) \cap (\bigcap_{i>0} (K^* W_n^i)) \subset j(\bar{E}_{n,1})$ et cela achève la démonstration.

REMARQUE 7.7. Bien que ce soit inutile pour la suite, nous allons donner une description de Z différente de celle donnée dans la proposition 7.5. Pour tout $n \geqslant 0$, on a une suite exacte évidente $0 \to \mathrm{Gal}(M_n/KL_n) \to \mathrm{Gal}(M_n/L_n) \to \mathrm{Gal}(KL_n/L_n) \to 0$; l'extension K/K_n étant totalement ramifiée en $\underline{\underline{p}}_n$, on a $L_n \cap K = K_n$ ce qui implique $\mathrm{Gal}(KL_n/L_n) = \mathrm{Gal}(K/K_n)$; en conséquence $\varprojlim(\mathrm{Gal}(KL_n/L_n))$ est réduit à l'élément neutre et donc $\varprojlim(\mathrm{Gal}(M_n/L_n)) = \varprojlim(\mathrm{Gal}(M_n/KL_n))$. Notons U'_n le sous-groupe de U_n formé des éléments dont la norme sur $\mathbb{Q}_p$ vaut 1 ; on montre (exercice sur la théorie du corps de classe) que l'image du sous-groupe $U'_n/\bar{E}_{n,1}$ de $U_n/\bar{E}_{n,1}$ par l'isomorphisme décrit dans la démonstration précédente est le sous-groupe $\mathrm{Gal}(M_n/L_nK)$ de $\mathrm{Gal}(M_n/L_n)$. On a donc $\varprojlim(U'_n/\bar{E}_{n,1}) = \varprojlim(\mathrm{Gal}(M_n/L_nK))$ et donc $\varprojlim(U'_n/\bar{E}_{n,1}) = Z$.

Pour terminer ce paragraphe, nous allons montrer que, si p ne divise pas le nombre de classes h_o^+ du sous-corps réel maximal de K_o^+ , alors le corollaire 7.5 implique la conjecture sous sa forme 7.3. Pour ce faire, nous démontrerons que l'hypothèse $p \nmid h_o^+$ implique, pour tout $n \geqslant 0$, d'une part que $\bar{E}_{n,1} = \bar{C}_n$ et, d'autre part, que $\mathrm{Gal}(M_n/L_n)^{(i)} = \mathrm{Gal}(M_n/K_n)^{(i)}$ si i est pair. On aura alors d'une part $U_n/\bar{E}_{n,1} = U_n/\bar{C}_n$ pour tout $n \geqslant 0$, donc $\varprojlim(U_n^{(i)}/\bar{E}_{n,1}^{(i)}) = \varprojlim(U_n^{(i)}/\bar{C}_n^{(i)})$ pour tout i et, d'autre part, $Z^{(i)} = X^{(i)}$ si i est pair. Compte-tenu du corollaire 7.5, cela démontrera la conjecture 7.3 dans ce cas.

Rappelons tout d'abord le résultat suivant dû à Iwasawa :

PROPOSITION 7.8 (Iwasawa 1956). Soit E/F une extension cyclique dont le degré $[E:F]$ est une puissance de p . On suppose qu'il existe un seul idéal premier λ de F ramifié dans E/F et que λ est totalement ramifié dans E/F . Alors p divise le nombre de classes h_F de F si il divise le nombre de classes h_E de E .

Avant de démontrer ce théorème donnons en le corollaire qui sera utile dans la suite :

COROLLAIRE 7.9. Si p ne divise pas h_o^+ , alors p ne divise aucun des h_n^+ .

Démonstration de la proposition 7.8. On suppose que p divise h_E ; on sait alors que la p-extension maximale non ramifiée A de E est non triviale. L'extension A/F est galoisienne, nous notons G son groupe de Galois et N le sous-groupe $Gal(A/E)$ de G ; l'ordre de G est une puissance de p et N est un sous-groupe distingué de G . Rappelons le lemme de théorie des groupes suivant :

LEMME 7.10. Soit G un groupe fini dont l'ordre est une puissance de p et soit N un sous-groupe distingué non trivial de G . Alors, il existe un sous-groupe M de N qui est d'indice p dans N et qui est distingué dans G .

Démonstration. On raisonne par récurrence sur l'ordre de G . Si G est le groupe à p éléments, alors $N=G$ et $M=\{1\}$ répond à notre question. Sinon, notons $Z(G)$ le centre de G et montrons que $N \cap Z(G)$ est non trivial : G agit sur lui-même par conjugaison ; considérons les orbites de G pour cette action ; l'orbite d'un $x \in G$ est réduite à x si $x \in Z(G)$ et possède $p^{n(x)}$ éléments avec $n(x) > 0$ sinon ; le sous-groupe N étant distingué dans G , une orbite est soit inclue dans N soit disjointe de N ; enfin l'orbite de l'élément neutre étant réduite à l'élément neutre et N étant la réunion de ses orbites, il existe au moins $p-1$ orbites de N réduites à l'élément neutre donc au moins $p-1$ éléments de $Z(G)$ dans N. Choisissons alors un x différent de l'élément neutre dans $N \cap Z(G)$ et notons $\langle x \rangle$ le sous-groupe engendré par x. Le groupe $G/\langle x \rangle$ et son sous-groupe $N/\langle x \rangle$ vérifient les hypothèses de notre lemme, donc l'hypothèse de récurrence affirme l'existence d'un sous-groupe $\mathfrak{M}$ de $N/\langle x \rangle$ d'indice p dans $N/\langle x \rangle$ et distingué dans $G/\langle x \rangle$. Notons M le sous-groupe de N formé des éléments de N dont la classe module $\langle x \rangle$ est dans $\mathfrak{M}$; on vérifie sans mal que M est d'indice p dans N et distingué dans G ce qui achève la démonstration du lemme.

