ANALYSE p-ADIQUE

B. Mazur.

Avant-propos

L'objet de ce rapport est de construire la série L p-adique de Kubota-Leopold et d'établir quelques propriétés fondamentales. Il est remarquable qu'il y a beaucoup de points de vues differents qui aboutissent à la construction de ces fonctions.

1. Le point de vue de Leopold-Kubota:

On essaie de trouver une série p-adique analytique $L(s,\chi)$ associée à un caractère (de 'Dirichlet') dont ces valeurs sur les entiers negatifs coincident avec celles de la série L (classique) de Dirichlet, aussi souvent que possible! (§ 4).

En fait on a bien mieux que cela. Par exemple, la série L p-adique satisfait à une formule analytique tres analogue à la formule analytique classique où le regulateur classique est remplacé par un regulateur p-adique. Un soupçon de cette formule est donné dans § 5 ci-dessous.

2. Le point de vue d'Iwasawa

On essaie d'étudier la croissance de la partie p-primaire du groupe de classes d'idéaux dan $Q(\zeta_{p^n})$ lorsque n tend vers l'infini (ζ_m = une racine m-ième primitive de l'unité). On trouve des formules qui donne une liaison étroite entre la vitesse de cette croissance et les zeros de certaines des séries L p-adiques dans un certain disque. Je n'ai même pas osé de mentionner ce genre de choses dans le texte parce que cela m'aurait conduit trop loin.

3. Le point de vue de Fresnel, Amice-Fresnel

On a envie d'approfondir les congruences mod p^n valables pour les nombres de Bernoulli (la congruence de Kummer, etc.).

4. Le point de vue de Serre

Les séries L p-adiques interviennent dans la théorie des formes modulaires p-adiques. Elles apparaissent comme les termes constants dans certaines familles des formes modulaires p-adiques (les séries d'Eisenstein).

Dans ce rapport j'ai utilisé la technique des mesures p-adiques qui mène facilement aux points de vue 1), 2), 3). J'ai essaye de donner des demonstrations complètes (probablement trop concises de temps en temps) sans faire appel à des références. Il y a cependant trois exceptions:

a)Il est très commode (mais pas du tout essentiel) d'employer le langage des groupes de Lie p-adiques. Donc, au debut je me sers du langage (tres peu) de cette theorie (Référence: LG = Lie algebras and Lie groups, Serre, Benjamin. Dans l'introduction de ce livre l'auteur dit qu'il se servait des manuscrits nonpubliées de Bourbaki... alors je suis justifié...)

(§2)

(b) Quelque part, on a besoin d'une formule intégrale pour $1/\Gamma(s)$ (la fonction complexe analytique)et ce n'est pas dans l'esprit de ce rapport ... donc je ~~fais~~ réfère à un texte de l'analyse complexe.

(c) Vers la fin de la dernière section j'ai donné des esquisses plûtot que des démonstrations complètes.

Bibliographie

J-P Serre: Cours de l'annee 73 College de France
Formes modulaires et fonctions zeta p-adiques, Antwerp

K. Iwasawa: Lectures on p-Adic L-functions
Annals of Math Studies.

1. L'Algèbre d'Iwasawa

(1.1) Fixons p un nombre premier. Soient K un corps localement compact qui est une extension finie de Q_p, et D son anneau d'entiers. D est un anneau topologique complet pour une valuation discrete

$$v: D^* \to Q$$
$$v(p) = 1 .$$

Pour la notion de groupe analytique sur K le lecteur doit se rapporter à LG (et, parait-il, quelques manuscrits nonpubliés dans les archives de Bourbaki). Nous allons considerer des échantillons parmi les plus inoffensifs de ce genre. A savoir: les groupes analytiques sur K, commutatifs et compacts. Soit G un tel groupe de dimension d. Son algèbre de lie $\mathfrak{g}$ est un espace vectoriel sur K de dimension d. L'algèbre $\mathfrak{g}$ elle-même peut être vue comme groupe analytique localement compact sur K. En se servant d'un théorème de LG, on peut trouver un sous-D-module $L \subset \mathfrak{g}$, libre de rang d sur D (un réseau) tel que l'exponentielle induit un isomorphisme de L sur un sous-groupe $G_o \subset G$, ouvert, d'indice fini.

Au moyen d'un tel réseau L on obtient un système fondamental de voisinages de 0, donné par ~~une~~ la suite de sous-groupes ouverts dans G:

$$\text{image}(p^nL) = p^nG_o = G_n \subset G \qquad n \geqslant 0.$$

Exemples

1. D^* : le groupe multiplicatif des elements inversibles de ~~dans~~ D. D^* est un groupe analytique de dimension 1 sur D. Son algèbre de lie est canoniquement isomorphe à K, et l'exponentielle du groupe analytique D est l'exponentielle ordinaire:

$$\exp(X) = \sum_{0}^{\infty} \gamma_n(X)$$

ou γ_n est la puissance n-ième divisée:

$$\gamma_0(X) = 1$$

$$\gamma_n(X) = X^n/n! \qquad n \geqslant 1.$$

Puisque $v(n!) < n/p-1$, on a

$$v(\gamma_n(p)) > n \cdot \frac{p-2}{p-1} \quad ,$$

et $\qquad v(\gamma_n(4)) > n.$ pour $p=2$.

Il s'ensuit que l'exponentielle est convergente sur $p \cdot D$ si $p \neq 2$ (resp. $4D$ si $p = 2$). Son inverse

$$\log(1-Y) = - \sum_{0}^{\infty} n! \cdot \gamma_{n+1}(Y)$$

est convergent pour $Y \in pD$.

Dans le cas $K = Q_p$, $D = Z_p$, appelons $U = (Z_p)^*$ et

$$U_1 = \left\{ u \in U \quad u \equiv 1 \quad \begin{array}{ll} \text{mod } p & \text{si } p \neq 2 \\ \text{mod } 4 & \text{si } p = 2 \end{array} \right\}$$

On a

$$U = U_1 \times F$$

ou F est le sous-groupe de racines(p-1) -ième d'unité: c'est un groupe cyclique d'order p-1, si $p \neq 2$. Si $p = 2$, $F = (\pm 1)$.

La décomposition ci-dessus est clair pour $p = 2$, et elle se voit pour $p \neq 2$ par une petite application du lemme de Hensel à l'équation $X^{p-1}-1 = 0$.

Designons par $u \to \langle u \rangle$ la projection sur le premier facteur dans la décomposition ci-dessus.

L'exponentielle induit un isomorphisme de groupes analytiques:

$$pZ_p \xrightarrow{\approx} U_1 \qquad (p \neq 2)$$

$$4Z_2 \xrightarrow{\approx} U_1 \qquad (p = 2).$$

2. X: <u>le groupe des caractères de G à valeurs dans D^*</u>

Soit G un groupe analytique sur Q_p, commutatif et compact. Soit $X = \mathrm{Hom}_{cont}(G,D^*)$, le groupe d'homomorphismes d'une façon telle que le morphisme inversion $x \mapsto x^{-1}$ est un homomorphisme de groupes analytiques sur K. (X = groupe des caractères de G)

continus. Lorsque $G \simeq Z_p^d$, X est isomorphe à un ouvert dans $(D^{\times})^d$, donc X est muni de la structure de groupe analytique sur K, commutatif et compact, de dimension d.

Puisque n'importe quel groupe analytique sur Q_p, commuti-tatif et compact, de dimension d, possède un sous-groupe G' ouvert isomorphe à Z_p^d, X peut toujours etre muni de la structure de groupe analytique sur K commutatif et compact, de dimension d. C'est facile à montrer que cette structure ne dépend que du groupe analytique G.