Revenons à la démonstration de la proposition 7.8. Soit M un sous-groupe de N d'indice p dans N et qui est distingué dans G (l'existence d'un tel groupe vient d'être démontrée) et soit A_o le sous-corps de A fixe par M. L'extension A_o/F est galoisienne et $Gal(A_o/E)$ est un sous-groupe distingué d'ordre p de $Gal(A_o/F)$. L'action par conjugaison du p-groupe $Gal(E/F)$ sur le groupe $Gal(A_o/E)$ est triviale (puisque le groupe des automorphismes de $Gal(A_o/E)$ est $(\mathbb{Z}/p\mathbb{Z})^*$ dont l'ordre est premier à p) ; le groupe $Gal(E/F)$ étant cyclique, on en déduit que $Gal(A_o/F)$ est abélien. Notons enfin $I_{\underline{\lambda}}$ le groupe d'inertie de $\underline{\lambda}$ dans A_o/F ; le groupe $I_{\underline{\lambda}}$ est d'ordre E/F, donc son corps des invariants B est de degré p sur F ; l'idéal $\underline{\lambda}$ est non ramifié dans B, donc aucun idéal premier de F ne se ramifie dans B. L'extension B/F étant abélienne il en résulte que p divise h_F, C.Q.F.D.

REMARQUE 7.11. Bien que ce soit inutile pour la suite, rappelons que si p divise h_o^+, alors p divise h_n^+ : en effet si p divise h_o^+, il existe une extension abélienne non ramifiée L_o^+ de degré p du sous-corps réel K_o^+ de K_o ; soit K_n^+ le sous-corps réel maximal de K_n, l'extension K_n^+/K_o^+ est totalement ramifiée au-dessus de p, donc $L_o^+K_n^+/K_n^+$ est une extension abélienne non ramifiée de degré p et donc p divise h_n^+. Cette remarque associée au corollaire 7.9 prouve que, pour tout $n \in \mathbb{N}$, on a l'équivalence $p \nmid h_o^+$ si et seulement si $p \nmid h_n^+$.

Montrons maintenant les deux propositions suivantes :

PROPOSITION 7.12. <u>Pour tout entier</u> $n \geqslant 0$, <u>on a</u> $\bar{E}_{n,1} = \bar{C}_n$ <u>si et seulement si</u> p <u>ne divise pas</u> h_n^+.

<u>Démonstration</u>. Rappelons (lemme 2.6 et proposition 2.8) que $h_n^+ = [E_n : \mathrm{Cycl}_n]$ et que $E_{n,1} = U_n \cap E_n$ et $C_n = U_n \cap \mathrm{Cycl}_n$; en conséquence, on a une injection de $E_{n,1}/C_n$ dans E_n/Cycl_n. L'élévation à la puissance $p-1$ envoie E_n dans $E_{n,1}$, donc les p parties de $E_{n,1}/C_n$ et de E_n/Cycl_n sont isomorphes. Mais $E_{n,1}/C_n$ est un p-groupe, donc on a $E_{n,1} = C_n$ si et seulement si p ne divise pas h_n^+. D'autre part, on a une surjection canonique de $E_{n,1} \otimes \mathbb{Z}_p$ sur $\bar{E}_{n,1}$; la proposition 3.1 montre que les $\mathbb{Z}_p$-modules $E_{n,1} \otimes \mathbb{Z}_p$ et $\bar{E}_{n,1}$ ont même $\mathbb{Z}_p$-rang, donc le noyau de notre surjection est un sous-$\mathbb{Z}_p$-module de torsion de $E_{n,1} \otimes \mathbb{Z}_p$. Mais le sous-$\mathbb{Z}_p$-module de torsion de $E_{n,1} \otimes \mathbb{Z}_p$ est $\mu_n \otimes \mathbb{Z}_p$ qui est cyclique d'ordre p^{n+1} ; son image est le sous-groupe μ_n de $\bar{E}_{n,1}$ qui est aussi cyclique d'ordre p^{n+1}, donc la restriction de notre surjection à ce sous-groupe de torsion est injective et donc notre surjection est un isomorphisme. L'anneau $\mathbb{Z}_p$ étant $\mathbb{Z}$-plat, $C_n \otimes \mathbb{Z}_p$ s'identifie à un sous-groupe de $E_{n,1} \otimes \mathbb{Z}_p$; l'image de ce sous-groupe par notre surjection est clairement $\bar{C}_n$, donc on a un isomorphisme de $(E_{n,1} \otimes \mathbb{Z}_p)/(C_n \otimes \mathbb{Z}_p)$ sur $\bar{E}_{n,1}/\bar{C}_n$. Enfin, toujours parce que $\mathbb{Z}_p$ est $\mathbb{Z}$-plat, on a un isomorphisme de $(E_{n,1} \otimes \mathbb{Z}_p)/(C_n \otimes \mathbb{Z}_p)$ sur $(E_{n,1}/C_n) \otimes \mathbb{Z}_p$, donc $\bar{E}_{n,1} = \bar{C}_n$ si et seulement si p ne divise pas $[E_{n,1} : C_n]$ i.e. si et seulement si $E_{n,1} = C_n$; comme on l'a remarqué

plus haut, il en est ainsi si et seulement si p ne divise pas h_n^+ et cela achève notre démonstration.

PROPOSITION 7.13. <u>Pour tout entier</u> $n \geqslant 0$ <u>et tout</u> $i \in 2\mathbb{Z}$, <u>on a</u> $\mathrm{Gal}(M_n/L_n)^{(i)} = \mathrm{Gal}(M_n/K_n)^{(i)}$ <u>si</u> p <u>ne divise pas</u> h_n^+.

<u>Démonstration</u>. De la suite exacte de $\mathbb{Z}_p[\mathrm{Gal}(K_n/\mathbb{Q})]$-module $0 \to \mathrm{Gal}(M_n/L_n) \to \mathrm{Gal}(M_n/K_n) \to \mathrm{Gal}(L_n/K_n) \to 0$ on tire, pour tout $i \in \mathbb{Z}$, la nouvelle suite exacte $0 \to \mathrm{Gal}(M_n/L_n)^{(i)} \to \mathrm{Gal}(M_n/K_n)^{(i)} \to \mathrm{Gal}(L_n/K_n)^{(i)} \to 0$. Le $\mathbb{Z}_p[\mathrm{Gal}(K_n/\mathbb{Q})]$-module $\mathrm{Gal}(L_n/K_n)$ étant isomorphe au $\mathbb{Z}_p[\mathrm{Gal}(K_n/\mathbb{Q})]$-module A_n (= p-groupe des classes de K_n), $\mathrm{Gal}(L_n/K_n)^{(i)}$ est isomorphe à $A_n^{(i)}$ pour tout $i \in \mathbb{Z}$. Mais le p-groupe des classes A_n^+ du sous-corps réel maximal K_n^+ de K_n est isomorphe à $\bigoplus_{i=2,4,\dots,p-1} A_n^{(i)}$, donc l'hypothèse p ne divise pas h_n^+ implique que $A_n^{(i)}$ est trivial pour tout $i \in 2\mathbb{Z}$ et donc que $\mathrm{Gal}(L_n/K_n)^{(i)}$ est trivial. Ce dernier point montre que, pour tout $i \in 2\mathbb{Z}$, on a $\mathrm{Gal}(M_n/L_n)^{(i)} = \mathrm{Gal}(M_n/K_n)^{(i)}$.

La juxtaposition du corollaire 7.9 et des propositions 7.12 et 7.13 montre que, si p ne divise pas h_o^+, alors $\bar{E}_{n,1} = \bar{C}_n$ et, pour tout $i \in 2\mathbb{Z}$, $\mathrm{Gal}(M_n/L_n)^{(i)} = \mathrm{Gal}(M_n/K_n)^{(i)}$; comme on l'a remarqué plus haut, cela implique le résultat suivant :

THEOREME 7.14. <u>La conjecture énoncée au début de ce paragraphe sous les 3 formes équivalentes</u> 7.1, 7.2 <u>et</u> 7.3 <u>est vraie si</u> p <u>ne divise pas</u> h_o^+.

§8. REMARQUES SUR LE Λ-MODULE A .

Pour tout $a \in \mathbb{Z}$ premier à p , on note σ_a l'élément de $G_n = \mathrm{Gal}(K_n/\mathbb{Q})$ dont l'action sur μ_n est l'élévation à la puissance a ; ainsi l'application qui à a associe σ_a induit un isomorphisme de $(\mathbb{Z}/p^{n+1}\mathbb{Z})^*$ sur G_n . On note Stick_n l'élément $\frac{1}{p^{n+1}}\left(\sum_{\substack{a=1\\(a,p)=1}}^{p^{n+1}} a.\sigma_a^{-1}\right)$ de $\mathbb{Q}[G_n]$. Dans ce paragraphe on conviendra de noter $[x]$ la partie entière d'un rationnel x et $\{x\}$ la différence $x-[x]$.

On a

LEMME 8.1. _Soit_ c _un élément de_ $\mathbb{Z}$ _premier à_ p ; _l'élément_ $(c-\sigma_c)\mathrm{Stick}_n$ _est dans_ $\mathbb{Z}[G_n]$.

Démonstration. On a $(c-\sigma_c)\mathrm{Stick}_n = \sum_{\substack{a=1\\(a,p)=1}}^{p^{n+1}} \frac{ac}{p^{n+1}}.\sigma_a^{-1} - \sum_{\substack{a=1\\(a,p)=1}}^{p^{n+1}} \frac{a}{p^{n+1}}.\sigma_a^{-1}\sigma_c$. Compte tenu de l'égalité $\sigma_a^{-1}\sigma_c = \sigma_{ac^{-1}}^{-1}$, on a
$$(c-\sigma_c)\mathrm{Stick}_n = \sum_{\substack{b=1\\(b,p)=1}}^{p^{n+1}} \left(\frac{bc}{p^{n+1}} - \left\{\frac{bc}{p^{n+1}}\right\}\right)\sigma_b^{-1}$$
; cela prouve notre assertion puisque $\frac{bc}{p^{n+1}} - \left\{\frac{bc}{p^{n+1}}\right\}$ est dans $\mathbb{Z}$.