L'accouplement

$$G \times X \to D$$
$$(g,x) \mapsto x(g)=g(x)$$

induit un morphisme

$$G \xrightarrow{\varphi} F(X,D)$$

ou F(X,D) est le D-module de fonctions analytiques sur X à valeurs dans D. Donnons à F(X,D) la topologie de convergence uniforme. Autrement dit, un système fondamental de voisinages de 0 est donné par $p^n \cdot F(X,D)$, $n \geq 0$.

C'est trivial ~~Un calcul facile montre~~ que φ est une application continue. Le théorème d'indépendance des caractères (de Dedekind) montre que φ s'étend à une injection de l'anneau

$$D[G] \to F(X,D)$$

($D[G]$ = l'anneau du groupe G à coefficients dans D
$= \{\Sigma\, a_i g_i$ (somme fini), $a_i \in D$, $g_i \in G\}$)

(1.3) Par définition, l'Algèbre d'Iwasawa de G sur D , Λ, est l'algebre topologique compacte

$$D[[G]] = \varprojlim_n D[G/G_n].$$

Si $G = Z_p^d$ l'algèbre d'Iwasawa prend la forme suivante:

Notons par $g_1,\ldots g_d \in Z_p^d = G$, la base canonique. Soit $D[[T_1,\ldots,T_d]]$ l'anneau de séries ~~puissances~~ formelles dans les variables T_i à coefficients dans D.

<u>Proposition</u>: Le morphisme de D-algèbres

$$D[T_1,\ldots,T_d] \xrightarrow{\psi} D[[G]]$$

$$T_i \to g_i - 1$$

s'étend en un isomorphisme de D-algèbres topologiques:

$$D[[T_1,\ldots,T_d]] \approx D[[G]]$$

<u>Démonstration</u>: Le morphisme ψ induit une surjection

$$\psi_n : D[T_1,\ldots,T_d] \to D[G/G_n] \qquad (G_n = p^nG;\ G/G_n = (Z/p^n)^d)$$

pour tout entier positif n. Le noyau de ψ_n est l'idéal $\mathfrak{a}_n$ engendré par $(1+T_i)^{p^n}-1$ pour $i = 1,\ldots,d$. Il suffit de montrer que $(1+T_i)^{p^n}-1$ est dans l'idéal I^n ou $I = (p,T_i)$, pour tout n et i. Puisque à ce moment-là ψ s'étendera à un homomorphisme surjectif et continu de $D[[T_1,\ldots,T_d]]$ sur $D[[G]]$.

N° 592

Le morphisme ?

est injectif parce que $\bigcap_n I^n$ est nul, et c'est un homéomorphisme puisque $D[[T_1,\dots,T_d]]$ est compact.

On démontre l'assertion par récurrence. Notons ~~par~~ a l'élément $(1+T_i)^{p^{n-1}}$ et supposons qu'on a déja montré que $a-1 \in I^{n-1}$. Alors, il faut montrer $a^p-1 \in I^n$. Mais

$$a^p-1 = (1+a+\dots+a^{p-1})(a-1)$$

et le premier facteur est contenu dans I.

c.q.f.d.

Si $G = C\times H$ ou C est un groupe fini, et H un groupe analytique sur Q_p on a

$$D[[G]] = \varprojlim D[C\times H/H_n] = \varprojlim D[C][H/H_n] = D[C][[H]]$$

On obtient aussi

$$D[[G]] = D[C] \otimes_D D[[H]].$$

Un groupe analytique sur Q_p commutatif et compact quelconque G est isomorphe (noncanoniquement) au produit

$$C\times Z_p^d$$

ou C est un groupe fini. Il s'ensuit que son algèbre d'Iwasawa est isomorphe a $D[C][[T_1,\dots,T_d]]$.

(2.6) **Proposition:**

Au moyen du morphisme naturel, $D[G] \to D[[G]]$, l'algèbre $D[G]$ s'identifie à une sous-algèbre dense dans $\Lambda = D[[G]]$.

Le morphisme $\varphi: G \to F(X,D)$ s'etend ~~à~~ en un homomorphisme continu $\varphi: \Lambda \to F(X,D)$. Soit $C \subset G$ le sous-groupe de torsion. Soit $c = \# C$. Si D contient une racine c-ième primitive de l'unité, le morphisme $\varphi: \Lambda \to F(X,D)$ est un homéomorphisme sur une sous-D-algèbre compacte de $F(X,D)$.

Demonstration:

Le morphisme $D[G] \to D[G/G_n]$ est surjectif pour tout n. D'autre part, si $\alpha \in D[G]$ n'est pas 0, on peut trouver un n tel que α n'~~est~~ soit pas dans le noyau de $D[G] \to D[G/G_n]$, d'où la première assertion.

Quant à la seconde, pour n'importe quel n, il existe un nombre m tel que si $h \in G_m$, $\varphi(h-1) \in p^n \cdot F(X,D)$. Donc φ envoie le noyau de $D[G] \to D[G/G_m]$ dans $p^n \cdot F(X,D)$. Il s'ensuit que φ s'étend ~~à~~ en un homomorphisme de Λ dans $F(X,D)$.

Supposons maintenant que D contient une racine c-ième primitive de l'unité. Ecrivons $G = C \times H$, avec $H \approx Z_p^d$. Chaque caractère $\chi: C \to D^*$ induit un homomorphisme d'anneaux

$$D[[G]] \xrightarrow{\chi} D[[H]]$$

et grace à notre hypothese, le produit

$$D[[G]] \xrightarrow{\times\chi} \mathop{\times}_{\chi} D[[H]]$$

est injectif. On voit donce que afin de montrer n° 592

l'injectivité de $\varphi: \Lambda \to F(X,D)$ on peut supposer que $G = H = Z_p^d$. Considérons une série

$$f = \Sigma\, a_{i_1,i_2,\ldots,i_d} T_1^{i_1} \ldots T_d^{i_d} \quad \varepsilon\ D[[T_1,\ldots,T_d]]$$

dans le noyau de φ. La série f a la propriété qu'elle s'annule pour n'importe quel choix de valeurs $T_i\ \varepsilon\ pD$. Alors, elle est identiquement nulle.

On a montré que φ est continu et injectif, ~~Elle est~~ donc un homéomorphisme de Λ sur un sous-algèbre compact puisque Λ est compact.

c.q.f.d.

Désormais on fera l'hypothèse que D possède une racine c-ième primitive de l'unité, et on identifiera l'Algèbre d'Iwasawa avec son image dans $F(X,D)$. Si $\alpha\ \varepsilon\ \Lambda$, on écrira $\alpha(x)$ pour la fonction analytique sur X à valeurs dans D qui est l'image de α dans $F(X,D)$.

~~Remarquons que lorsque $G \approx Z_p^d$, $\Lambda \cong D[[T_1,\ldots,T_d]]$ le théorème de préparation de Weierstrass implique~~

2. Distributions et mesures

Soit T un espace topologique localement compact et totalement discontinu. Soit E_T (fonctions en escaliers) le groupe de fonctions sur T, à valeurs dans $\mathbb{Z}$, localement constante~~s~~, a support compact. Soit W un groupe abelien.