Rappelons le théorème de Stickelberger :

THEOREME 8.2 (Stickelberger). _Pour tout_ c _de_ $\mathbb{Z}$ _premier à_ p , _l'élément_ $(c-\sigma_c)\mathrm{Stick}_n$ _annule le_ $\mathbb{Z}[G_n]$_-module_ A_n .

<u>Démonstration</u>. Voir [4], [6] par exemple.

Intéressons-nous plus spécialement au cas $n=0$. On a alors $G_o = \Delta$ et, pour chaque $i \in \mathbb{Z}$, on a noté $A_o^{(i)}$ le sous-$\mathbb{Z}_p[\Delta]$-module de A_o invariant par l'idempotent $\frac{1}{p-1} \sum_{\sigma\in\Delta} \chi^i(\sigma^{-1})\sigma$ que nous noterons e_i ; on a donc $A_o = \bigoplus_{i=1}^{p-1} A_o^{(i)}$. Le p-groupe des classes du sous-corps réel maximal K_o^+ de K_o s'identifie à $\bigoplus_{\substack{i=2\\ i \text{ pair}}}^{p-1} A_o^{(i)}$ et on pose $A_o^- = \bigoplus_{\substack{i=1\\ i \text{ impair}}}^{p-1} A_o^{(i)}$; ainsi $A_o = A_o^+ \oplus A_o^-$. D'autre part, si x est un rationnel, on note $(x)_p$ la puissance de p telle que $x = (x)_p y$ pour une p-unité y . Enfin, si X est un ensemble fini, on note $|X|$ le cardinal de X . On a :

LEMME 8.3. <u>Soit</u> h_o^- <u>le nombre de classes relatif de</u> K_o , <u>on a</u>

$$(h_o^-)_p = \prod_{\substack{i=1\\ i \text{ impair}}}^{p-2} |A_o^{(i)}| .$$

<u>Démonstration</u>. Par définition, $h_o^- = \frac{h_o}{h_o^+}$ si h_o et h_o^+ désignent respectivement le nombre de classes de K_o et le nombre de classes de K_o^+ . On a donc $(h_o^-)_p = \frac{(h_o)_p}{(h_o^+)_p}$ et notre lemme résulte des deux égalités $(h_o)_p = \prod_{i=1}^{p-1} |A_o^{(i)}|$ et $(h_o^+)_p = \prod_{\substack{i=2\\ i \text{ pair}}}^{p-1} |A_o^{(i)}|$.

Montrons comment le théorème 8.2 implique le résultat suivant :

PROPOSITION 8.4. <u>Soit</u> i <u>un entier tel que</u> $1 \leqslant i \leqslant p-1$; <u>pour tout</u> c <u>de</u> $\mathbb{Z}$ <u>premier à</u> p , <u>le groupe</u> $A_o^{(1-i)}$ <u>est annulé par</u> $(c-\omega^{1-i}(c))L(0,\omega^{i-1})$.

<u>Démonstration</u>. On sait que $A_o^{(1-i)}$ est l'image de A_o par la multiplication par e_{1-i} . Le théorème 8.2 montre donc que $A_o^{(1-i)}$ est annulé par $e_{1-i}((c-\sigma_c)\mathrm{Stick}_o)$. Pour tout $\sigma \in \Delta$, on a l'égalité

$\sigma.e_{1-i} = \chi^{1-i}(\sigma).e_{1-i}$; on en déduit que $e_{1-i}(c-\sigma_c) = (c-\omega^{1-i}(c))e_{1-i}$ et que $e_{1-i}.\mathrm{Stick}_o = \sum_{a=1}^{p} \frac{a}{p}.\omega^{i-1}(a)$; on a donc $e_{1-i}((c-\sigma_c)\mathrm{Stick}_o) = (c-\omega^{1-i}(c))(\sum_{a=1}^{p} \frac{a}{p}.\omega^{i-1}(a)) = -(c-\omega^{1-i}(c))L(0,\omega^{i-1})$ (avec les notations de la partie I). Il en résulte que $(c-\omega^{1-i}(c))L(0,\omega^{i-1})$ annule $A_o^{(1-i)}$, C.Q.F.D.

REMARQUE 8.5. Si i est impair, $L(0,\omega^{i-1}) = 0$ (comme nous l'avons vu dans la partie I) donc la proposition précédente n'a pas d'intérêt.

COROLLAIRE 8.6. <u>Soit</u> i <u>un entier pair tel que</u> $2 \leqslant i \leqslant p-1$; <u>le groupe</u> $A_o^{(1-i)}$ <u>est annulé par</u> $L(0,\omega^{i-1})$ <u>si</u> $i \neq p-1$ <u>et le groupe</u> $A_o^{(1)}$ <u>est trivial</u>.

<u>Démonstration</u>. Si $i \neq p-1$, on peut choisir c dans $\mathbb{Z}$ premier à p tel que $c-\omega^{1-i}(c)$ est une p-unité ; la première assertion de notre corollaire résulte donc de la proposition 8.4. D'autre part, si $i = p-1$, on voit en prenant $c = 1+p$ que $pL(0,\omega^{-1})$ annule $A_o^{(1)}$; la seconde assertion de notre corollaire résulte donc du lemme suivant :

LEMME 8.7. $pL(0,\omega^{-1})$ <u>est une</u> p-<u>unité</u>.

<u>Démonstration</u>. $pL(0,\omega^{-1}) = -\sum_{a=1}^{p-1} (a-\frac{p}{2})\omega^{-1}(a) = -\sum_{a=1}^{p-1} a\omega^{-1}(a)$ qui est congru à $-(p-1)$ modulo p donc est une p-unité.

Les propositions 0.8 et 0.12 montrent que

$$h_o^- = 2p \prod_{\substack{i=1 \\ i \text{ impair}}}^{p-2} (\tfrac{1}{2} L(0,\omega^i)) \quad \text{(on rappelle que } p \text{ est supposé impair).}$$

Compte tenu du lemme précédent, on en tire $(h_o^-)_p = \prod_{\substack{i=1 \\ i \text{ impair}}}^{p-4} (L(0,\omega^i))_p$

i.e. $(h_o^-)_p = \prod_{\substack{i=2 \\ i \text{ pair}}}^{p-3} (L(0,\omega^{i-1}))_p$. On conjecture parfois la propriété suivante :

CONJECTURE 8.8. Soit i un entier pair compris entre 2 et $p-3$, alors le groupe $A_o^{(1-i)}$ est isomorphe à $\mathbb{Z}_p/L(0,\omega^{i-1})\mathbb{Z}_p$ i.e. le groupe $A_o^{(1-i)}$ est cyclique d'ordre $(L(0,\omega^{i-1}))_p$.

En juxtaposant le lemme 8.3, le corollaire 8.6 et l'égalité $(h_o^-)_p = \prod_{\substack{i=2 \\ i \text{ pair}}}^{p-3} (L(0,\omega^{1-i}))_p$, on voit qu'il suffit de démontrer que les $A_o^{(1-i)}$ sont cycliques pour i pair compris entre 2 et $p-3$ pour avoir la conjecture 8.8. En particulier, si l'on savait que p ne divise pas h_o^+ (conjecture de Vandiver), on aurait $A_o^{(i)} = \{1\}$ pour tout i pair, donc (Spiegelungsatz de Léopoldt) $A_o^{(1-i)}$ cyclique pour tout i pair et donc la conjecture 8.8 serait démontrée.

Montrons que la conjecture du §7 implique la conjecture 8.8. Pour cela notons $\tilde{K}_{o,p}$ l'extension abélienne maximale de K_o dont le groupe de Galois est annulé par p et posons $M_{o,p} = M_o \cap \tilde{K}_{o,p}$. Notons η_o l'homomorphisme de $K_o^*/(K_o^*)^p$ vers $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\tilde{K}_{o,p}/K_o),\mu_p)$ qui à la classe de $\alpha \in K_o^*$ associe $\eta_o(\alpha)$ défini de la manière suivante : on choisit une racine $p^{\underline{\text{ième}}}$ de α et, pour tout $\tau \in \mathrm{Gal}(\tilde{K}_{o,p}/K_o)$, on pose $[\eta_o(\alpha)](\tau) = \dfrac{\tau(\sqrt[p]{\alpha})}{\sqrt[p]{\alpha}}$. On sait (théorie de Kummer) que η_o est un isomorphisme de $\mathbb{Z}_p[\Delta]$-module. Soit $V_{o,p}$ le sous-$\mathbb{Z}_p[\Delta]$-module de K_o^* tel que $\eta_o(V_{o,p}/(K_o^*)^p) = \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(M_{o,p}/K_o),\mu_p)$ et soit $A_{o,p}$ le sous-groupe de A_o formé des classes dont l'ordre divise p ; en raisonnant comme dans la démonstration de la proposition 6.10, on voit que l'on a une surjection de $Z_p[\Delta]$-module de $V_{o,p}/(K_o^*)^p$ sur $A_{o,p}$; pour tout entier i, on en déduit une surjection de $(V_{o,p}/(K_o^*)^p)^{(1-i)}$ sur $A_{o,p}^{(1-i)}$. On a donc une surjection de $(\mathrm{Hom}_{\mathrm{cont}}((\mathrm{Gal}(M_{o,p}/K_o),\mu_p))^{(1-i)}$ sur $A_{o,p}^{(1-i)}$, c'est-à-dire une surjection de $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(M_{o,p}/K_o)^{(i)},\mu_p)$ sur $A_{o,p}^{(1-i)}$.

D'autre part, en raisonnant comme dans la démonstration de la proposition 4.3, on montre que X_o est isomorphe à $X/\omega_o(T)X$ donc que $X_o^{(i)}$ est isomorphe à $X^{(i)}/\omega_o(T)X^{(i)}$. Admettons la conjecture du paragraphe 7 sous sa forme 7.2 ; pour $i=2,4,\ldots,p-3$, on a alors $X_o^{(i)} = \Lambda/(\omega_o(T),F_i(T)) = \mathbb{Z}_p/F_i(0)\mathbb{Z}_p$ ce qui montre que $X_o^{(i)}$ est cyclique ; en conséquence $(\mathrm{Gal}(M_{o,p}/K_o))^{(i)}$ qui est un quotient de $X_o^{(i)}$ est cyclique pour $i=2,4,\ldots,p-3$ et donc $\mathrm{Hom}_{\mathrm{cont}}((\mathrm{Gal}(M_{o,p}/K_o))^{(i)},\mu_p)$ est cyclique pour ces valeurs de i. Il en résulte que $A_{o,p}^{(1-i)}$, donc $A_o^{(1-i)}$ est cyclique pour $i=2,4,\ldots,p-3$ ce qu'on voulait.

Nous terminons ce paragraphe en démontrant la proposition suivante qui est une partie de la conjecture 7.1.