Définition: Une distribution sur T, à valeurs dans W, est un homomorphisme,

$$(*) \quad E_T \xrightarrow{\mu} W$$

(~~nous~~ écrirons: $\varphi \longmapsto \int_T \varphi(t)\mu(t)$)

Si $U \subset T$ est un ouvert compact, notons ~~par~~ $\mu(U) \in W$ l'image par μ de la fonction caractéristique de U:

$$\mu(U) = \mu(\chi_U) = \int_T \chi_U \mu = \int_U \mu$$

On obtient ainsi une fonction

$$(**) \quad \left\{\begin{matrix}\text{ouverts}\\ \text{compacts}\\ \text{dans } T\end{matrix}\right\} \xrightarrow{\quad\mu\quad} W$$

qui est finiement additive. ('finiement additive' veut dire que si l'on a une réunion disjointe d'ouverts compacts dans T: $U = \cup_i U_j$

№ 592

(Une fonction μ sur les ouverts compacts dans T est <u>finiement additive</u> si elle satisfait à la propriété suivante:

$$\mu(\cup_j U_j) = \Sigma_j \mu(U_j)$$

pour toute réunion disjointe finie $\cup_j U_j$ d'ouverts compacts dans T.)

A n'importe quelle fonction finiement additive sur les ouverts compact dans T à valeurs dans W on peut associer une distribution par la regle suivante:

Soit $f \varepsilon E_T$. Soit U un ouvert compact dans T qui contient le support de f. Soit $U = \cup_j U_j$ une decomposition de U en ouverts compacts disjoints U_j telle que f est constante sur chaque U_j. Définissons

$$\int_T f\mu = \Sigma_j f(U_j)\mu(U_j)$$

C'est clair que la somme à la droite ne dépend pas de la décomposition $U = \cup_j U_j$ parce que μ est finiement additive. Donc $\int_T -\mu$ est bien-defini et clairment un homomorphisme. C'est une distribution alors.

On a établi ainsi une correspondance biunivoque entre les fonctions finiement additives sur les ouverts compacts dans T, à valeurs dans W, et les distributions sur T, à valeurs dans W.

Notons le groupe abélien de distributions sur T à valeurs dans W : dist(T,W).

Si T est fini (et discret) dist (T,W) s'identifie au groupe abélien des fonctions sur T à valeurs dans W.

Si T est un espace compact, qui s'exprime comme limite projective d'espaces finis,

$$T = \varprojlim_{n} T_n \qquad n \geqslant 0$$

avec $T_{n+1} \to T_n$ surjectif.

Pour chaque n, on définit une application

$$\mathrm{dist}(T_{n+1}, W) \xrightarrow{N} \mathrm{dist}(T_n, W)$$

ainsi: pour μ_{n+1} une distribution sur T_{n+1}

soit $N\mu_{n+1} = \mu_n$ où,

$$\mu_n(t) = \sum_{t'} \mu_{n+1}(t')$$

et t' parcourt les éléments dans T_{n+1} qui se projette à $t \in T_n$.

On a

$$\mathrm{dist}\,(T,W) = \varprojlim_{n} \mathrm{dist}(T_n, W)$$

où la limite projective est formée au moyen des applications N.

On peut représenter, par conséquent, une distribution sur T comme une suite $(\mu_n)_{n \geq 0}$ de fonctions,

$$\mu_n \in \mathrm{dist}(T_n, W) = \mathrm{fonctions}\ (T_n, W)$$

telle que

$$\mu_n(t) = \sum_{t'} \mu_{n+1}(t') \qquad \text{pour tout } n,\ t \in T_n$$

où t' parcourt les éléments dans T_{n+1} qui se projette sur $t \in T_n$.

Prenons maintenat pour W le corps K (muni de sa valeur absolue ultramétrique $|\ |$: $|p| = p^{-1}$).

(2.2) **Définition**: Une distribution sur T à valeurs dans K

(à valeurs dans K)

est une mesure si $|\mu(U)|$ est borné sur l'ensemble d'ouverts compacts dans T.

Il revient au meme de demander qu'il existe un élément nonnul $c \in K$ tel que $c \cdot \mu$ prend ses valeurs dans $D \subset K$.

Supposons que T est compact. Soit $C(T,K)$ l'espace (de Banach sur K) de fonctions continues sur T à valeurs dans K.

$$\|f\| = \sup_{t \in T} |f(t)|$$

à valeurs dans K

Proposition: Si T est compact, et μ une mesure sur T à valeurs dans K, l'application

$$\mu : E_T \to K$$

s'étend (uniquement) à une fonctionelle K-linéaire et bornée

$$C(T,K) \xrightarrow{\mu} K$$

$$f \mapsto \int_T f\mu$$

Démonstration: Si c est une constante telle que $c \cdot \mu$ prend ses valeurs dans D, on aura

$$(*) \quad \left|\int_T f\mu\right| \leq 1/|c| \cdot \|f\|$$

Il n'ya pas aucune difficulté de montrer la proposition: Si $C_{esc}(T,K) \subset C(T,K)$ est le sous-espace vectoriel sur K engendré par E_T, μ s'étend par linéairité à $C_{esc}(T,K)$.

L'inégalité (*) est evidente pour $f \in C_{esc}(T,K)$.

Mais $C_{esc}(T,K)$ est dense dans l'espace de Banach $C(T,K)$ et μ s'étend alors à $C(T,K)$ par continuité, satisfaisant encore à l'inégalité (*). L'unicité est aussi clair.

Remarques:

La dernière proposition établit une correspondence biunivoque: (lorsque T est compact)

$$\begin{array}{c} \text{mesures} \\ \text{sur } T \text{ à} \\ \text{valeurs} \\ \text{dans } K \end{array} \longleftarrow - - \longrightarrow \begin{array}{l} \text{fonctionelles} \\ K\text{-linéaires et} \\ \text{bornées sur} \\ C(T,K) \end{array} .$$

Etant donné une mesure μ sur T (toujours compact) et une fonction $g \in C(T,K)$ notons $g \cdot \mu$ la mesure

$$f \longmapsto \int_T fg\mu .$$

Soit maintenant G un groupe analytique sur Q_p, (commutatif et) compact. On a

$$G = \varprojlim_n G/G_n \qquad n \geqslant 0$$

pour le systeme de sous-groupes ouverts $G_n \subset G$ décrit en §1.

On a des correspondences biunivoques:

$$\mathrm{dist}(G/G_n, D) \xrightarrow{\beta} D[G/G_n]$$

$$\varphi \longmapsto \sum_{g \in G/G_n} \varphi(g)\cdot g$$

induisant des carrés commutatifs:

$$\begin{array}{ccc} \mathrm{dist}(G/G_{n+1}, D) & \xrightarrow{\beta} & D[G/G_{n+1}] \\ \downarrow N & & \downarrow \mathrm{proj} \\ \mathrm{dist}(G/G_n, D) & \xrightarrow{\beta} & D[G/G_n] \end{array} .$$

Par passage à la limite on obtient

(2.5 **Proposition**: Soit G un groupe analytique sur Q_p (commutatif et) compact. Les morphismes β ci-dessus induisent une correspondence biunivoque

$$\mu \longmapsto \alpha_\mu$$
$$\mu_\alpha \longleftarrow\!\shortmid\ \alpha$$

entre les mesures sur G à valeurs dans D et les éléments dans l'algèbre d'Iwasawa de G. On a

$$\alpha_\mu(x) = \int_G x(g)\,\mu(g) \qquad x \in X .$$

Proposition:

Soit G un groupe analytique sur Q_p (commutatif et) compact. Le morphisme

$$C(G,K)\times\Lambda \to K$$
$$(f,\alpha) \to \int_G f\cdot\mu_\alpha$$

est continu.