PROPOSITION 8.9. <u>Pour</u> $i=2,4,\ldots,p-3$, <u>le</u> Λ-<u>module</u> $\mathrm{Hom}(A^{(1-i)},\mathbb{Q}_p/\mathbb{Z}_p)$ <u>est annulé par la série</u> $g_i(T)$.

<u>Démonstration</u>. Choisissons un élément $C \in \hat{\mathbb{Z}}^*$ tel que $1 \neq \omega^i(C)$. On rappelle (I, §7, prop. 7.6, cor. 7.7) que $g_i(T) = \dfrac{f_i(T)}{1-\omega^i(C)\langle C\rangle(1+T)^{\alpha(C)}}$ où $\alpha(C)$ est défini par l'égalité $\langle C\rangle = \kappa(\gamma)^{\alpha(C)}$ (dans la partie I, γ désignait un générateur topologique de $1+p\mathbb{Z}_p$; dans la partie II, nous désignons par γ un générateur du groupe de Galois Γ, donc $\kappa(\gamma)$ est un générateur de $1+p\mathbb{Z}_p$). L'hypothèse $\omega^i(C) \neq 1$ implique que $1-\omega^i(C)\langle C\rangle$ est une unité dans $\mathbb{Z}_p$, donc que $1-\omega^i(C)\langle C\rangle(1+T)^{\alpha(C)}$ est inversible dans Λ. En conséquence, notre proposition est équivalente à l'assertion suivante :

pour $i=2,4,\ldots,p-3$, le Λ-module $\mathrm{Hom}(A^{(1-i)},\mathbb{Q}_p/\mathbb{Z}_p)$ est annulé par la série $f_i(T)$.

Nous démontrerons cette assertion en 3 étapes ; fixons quelques notations : on identifie Λ et $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$ en envoyant $1+T$ sur $(\gamma_n)_{n\in\mathbb{N}}$ où γ_n désigne la classe dans Γ/Γ_n du générateur γ de Γ ; on note $(f_{i,n})_{n\in\mathbb{N}}$ l'élément de $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$ correspondant à $f_i(T)$ dans cette identification ; pour chaque $n\in\mathbb{N}$, l'élément $f_{i,n}$ s'écrit de manière unique $\sum_{k=0}^{p^n-1} f_{i,n}^{(k)}\gamma_n^k$ avec $f_{i,n}^{(k)}\in\mathbb{Z}_p$ et on pose $f_{i,n}^* = \sum_{k=0}^{p^n-1} f_{i,n}^{(k)}\gamma_n^{-k}$.

1) Montrons que notre assertion est impliquée par l'assertion suivante : pour chaque $n\in\mathbb{N}$, le $\mathbb{Z}_p[\Gamma/\Gamma_n]$-module $A_n^{(1-i)}$ est annulé par $f_{i,n}^*$. Pour tout $\varphi\in \mathrm{Hom}(A_n^{(1-i)},\mathbb{Q}_p/\mathbb{Z}_p)$, on a $[f_{i,n}.\varphi](a) = \varphi(f_{i,n}^*.a)$ pour tout $a\in A_n^{(1-i)}$ (par la définition de la structure de $\mathbb{Z}_p[\Gamma/\Gamma_n]$-module de $\mathrm{Hom}(A_n^{(1-i)},\mathbb{Q}_p/\mathbb{Z}_p)$). En passant à la limite projective, on en déduit que $(f_{i,n})_{n\in\mathbb{N}}\in\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$ annule $\varprojlim(\mathrm{Hom}(A_n^{(1-i)},\mathbb{Q}_p/\mathbb{Z}_p))$ si les $f_{i,n}^*$ annulent les $A_n^{(1-i)}$; cela signifie que, dans ce cas, $f_i(T)$ annule le Λ-module $\varprojlim(\mathrm{Hom}(A_n^{(1-i)},\mathbb{Q}_p/\mathbb{Z}_p))$. On achève ce 1) en remarquant que l'isomorphisme canonique de $\varprojlim(\mathrm{Hom}(A_n^{(1-i)},\mathbb{Q}_p/\mathbb{Z}_p))$ sur $\mathrm{Hom}(\varinjlim(A_n^{(1-i)}),\mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}(A^{(1-i)},\mathbb{Q}_p/\mathbb{Z}_p)$ est un isomorphisme de Λ-module (il est clair que c'est un isomorphisme de $\mathbb{Z}_p[\Gamma]$-module ; nos deux Λ-modules étant des Λ-modules topologiques, on voit par continuité que notre isomorphisme est un isomorphisme de Λ-module).

2) Le calcul de $f_{i,n}^{(k)}$. Rappelons que $f_i(T)$ est la série associée à la mesure $\alpha_*\nu_{C,\omega^{i-1}}$, c'est-à-dire que $f_i(T) = \sum_{j=0}^{\infty} f_i^{(j)}T^j$ avec $f_i^{(j)} = \int_{\mathbb{Z}_p}\binom{x}{j}\,d(\alpha_*\nu_{C,\omega^{i-1}}(x))$. En explicitant l'isomorphisme de $\varprojlim(\mathbb{Z}_p[\Gamma/\Gamma_n])$ sur Λ (isomorphisme qui est décrit dans la démonstration de la proposition 3.4), on voit que $\sum_{k=0}^{p^n-1} f_{i,n}^{(k)}(1+T)^k$ est l'unique polynôme de degré strictement inférieur à p^n qui est

congru à $f_i(T)$ modulo $\omega_n(T)\Lambda$. Le lemme suivant montre donc que $f_{i,n}^{(k)} = \int_{\mathbb{Z}_p} \chi_{n,k}(x)\, d(\alpha_* \nu_{C,\omega^{i-1}})(x)$ où $\chi_{n,k}$ est la fonction caractéristique du sous-ensemble $k + p^n\mathbb{Z}_p$ de $\mathbb{Z}_p$.