Démonstration:

Puisque

$$\left|\int_G f'\mu_{\alpha'} - \int_G f\mu_\alpha\right| \leq \max\left(\|f'-f\|,\ \left|\int_G f\mu_{(\alpha'-\alpha)}\right|\right)$$

on se ramène à montrer que pour f et $\varepsilon>0$ donné il existe un n tel que si $\alpha\ \varepsilon\ \Lambda$ se projette à 0 dans $D[G/G_n]$ alors
$p^\mu D$

$$\left|\int_G f\mu_\alpha\right| < \varepsilon$$

Mais il ne faut que trouver un n tel que

$$|f(gh) - f(g)| < \varepsilon \quad \text{pour tout } g\varepsilon G,\ h\varepsilon G_n :$$

Prenons $g_j\ \varepsilon\ G$ un système de représantants modulo G_n.
Considérons $\bar{f} = \Sigma f(g_j)\cdot\chi_{g_j\cdot G_n}$ (χ_U= fonction caractéristique de U).
On a $\|f-\bar{f}\| < \varepsilon$ et $\int_G \bar{f}\mu_\alpha = 0$, d'où la proposition.

Exemple: 1) La distribution de Haar

Soit G un groupe analytique sur Q_p et compact. Il existe une distribution unique μ à valeurs dans Q_p invariante par translation à gauche et telle que $\mu(G) = 1$. Mais ce n'est pas une mesure à valeurs dans Q_p!

2) La mesure de Dirac

Soit G comme ci-dessus, et $g \varepsilon G$. La mesure de Dirac supportee à g, δ_g, se defini par la règle usuelle:

$$\delta_g(U) = 1 \quad \text{si } g \varepsilon U$$
$$= 0 \quad \text{sinon.}$$

On a, comme d'habitude,

$$f(g) = \int_G f \cdot \delta_g$$

C'est facile à voir que la mesure associée à l'élément $g \varepsilon G \subset \Lambda$ par la proposition (2.5) n'est que la mesure de Dirac δ_g.

Proposition: Un caractère $\chi : G \to D^*$ se prolonge à un homomorphisme continu des D-algèbres $\rho : \Lambda \to D$ par la formule

$$\rho(\alpha) = \int_G \chi \mu_\alpha$$

où μ_α est la mesure associée à α.

Démonstration:

Définissons ρ par la formule. C'est continu par la proposition et c'est D-linéaire. Si $g \in G$,

$$\rho(g) = \int_G \chi \delta_g = \chi(g)$$

et donc ρ est bien une extension de χ. Puisque χ est un homomorphisme de G dans D^*, ρ est un homomorphisme du D-algebre $D[G]$ sur D. On voit que $\rho : \Lambda \to D$ est aussi un homomorphisme par continuité.

3. Le groupe multiplicatif et la coordonnée canonique s

Soit $G = U_1$ et désignons par χ le caractère sur U_1 à valeurs dans D^* donné par la composition:

$$\chi : U_1 \subset Z_p^* \subset D^*$$

Pour $z \in D$ on obtient un caractère

$$\chi^z : U_1 \to D^*$$

par $\chi^z(u) = u^z = \exp(\log u \cdot z) = \sum \gamma_n(\log u) \cdot z^n$. (7)

Par la proposition précédente, le caractère χ^z s'étend ~~à~~ en un homomorphisme continu des D-algèbres

$$\rho^z : D[[U_1]] \to D$$

par la formule:

$$\rho^z(\alpha) = \int_{U_1} \chi^z \cdot \mu_\alpha$$

où $\alpha \in D[[U_1]]$ et μ_α est la mesure sur U_1 associée à α.

(3.) **Proposition**: Soit $u \in U_1$ un generateur topologique. Fixons l'identification

$$D[[T]] \to D[[U_1]]$$
$$T \mapsto 1 - u$$

Si $\alpha \in D[[U_1]]$ s'identifie à la série formelle $f(T)$, on a la formule

$$(*)\quad \rho^z(\alpha) = f(1-u^z).$$

Il existe une série formelle

$$a(s) = \sum a_n s^n \quad \in D[[s]]$$

uniquement caracterisée par la formule $a(z) = \rho^z(\alpha)$ pour tout $z \in D$. Les coéfficients a_n sont donnés par

$$a_n = \int_{U_1} \gamma_n(\log u) \cdot \mu_\alpha . \qquad (\gamma_n = \text{n-ieme puissance divisée})$$

Démonstration:

Puisque $\rho^z(1-u) = 1-u^z$, la première formule provient de linéairité et continuité de l'operateur ρ^z. La série formelle $a(s)$ peut être obtenue tout simplement comme $f(-\sum_1 \gamma_n(\log u) \cdot s^n)$ ou par une intégration terme-par-terme de $(*)$ ci-dessus (facile à justifier) d'où la dernière formule de la proposition.

Considérons l'homomorphisme des D-algèbres

$$\Lambda = D[[U_1]] \xrightarrow{\eta} D[[s]]$$

L'injectivite et continuité de η se voit facilement par la formule (*). La question s'impose de determiner l'image de η dans $D[[s]]$. Appelons-le $\Lambda_s \subset D[[s]]$.

Commencons avec un résultat qui s'obtient immediatement de la proposition précédente.

<u>Corollaire</u>: Soit $\Sigma a_n s^n$ dans Λ_s. Alors,

$$|a_n| \leq |\gamma_n(p)| \leq p^{-n\left(\frac{p-2}{p-1}\right)}$$

et

$$|a_n| \leq |\gamma_n(4)| \quad \text{si } p=2.$$

$\Sigma a_n s^n$ converge dans le disque ouvert de rayon $p^{\left(\frac{p-2}{p-1}\right)}$ (resp. le disque fermé de rayon 1 si $p = 2$).

Démonstration:

$$|a_n| = \left|\int_{U_1} \gamma_n(\log u)\, \mu_\alpha\right| \leq \|\gamma_n(\log u)\| = |\gamma_n(p)|$$

(et de la même façon la petite amélioration pour $p = 2$).

(3.4) On se prépare maintenant à déterminer Λ_s dans le cas spécial: $K = Q_p$, $D = Z_p$.

Soit $f(z)$ une fonction continue sur Z_p à valeurs dans Z_p.

(3.5) <u>Definition</u>: Les <u>coefficients d'interpolation</u> $\delta_k(f) \in Z_p$ $(k \geq 0)$ <u>de f</u> sont définies ainsi:

$$\delta_o(f) = f(0)$$
$$\delta_1(f) = f(1)-f(0)$$
$$\delta_2(f) = (f(2)-f(1))-(f(1)-f(0))$$
$$\cdots\cdots\cdots$$
$$\delta_k(f) = \sum_0^k (-1)^i \binom{k}{i} f(k-i)$$

(3.6) <u>Exemple</u>: Considérons le polynome à coefficients dans $(1/n!)Z$

$$C_n(s) = \binom{s}{n} = \frac{s(s-1)\ldots(s-n+1)}{n!} = \sum_o^n c_{n,j}s^j = \gamma_n(s) + \text{termes de degré inférieur à } n.$$

Pour $s \in Z, C_n(s) \in Z$. Puisque C_n est continue et Z est dense dans Z_p, on a

$$C_n: Z_p \to Z_p$$

Appelons C_n <u>le polynome de Pascal de dégré n</u>.

<u>Lemme</u>: $\delta_k(C_n) = 0$ si $k \neq n$
$= 1$ si $k = n$.

Démonstration: Par récurrence, tenant compte de la relation

$$C_n(s) - C_n(s-1) = C_{n-1}(s-1) .$$

Pour $f\colon Z_p \to Z_p$ une fonction continue quelconque, formons la série

$$\Sigma\, \delta_k(f)\cdot C_k \quad \text{(le \underline{developpement de Pascal} de f)}$$

Théorème de Mahler:

Si ~~Soit~~ $(\delta_k)_{k \geqslant 0}$ est une suite d'éléments dans Z_p telle que $\delta_k \to 0$, la série de Pascal $\Sigma\delta_k\cdot C_k$ ~~se~~ converge à une fonction continue sur Z_p à valeurs dans Z_p.