LEMME 8.10. <u>Soient</u> ν <u>une mesure sur</u> $\mathbb{Z}_p$ <u>et</u> $F_\nu(T)$ <u>la série formelle qui lui est associée</u> (I, <u>définition</u> 4.3). <u>Soit</u> n <u>un entier positif ou nul ; pour chaque entier</u> k <u>tel que</u> $0 \leqslant k < p^n$, <u>on note</u> $\chi_{n,k}$ <u>la fonction caractéristique du sous-ensemble</u> $k + p^n\mathbb{Z}_p$ <u>de</u> $\mathbb{Z}_p$ <u>et</u> $a_n^{(k)}$ <u>l'intégrale</u> $\int_{\mathbb{Z}_p} \chi_{n,k}(x)\, d\nu(x)$. <u>Alors</u>, $\sum_{k=0}^{p^n-1} a_n^{(k)}(1+T)^k$ <u>est l'unique polynôme de degré strictement inférieur à</u> p^n <u>qui est congru à</u> $F_\nu(T)$ <u>modulo</u> $\omega_n(T)\Lambda$.

<u>Démonstration</u>. La proposition 3.5 (appliquée avec $g(T) = \omega_n(T)$) montre qu'il existe un unique polynôme $r(T)$ de degré strictement inférieur à p^{n+1} tel que $F_\nu(T) = \omega_n(T)Q(T) + r(T)$ pour un $Q(T) \in \Lambda$. L'assertion de notre lemme est donc équivalente à l'égalité $r(T) = \sum_{k=0}^{p^n-1} a_n^{(k)}(1+T)^k$. Pour montrer cette égalité entre polynôme de degré strictement inférieur à p^n , il suffit de montrer que ces polynômes prennent les mêmes valeurs pour p^n-1 éléments distincts ; nous terminerons donc notre démonstration en montrant que, pour toute racine p^{n} <u>ième</u> de l'unité ζ différente de 1 , on a $r(\zeta-1) = \sum_{k=0}^{p^n-1} a_n^{(k)}\, \zeta^k$. Le lemme 5.6 du §5 de la partie I montre que $F_\nu(\zeta-1) = \int_{\mathbb{Z}_p} \zeta^x\, d\nu(x)$; comme $\omega_n(\zeta-1) = (1+(\zeta-1))^{p^n} - 1 = 0$, on en déduit que $r(\zeta-1) = \int_{\mathbb{Z}_p} \zeta^x\, d\nu(x)$. Mais, pour tout $x \in \mathbb{Z}_p$, on a $\zeta^x = \sum_{k=0}^{p^n-1} \zeta^k \chi_{n,k}(x)$ donc $\int_{\mathbb{Z}_p} \zeta^x\, d\nu(x) = \sum_{k=0}^{p^n-1} \zeta^k \int_{\mathbb{Z}_p} \chi_{n,k}(x)\, d\nu(x) = \sum_{k=0}^{p^n-1} a_n^{(k)}\, \zeta^k$; en conséquence on a $r(\zeta-1) = \sum_{k=0}^{p^n-1} a_n^{(k)}\, \zeta^k$ et cela démontre notre lemme.

Revenons au point 2) de la démonstration de la proposition 8.9. Par définition de $\nu_{C,\omega^{i-1}}$ (I, §3) et de $\alpha_*\nu_{C,\omega^i}$ (I, §5) on a $\int_{\mathbb{Z}_p} \chi_{n,k}(x)d(\alpha_*\nu_{C,\omega^i})(x) = \int_{\mathbb{Z}_p} \varepsilon(x)d\mu_C(x)$ où $\varepsilon(x)$ est défini de la manière suivante : si $x \notin \mathbb{Z}_p^*$ alors $\varepsilon(x)=0$; si $x\in\mathbb{Z}_p^*$ alors $\varepsilon(x)=\omega^{i-1}(x)$ si $\alpha(x)\equiv k$ modulo $p^n\mathbb{Z}_p$ et $\varepsilon(x)=0$ sinon. Pour un $x\in\mathbb{Z}_p^*$, on a $\alpha(x)\equiv k$ modulo $p^n\mathbb{Z}_p$ si et seulement si $\langle x\rangle \equiv \varkappa(\gamma)^k$ modulo $p^{n+1}\mathbb{Z}_p$, donc ε est une fonction de $\mathbb{Z}_p$ périodique de période $p^{n+1}\mathbb{Z}_p$. Par définition de μ_C, on a donc $\int_{\mathbb{Z}_p} \varepsilon(x)d\mu_C(x) = L(0,\varepsilon) - CL(0,\varepsilon_C)$. Rappelons que