Soit $f\colon Z_p \to Z_p$ une fonction continue, alors ses coéfficients d'interpolation $\delta_k(f)$ tendent vers zéro dans Z_p et on a

$$f(s) = \Sigma\, \delta_k(f) C_k(s) = \Sigma\, \delta_k(f) \binom{s}{k} \qquad s \in Z_p .$$

Démonstration: La première assertion est claire. Quant à la seconde, fixons f, une fonction continue.

Pour un entier $m > 0$ quelconque, ~~tachons~~ prenons un entier $n \geqslant m$ tel que $f(a) \equiv f(a') \bmod p^m$ si $a \equiv a' \bmod p^n$.

Vu le lemme ci-dessus, en remplacant f par

$$\tilde{f} = f - \sum_{0}^{p^n-1} \delta_k(f)\cdot C_k$$

on se ramène à supposer

$\delta_k(\overline{f}) = 0 \quad$ pour $k = 0,1,\dots, p^n-1$

ce qui équivaut à dire

$$\overline{f}(k) = 0 \quad \text{pour } k = 0,1,\dots, p^n-1$$

Il s'ensuit que $\overline{f}(Z_p) \subset p^m Z_p$ par le choix de n.
Alors,

$$\delta_k(\overline{f}) = \delta_k(f) \in p^m Z_p \quad \text{si } k \geqslant p^n.$$

Il s'ensuit que $\delta_k(f) \to 0$ et le développement de Pascal de f tend vers f.

c.q.f.d.

Maintenant on va généraliser le domaine de la fonction

$$C_n(s) = \Sigma\, c_{n,j} s^j .$$

Soit $(b_0,\dots,b_n)$ un (n+1)-tuple d'entiers p-adiques. Formons

$$C_n(b_0,\dots,b_n) = \Sigma\, c_{n,j} b_j \in Q_p .$$

Si β est une suite infinie d'entiers p-adiques $(b_n)_{n\geqslant 0}$, écrivons

$$C_n(\beta) = C_n(b_0,\dots,b_n)$$

pour chaque $n \geqslant 0$.

<u>Définition</u>: Une suite β d'entiers p-adiques est appelée une suite <u>presque-géometrique</u> ($\beta \in$ P.G.) si $C_n(\beta) \in Z_p$ pour chaque $n \geqslant 0$.

Ai°592 \ 25

(39) **Proposition:**

(a) Si β est une suite géometrique ($b_n = b^n$ pour un entier p-adique b) alors β est une suite presque-géometrique.

(b) Une combinaison lineaire de suites presque-geometriques à coefficients dans Z_p est encore presque-géométrique: P.G. est un Z_p-module.

(c) Donnons à P.G. la topologie de convergence simple de chaque b_n (la topologie induit par son injection dans le produit Z_p^N). Soit Σ le sous-Z_p-module engendré par les suites geométriques. Alors Σ est dense dans P.G.

(d) Si $\beta \in$ P.G. on a les congruences

$$b_{n+p-1} \equiv b_n \qquad \text{modulo } p$$

pour tout $n \geq 0$. mieux: $b_{n+\varphi(p^i)} \equiv b_n$ mod p^i si $n \gg 0$.

Démonstration:

(a) Si β est une suite géometrique, $C_n(\beta) = C_n(b)$ pour l'entier p-adique b.

(b) La condition d'étre presque-géoemtrique est une suite de congruences linéaires en les b_i.

(c) Soit $m \geq 1$ et soient $b_o, \ldots, b_m \in Z_p$ satisfaisant aux conditions suivantes:

$$C_k(b_o, \ldots, b_k) \in Z_p \qquad \text{pour } k = 0, 1, \ldots, m$$

(une suite presque-geométrique tronquée). On va montrer que cette suite tronquée peut être réalisée par un élément de Σ. En effet, par récurrence on se ramène au cas $b_j = 0$ pour $j \leq m-1$. A ce moment-là on voit que $b_m \in m!Z_p$.

On est reduit, alors, à montrer que la suite

$$(*) \qquad 0,0,\ldots,0, m!$$

est réalisée par un élément de Σ. Prenons $\beta = (b_n)_{n\geq 0}$:

$$b_n = \sum_{0}^{m} (-1)^{m-j}\binom{m}{j} j^n$$

Alors, β est clairment dans Σ, et elle réalise la suite tronquée $(*)$ parce que b_n est le n-ième coéfficient de l'expansion de Taylor de la fonction

$$(\exp(t)-1)^m .$$

(d) La congruence de la partie (d) de la proposition est évidente pour les suites géométriques. Donc elle est vrai pour les éléments de Σ et, vu la densité de Σ dans P.G., on a gagné.

c.q.f.d.

(3.10) Remarque: La condition d'être presque-géométrique se traduit comme une suite de congruences: Pour chaque n, b_n doit être congrue, modulo $n!Z_p$, à une combinaison linéaire de b_j ($j < n$).

$$b_2 \equiv b_1 \mod (2\cdot Z_p)$$

$$b_3 \equiv 3b_2 - 2b_1 \mod (6\cdot Z_p)$$

$$b_4 \equiv 6b_3 - 11b_2 + 6b_1 \mod (24\cdot Z_p)$$

....

N° 592 ~~27~~

(3.11) **Théorème:** Si $p \neq 2$, les trois conditions suivantes sont équivalentes:

1. $f \in \Lambda_s$.

2. Si l'on écrit le développement de Pascal de f sous ~~dans~~ la forme

$$f = \Sigma\, \Delta_k \cdot p^k \cdot C_k\ ,$$

la suite $(\Delta_k)_{k>0}$ est une suite presque-géométrique d'entiers p-adiques.

3. Si l'on écrit le développement de Taylor de f dans la forme

$$f(s) = \Sigma\, d_k \cdot p^k \cdot \gamma_k(s)$$

la suite $(d_k)_{k \geq 0}$ est une suite presque-géométrique d'entiers p-adique.

(L'équivalence des trois conditions reste vrai pour $p = 2$ pourvu qu'on remplace p par 4 dans les énoncés 2) et 3).)

Démonstration:

~~En employant la~~ terminologie de l'énoncé de notre Théorème ~~proposition~~, considérons les applications

$$\Lambda_s \to Q_p^N$$

$$\Delta:\ f \longmapsto \{\Delta_k(f)\}_{k>0}$$

$$d:\ f \longmapsto \{d_k(f)\}_{k\geq 0}$$

La démonstration sera faite en trois étapes:

I) Rappelons que Λ_s est ~~donne la~~ munie de la topologie induite par inclusion dans $D[[s]]$, et cette topologie coincide avec celle définie par convergence simple sur les entiers $Z \subset Z_p$.

Il s'ensuit que $f \to d_k(f)$ et $f \to \Delta_k(f)$ sont des applications continues.

II) Soit $b \in Z_p$. La suite géométrique $(b^n)_{n\geq 0}$ est dans l'image de d et de Δ:

$$(\exp(pb))^s \xmapsto{d} (b^n)_{n\geq 0}$$

$$(1+pb)^s \xmapsto{\Delta} (b^n)_{n\geq 0} .$$

Plus precisement, alors, on a pour d ou Δ:

$$\begin{tikzcd}
D[[U_1]] \arrow[r] & \Lambda_s \arrow[r, "d \text{ ou } \Delta"] & Q_p^N & (D=Z_p) \\
U_1 \arrow[u, hook] \arrow[rr, leftrightarrow, "\text{correspondance biunivoque}"'] & & \text{Suites Geometriques d'entiers p-adiques} \arrow[u, hook] &
\end{tikzcd}$$

III) Puisque $D[U_1]$ est dense dans $D[[U_1]]$ et son image est contient dans $P.G. \subset Q_p^N$ (étape II et prop. 3.9 (b)) il s'ensuit que d et Δ envoient Λ_s dans $P.G. \subset Q_p^N$. L'image de $D[U_1]$ est précisément Σ, le sous-Z_p-module engendré par les suites géométriques. Puisque Σ est dense dans $P.G.$ et Λ_s est compact, on a que d et Δ sont des homéomorphismes de Λ_s sur $P.G.$

c.q.f.d.

n° 592.

4. Distributions de Bernoulli

Si $\alpha \in Z/mZ$ désignons par $\{\alpha\}$ la fraction $\frac{a}{m} \in Q$ ou a est un entier $0 \leqslant a < m$ et a se projette à α.†

Soit m_o premier à p et $m_n = m_o p^n$. Si $B(x)$ est un polynome de degré k dans $Q[x]$, formons la fonction

$$E : Z/mZ \to Q \qquad (m \text{ un entier})$$

$$\alpha \mapsto m^{k-1} B(\{\alpha\})$$

Disons que $B(x)$ est <u>un polynome qui définit une distribution sur T</u> $= \varprojlim Z/m_nZ = Z/m_oZ \times Z_p$ si, en effet, les fonctions

$$E^{(n)}: Z/m_nZ \to Q$$

se recollent par les projections $Z/m_{n+1}Z \to Z/m_nZ$ pour $n \geqslant 0$. Çela veut dire:

$$E^{(n)}(\alpha) = \sum_{\alpha'} E^{(n+1)}(\alpha')$$

ou $\alpha \in Z/m_nZ$ et α' parcourt les éléments de $Z/m_{n+1}Z$ dans l'image inverse de α. Par la discussion de (2.1) la suite $(E^{(n)})_n$ nous donne une distribution qu'on appellera E.

---

† Le choix $0 \leqslant a < m$ des représentants nous mènera aux polynomes de Bernoulli traditionels, avec $b_1 = -1/2$. Si nous prenions le choix $-1/2 \leqslant \frac{a}{m} < 1/2$ on aurait $b_1 = 0$.

(2.2) Remarques:

On ne perd pas de généralité en supposant que $B(x)$ soit ~~monique~~ unitaire. Supposons-le alors et écrivons:

$$B(x) = x^k + k\cdot b_1 x^{k-1} + \dots.$$

L'hypothèse que les $E^{(n)}$ se recollent se traduit ainsi:

$$(1)\quad B(a/m) = p^{k-1}\cdot\sum_{j=0}^{p-1} B(a+jm/pm)$$

pour tout entier $0 \leq a < m$ et $m = m_n$ $n=0,1,\dots$.

(2.3) Théorème: Pour chaque $k \geq 0$ il existe un et un seul polynome $B_k(x)$, ~~monique~~ unitaire, de degré k, qui définit une distribution. $B_k(x)$ est le k-ième polynome de Bernoulli. (Voir Bourbaki, fonctions d'une variable réelle ch. VI §1 no.4 pour une discussion des polynomes de Bernoulli)

Démonstration:

Unicité: Soient B, B' deux polynomes, moniques et de degré k, qui définissent des distributions. [illegible]. La difference $\beta = B'-B$ est de degré $j < k$, et par (1) elle satisfait à la formule

$$(2)\quad \beta(x) = p^{n(j+h)}\sum_{i=0}^{p^n-1} \beta(x+i/p^n)$$

où $h = k-1-j \geqslant 0$, n est un entier quelconque, et $x = a/m_0 p^r$, $0 \leq x < 1$.

Soit Δ = ppcm des denominateurs des coefficients de β. Considerons deux cas:

<u>$h > 0$</u>: Alors la formule (2) implique

$$(3) \qquad \beta(x) \equiv 0 \mod p^{nh}\Delta^{-1}Z_p \quad .$$

Puisque (3) est valable pour tout n et tout $x = a/m_o p^r$, $0 \leq x < 1$, on a que doit ètre identiquement nul.

<u>$h = 0$</u>: Encore par la formule (2) on a

$$(4) \quad \beta(x) = \beta_o \sum_{i=0}^{p^n-1} (x+i)^j \mod p^n\Delta^{-1}Z_p$$

$\beta(x)=\beta_o x^j+\dots$
$\beta_o \neq 0$

ce qui est aussi impossible, tenant compte des formules:

$$p^{nj}\beta(1/p^n) \equiv \beta_o \mod p^n\Delta^{-1}Z_p$$

et

$$p^{nj}\beta_o \sum_{o}^{p^n-1} (1/p^n +i)^j \equiv 0 \mod p^n\Delta^{-1}Z_p.$$

Existence:

Les polynomes de Bernoulli satisfont aux relations (1) ci-dessus: (loc.cit. exercice 3 p.150). Vous le trouvez un peu aride? pas tellement lumineux? Attendez parce qu'il y a d'autre moyen de voir que les polynomes de Bernoulli definissent des distributions.

c.q.f.d.

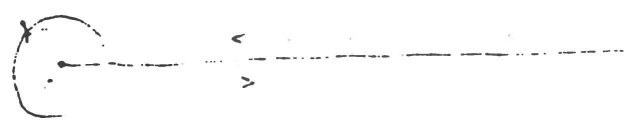
Alors, $L(1-k,f)$ est bien-définie pour k un entier ≥ 1 et on a

$$L(1-k,f) = -b_k(f)/k \ -f(0)\cdot\varepsilon/k$$

ou $\varepsilon = 1$ si $k = 1$ et $\varepsilon = 0$ sinon.

<u>Esquisse de la démonstration due, essentiellement, à Hurwitz</u>:

On prend le chemin d'intégration C



et la cle est à montrer

$$2\pi i\cdot \sum_{0}^{\infty} (n+a)^{-s} = \exp(-i\pi s)\,\Gamma(1-s)\int_C \frac{\exp(-az)}{1-\exp(-z)}\, z^{s-1}dz\ .$$

(provenant de la représentation intégrale pour l'inverse de la fonction Γ

$$1/\Gamma(s) = (2\pi i)^{-1}\int_{z\in C} e^{-z}(-z)^{-s}d(-z)$$

.... Référence? Faut-il le démontrer dans ce rapport?)
Parmi les livres qui se trouvent à côté de moi à l'instant, c'est dans Bieberbach <u>Lehrbuch Der Funktionentheorie</u> Vol. I dernière page.

Bon, dès que la clé est montrer on a presque gagné.

On obtient

$$L(s,f) = \sum_{0 < a \leq m} f(a) \cdot \sum_{n=0}^{\infty} (nm + a)^{-s}$$

$$= m^{-s} \sum_{a} f(a) \sum_{0}^{\infty} (n+a/m)^{-s}$$

$$= m^{-s} \frac{\exp(-i\pi s)}{2\pi i} \cdot \Gamma(1-s) \sum_{a} f(a) \int_{C} \frac{\exp(-(a/m)\cdot z)}{1 - \exp(-z)} z^{s-1} dz$$

où l'expression intégrale à droite donne la continuation analytique de la série de Dirichlet à gauche.

On met $s = 1-k$:

$$L(1-k,f) = (-1)^{k-1}(k-1)!\, m^{k-1} \sum_{a} f(a) \cdot \operatorname{Res}_{z=0} \left[\frac{\exp(-\frac{a}{m} \cdot z)}{1 - \exp(-z)} \cdot z^{-k} \right]$$

Vu la définition des polynomes de Bernoulli:

$$\frac{te^{Xt}}{e^{t} - 1} = \sum B_k(X)\, t^k/k!$$

on obtient

$$L(1-k,f) = -m^{k-1}/k \cdot \sum_{0 < a \leq m} f(a) \cdot B_k(a/m) = -b_k(f)/k - f(0) \cdot \varepsilon/k$$

n°592 34

ou $\varepsilon = m^{k-1}(B_k(1)-B_k(0))$.