$L(0,\varepsilon) = -\sum_{a=0}^{p^{n+1}-1} \varepsilon(a)\left(\frac{a}{p^{n+1}} - \frac{1}{2}\right)$; notons X_k le sous-ensemble de $\{0,\ldots,p^{n+1}-1\}$ formé des a tels que $\langle a\rangle \equiv \varkappa(\gamma)^k$ modulo $p^{n+1}\mathbb{Z}_p$, on a alors $L(0,\varepsilon) = -\sum_{a\in X_k} \omega^{i-1}(a)\left(\frac{a}{p^{n+1}} - \frac{1}{2}\right)$; il est clair que les classes dans $(\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p)^*$ des $a\in X_k$ décrivent l'orbite de la classe de $\varkappa(\gamma)^k$ modulo le sous-groupe d'ordre $p-1$ de $(\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p)^*$; on en déduit que $\sum_{a\in X_k} \omega^{i-1}(a) = 0$, donc que $L(0,\varepsilon) = -\sum_{a\in X_k} \omega^{i-1}(a)\,\frac{a}{p^{n+1}}$. De même, si pour tout $x\in\hat{\mathbb{Z}}$ on note $\left\{\frac{x}{p^{n+1}}\right\}$ la fraction $\frac{a}{p^{n+1}}$ où a est l'entier congru à x modulo $p^{n+1}\hat{\mathbb{Z}}$ qui est tel que $0 \leqslant a < p^{n+1}$, on a $L(0,\varepsilon_C) = -\sum_{a\in X_k} \omega^{i-1}(a)\left\{\frac{aC^{-1}}{p^{n+1}}\right\}$. On a donc $f_{i,n}^{(k)} = \sum_{a\in X_k} \omega^{i-1}(a)\left[C\left\{\frac{aC^{-1}}{p^{n+1}}\right\} - \frac{a}{p^{n+1}}\right]$.

3) Fin de la démonstration. Du point 2) on tire que $f_{i,n}^* = \sum_{k=0}^{p^n-1}\left[\sum_{a\in X_k} \omega^{i-1}(a)\left(C\left\{\frac{aC^{-1}}{p^{n+1}}\right\} - \frac{a}{p^{n+1}}\right)\right]\gamma_n^{-k}$; pour tout a entier premier à p, on a noté σ_a l'élément de $G_n = \mathrm{Gal}(K_n/\mathbb{Q})$ tel que l'action de σ_a sur μ_n est l'élévation à la puissance a. Le groupe G_n s'identifie au produit $\Delta\times\Gamma/\Gamma_n$; si $a\in X_k$, on vérifie

facilement que la composante de σ_a sur Γ/Γ_n est γ_n^k ; de plus lorsque a décrit X_k , la composante τ_a de σ_a sur Δ décrit le groupe Δ tout entier. En remarquant que, sur $A_n^{(1-i)}$, l'élément $\omega^{i-1}(a) \in \mathbb{Z}_p$ agit comme l'élément τ_a^{-1} de Δ , on voit que $f_{i,n}^*$ agit sur $A_n^{(1-i)}$ comme l'élément $\sum_{k=0}^{p^{n+1}-1}\left(\sum_{a\in X_k}\left(C\left\{\frac{aC^{-1}}{p^{n+1}}\right\} - \frac{a}{p^{n+1}}\right)\right)\tau_a^{-1}\gamma_n^k =$
$\sum_{\substack{a=0\\(a,p)=1}}^{p^{n+1}-1}\left(C\left\{\frac{aC^{-1}}{p^{n+1}}\right\} - \frac{a}{p^{n+1}}\right)\sigma_a^{-1} = (1-c\sigma_c^{-1})\mathrm{Stick}_n$. Le théorème de Stickelberger (théorème 8.2) montre donc que $f_{i,n}^*$ annule $A_n^{(1-i)}$ ce qui, comme nous l'avons vu au point 1), démontre notre proposition.

BIBLIOGRAPHIE

[1] BOREVITCH, CHAFAREVITCH.- Théorie des nombres ; monographie internationale de Mathématiques modernes. Gauthier-Villars, Paris.

[2] BOURBAKI.- Algèbre linéaire. Chap. II, Hermann (1967).

[3] A. BRUMER.- On the units of algebraic number fields. Mathematika, 14 (1967), 121-124.

[4] J. COATES.- p-adic L functions and Iwasawa's theory. Algebraic Number Fields, edited by A. Fröhlich, Academic Press (1977), 269-351.

[5] J. COATES and WILES.- On p-adic L-functions and elliptic units. J. Austr. Math. Soc. (series A) 26 (1978) 1-25.

[6] R. GILLARD.- Relations de Stickelberger. Séminaire de théorie des nombres, Grenoble (1974).

[7] H. HASSE.- Uber die Klassenzahl abelscher Zahlkörper. Akademie Verlag Berlin (1952).

[8] K. IWASAWA.- On p-adic L functions. Ann. of Math., 89 (1969), 198-205.

[9] K. IWASAWA.- Some modules in the theory of cyclotomic fields. J. Math. Soc. Japan, 16 (1964), 42-82.

[10] K. IWASAWA.- Lectures on p-adic L-functions. Ann. Math. Studies, 74, Princeton (1972).

[11] N. KATZ.- A course at Princeton (1976-1977).

[12] S. LANG.- Algebraic Number Theory. Addison-Wesley Publishing Co. (1970).

[13] S. LANG.- Cyclotomic Fields. Graduate Texts in Mathematics, Springer-Verlag Berlin (1978).

[14] J.-P. SERRE.- Classes des corps cyclotomiques. Séminaire Bourbaki, exposé 174 (1958-1959).

[15] J.-P. SERRE.- Corps locaux. Hermann.