Pour établir le théorème il ne faut que montrer

$$B_k(1) = B_k(0) \quad \text{si } k \;\; 2.$$

(en effet Bourbaki loc. cit. on a la relation de récurrence: $B_n(X+1) - B_n(X) = nX^{n-1}$)

c.q.f.d.

Proposition:

Soit $f: Z \to L$ une fonction periodique et définissons $f_-: Z \to L$ par $f_-(x) = f(-x)$. Alors,

$$b_k(f) = (-1)^k b_k(f_-) + f(0)\cdot\varepsilon$$

Démonstration:

$$\frac{z\sum_{0}^{m-1} f(a)\cdot e^{az}}{e^{mz}-1} = \frac{z\sum_{1}^{m} f(m-a)\cdot e^{(m-a)z}}{e^{mz}-1} = \frac{z'\sum_{1}^{m} f_-(a)\cdot e^{az'}}{e^{mz'}-1}$$

$b_k(f) = \sum m^{k-1} \sum_1$ c.q.f.d. $z' = -z$

(4.9) **Remarques:**

1. Si $f(0) = 0$ ou bien $k > 1$, on a

$$L(1-k,f) = -b_k(f)/k \qquad \text{et}$$

$$b_k(f) = (-1)^k b_k(f_-)\ .$$

En particulier si k est pair et f impaire

$$L(1-k,f) = 0$$
$$b_k(f) = 0$$

Si k est impair ($k>1$) et f paire on a la même chose.

2) Si $\chi : Z/m^* \to C^*$ est un homomorphisme, désignons par la même lettre la fonction périodique sur Z obtenue par

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

La fonction périodique χ est un <u>caractère de Dirichlet</u> et $L(s,\chi)$ est la <u>série L de Dirichlet</u>. Encore

$$L(1-k,\chi) = -b_k(\chi)/k.$$

3) Par la formule du théorème, $b_k(f)$ dépend de la fonction $f : Z \to C$ et non pas de la période m. Ca donne une autre méthode ~~de~~ pour voir que les E_k sont des distributions!

4) Considérons les distributions $E_k(\alpha)$ $\alpha \in T$ à valeurs dans Q. Rappelons $T = Z/m_o \times Z_p$. Soit c un élément inversible dans l'anneau T. Soit $E_k(c^{-1}\alpha)$ la nouvelle distribution qui provient de E_k par composition avec l'automorphisme $c^{-1} : T \to T$.

Soit $E_{k,c}$ la distribution sur T à valeurs dans Q définie par la formule

$$E_{k,c}(\alpha) = E_k(\alpha) - c^k E_k(c^{-1}\alpha) .$$

Pour le formulaire en bas de la page, fixons les notations suivantes:

Si $\alpha \in Z/m$, soit $a = \alpha$. Soit b l'entier unique tel que $0 \leq b < m$ et $cb \equiv a \bmod m$.

Ècrivons

$$cb = a + n_a m \text{ .}$$

Soit Δ_k = ppcm des dénominateurs des coefficients de $B_k(X)$.

(2.11) FORMULAIRE

A) $E_{0,c} = 0$ pour tout c (élément inversible dans T).

B) $$\boxed{E_{k,c}(\alpha) - d^k E_{k,c}(d^{-1}\alpha) = E_{k,d}(\alpha) - c^k E_{k,d}(c^{-1}\alpha)}$$

pour m quelconque, c,d, premier à m. ~~Aussi pour c,d,~~ ~~éléments inversibles dans T, où les E sont vues comme~~ ~~distributions sur T.~~ où les E sont vues comme distributions

C) $$\boxed{E_{1,c}(\alpha) = -n_a + (c-1)/2}$$

($E_{1,c}$ est vue comme distribution sur Z/m et c est premier à m)

D) $$\boxed{E_{k,c}(\alpha) \equiv k \cdot a^{k-1}(-n_a + (c-1)/2) \quad \bmod m\Delta_k^{-1}Z}$$

Démonstration:

Désignons par E_k la distribution sur Z/m definie par le k-ième polynome de Bernoulli B_k. On désigne par le même symbole la distribution définie par B_k sur $T = Z/m_o \times Z_p$. Appelons E_k la <u>k-ième distribution de Bernoulli</u>. C'est une distribution à valeurs dans Q.

<u>Exemple</u>:

$B_o = 1$; $E_o : Z/m \to Q$ est la distribution de Haar, $E_o(\alpha) = 1/m$.

$B_1 = X - 1/2$; $E_1 : Z/m \to Q$ est la distribution

$$\alpha \to \{\alpha\} - 1/2$$

<u>Definition</u>:

Soit L un corps de caracteristique O. Soit $f: Z \to L$ une fonction qui se factorise a travers Z/m pour un m convenable (f est une fonction <u>périodique</u>).

Le <u>k-ième hombre de Bernoulli</u> (<u>generalisé</u>) <u>associé à f</u> est

$$b_k(f) = \int_{Z/m} f \cdot E_k = m^{k-1} \sum_{j=0}^{m-1} B_k(j/m) \cdot f(j).$$

<u>Remarque</u>: Les $b_k(f)$ ne dépend ~~de~~ que $f: Z \to L$ et non pas de m. Cette dernière phrase équivaut à dire que E_k est une distribution.

(4.7) <u>Théoreme</u>: Soit $f: Z \to \mathbb{C}$ une fonction periodique, et notons par $\Gamma(s,f)$ ~~la continuation~~ analytique de la série

$$\sum_{0}^{\infty} f(n) \cdot n^{-s}$$ sur le plan complexe

Convention: $0^{-s} = 0$

Grace à la formule D) du formulaire pour $m = m_n$ (n suffisament grand tel que $m_n \Delta_k^{-1} \in Z_p$) on a gagné. Même dans le cas p=2; $c \equiv 1$ mod 2 et $(c-1)/2$ est dans Z_2.

c.q.f.d.

(4.1) Considérons le groupe de lie analytique $G = T^*$ des éléments inversibles dans $T = Z/m_0 \times Z_p$. En tant que espace topologique T^* est un ouvert fermé dans T.

Les caractères χ^z sur U_1 peuvent être considérés ~~comme~~ caractères sur T^* par la projection:

$$T^* = Z/m_0^* \times Z_p^* \to U_1$$

$$(\alpha, u) \longmapsto \langle u \rangle^z$$

Pour n un entier, posons $\chi_n : T^* \to Z_p^*$, le caractère défini par $(\alpha,u) \mapsto u^n$. Alors,

$$\chi_n = (\chi_1)^n$$

$$\chi_n = \chi^n \cdot \omega^n$$

où ω est le <u>caractère de Teichmuller</u>

$$Z_p^* \xrightarrow{\omega} \begin{cases} \text{racines } (p-1)\text{-ièmes d'unité} \subset Z_p^* & (p \neq 2) \\ \{\pm 1\} \subset Z_2^* & (p = 2) \end{cases}$$

Puisque $E_{k,c}$ est une mesure sur T à valeurs dans Z_p, sa restriction à $G = T^*$ donne une mesure sur G.

Théorème: $E_{k,c} = k\cdot \chi_{k-1}\cdot E_{1,c} = k\cdot \chi^{k-1}\cdot \omega^{k-1}\cdot E_{1,c}$
sur G

(Rappelons que le produit d'une mesure par une fonction continue est encore une mesure)

Démonstration:

Ça provient du formulaire (C + D). On pose $m = m_n$ et on laisse n tend vers l'infini dans la formule D.

c.q.f.d.

primitive

(qui contient une racine $\varphi(m_o)$-ième d'unité)

(4.15) Soit K une extension finie de Q_p (qui contient une racine $\varphi(m_o)$-ième d'unité primitive) et soit D son anneau d'entiers. Soit X le groupe analytique des caractères de $G = T^*$ à valeurs dans D^*. X est un groupe analytique sur K.

Pour f une fonction continue sur G à valeurs dans D, et $c \in G$ tel que $f(c) \neq 1$, posons

$$L(f) = \frac{1}{k(f(c)-1)} \cdot \int_G f(g)\chi_{-k}(g)\cdot E_{k,c}(g) \in K \qquad (4.16)$$

Lemme:

$L(f) \in K$ ne dépend pas du choix de c et de $k \geq 1$.

Démonstration: L'indépendance par rapport à c provient facilement de la formule B du formulaire. L'indépendance par rapport à $k \geq 1$ provient du théorème précédent.

On a alors:

$$L(f) = \frac{1}{f(c)-1}\int_G f(g)\,\chi_{-1}(g)\,E_{1,c}(g).$$

Écrivons aussi:

$$L(s,f) = L(\gamma^{1s}.f) \quad \text{pour } s \in D .$$

Pour $\gamma \in X$, $L(\gamma)$ s'exprime dans la formule ci-dessus comme quotient de fonctions d'Iwasawa sur X.

Autrement dit, $L(\gamma)$ est dans le corps de fractions de l'anneau d'Iwasawa $\Lambda = D[[G]]$ et en particulier, $L(\gamma)$ est une fonction <u>meromorphe</u> (à valeurs dans K) sur le groupe analytique X. $L(\gamma)$ est même <u>analytique</u> en dehors de $\gamma = 1$.

On a défini $L(f)$ au moyen du choix de m_0, p, et de K, mais c'est clair par la formule ci-dessus que le comportement de $L(f)$ par rapport aux changements des choix ne produit pas de surprises. A savoir: Si $m_0 \mid m_0'$ et $K \subset K'$

?

et si

$$\begin{array}{ccc} Z/m_0' \times Z_p & \xrightarrow{f'} & K' \\ {\scriptstyle \text{proj.}}\downarrow & & \uparrow{\scriptstyle \subseteq} \\ Z/m_0 \times Z_p & \xrightarrow{f} & K \end{array}$$

est un diagramme commutatif, alors $L(f') = L(f)$.

(4.17) <u>Définition</u>: $L(\psi)$ est <u>la série L</u> (<u>p-adique</u>) <u>de Kubota-Leopold</u>, (<u>sur X</u>).

(4.18) **Théorème:** Soit $\chi \in X$ d'ordre fini. Alors

$$L(1-k, \chi) = -b_k(\chi\omega^{-k})/k \qquad \text{pour } k \geqslant 1.$$

Démonstration:

$$L(1-k, \chi) = L(\chi\omega^{-k}) = L(\chi\omega^{-k}) = \frac{1}{k(f(c)c^k-1)} \int_G f(g)\cdot E_{k,c}(g)$$

où $f = \chi\omega^{-k}$. Puisque f est localement constante,

$$\int_G f(g)E_{k,c}(g) = \int_G f(g)E_k(g) - c^k \int_G f(g)E_k(c^{-1}g) \ .$$

Puisque f est un homomorphisme on fait le changement de variables dans l'intégrale à gauche et on obtient:

$$\int_G f(g)E_{k,c}(g) = (1- c^k f(c))b_k(f)$$

d'après (4.5).

c.q.f.d.

(4.19) **Remarques:**

1) Si $k \begin{cases} \equiv 0 \mod p-1 & (p \neq 2) \\ \equiv 0 \mod 2 & (p = 2) \end{cases}$,

$\omega^k = 1$, et par conséquent,

$$L(1-k, \chi) = -b_k(\chi)/k \ .$$

n° 592 42

2) Si ψ est un caractère ~~impair~~ impair il résulte du théorème précédent et de la remarque 1) que

$$L(1-k,\psi) = 0 \quad k \geqslant 1$$

Par conséquent,

$$L(s,\psi) = 0 \text{ (identiquement).}$$

3) La dénominateur de ψ. Soit $Dén(\psi) \in D$ un élément tel que

~~Posons~~

(*)

$$Dén(\psi) = \min_{c \in T^*} \|\psi(c)c^s - 1\| = \min_{c \in T^*}\left(\max_{k \in Z_p} \|\psi(c)c^k - 1\|\right).$$

Alors on a

$$Dén(\psi) \cdot L(s,\psi) \in \Lambda_s .$$

lorsque $D = Z_p$

On peut calculer $Dén(\psi)$ facilement: Si $T^* = F \times U_1$, n'importe quel caractère ψ sur T^* se décompose (uniquement)

$$\psi = \psi_{\text{modéré}} \times \psi_{\text{sauvage}}$$

ou $\psi_{\text{modéré}}$ s'annule sur U_1 et ψ_{sauvage} s'annule sur F.

$\frac{1}{c^s-1}$

(*)

Alors, si $D = Z_p$, la formule ci-dessus donne

$$\left|\text{Dén}(\psi)\right| = \min_{c} \left|\psi_{\text{modéré}}(c) - 1\right|$$

et puis on peut prendre $\text{Dén}(\psi) = 0,1$ suivant les cas que $\psi_{\text{modéré}}$ est le caractère trivial ou pas.

Par conséquent,

$$L(s,\psi) \in \Lambda_s$$

lorsque $D = Z_p$, et $\psi_{\text{modéré}}$ n'est pas le caractère trivial.

4) <u>Le pôle à $\psi = 1$</u>

Soit ψ le caractère trivial sur T^* ($\psi(\alpha) = 1$ pour $\alpha \in T$). Considérons

$$L(s,\psi) = 1/(\langle c\rangle^s - 1) \cdot \int_G \chi^{1-s} \cdot \chi_{-1} \cdot E_{1,c}$$

qui se développe en serie:

$$L(s,\psi) = \left[\frac{\int_G \chi_{-1} E_{1,c}}{\log \langle c\rangle}\right] \cdot \frac{1}{(s-1)} + \text{holomorphe en } s$$

Puisque $L(s,\psi)$ est indépendant de $c \in U_1 - 1$
on déduit que

$$(*) \quad \int_G \chi_{-1} E_{1,c} \quad = \quad R \cdot \log(c)$$

(en tant que fonctions de $c \in U_1 - 1$) ou R est un constante qui s'interprète comme ~~la~~ résidu de $L(s,\psi)$ à $s = 1$.

La question s'impose de calculer ~~la~~ résidu R. Calculé plus tard: [illegible]

Proposition: $R = \varphi(m_o p)/m_o p$ [illegible] (φ = la fonction phi
$\varphi(4m_o)/4m_o$ [illegible] d'Euler)

5) Comparaison avec la série L classique.

Soit F un corps qui s'identifie (à la fois) à un sous-corps du corps complexe $\mathbb{C}$ et à un sous-corps du corps K (une extension finie de Q_p). Soit ψ un caractère sur T^* d'ordre fini à valeurs dans F. On peut considérer ψ à la fois comme caractère de Dirichlet, et comme caractère à valeurs dans K.

Soient $L_C(s,\psi)$ la série L de Dirichlet et $L_K(s,\psi)$ la serie L de Kubota-Leopold. Alors,

$$L_K(1-k,\psi) = L_{\mathbb{C}}(1-k,\psi\omega^{-k}) \in F \qquad (k \geqslant 1)$$

et en particulier

$$(*) \quad L_K(1-k,\psi) = L_{\mathbb{C}}(1-k,\psi) \in F \qquad \left(k \geqslant 1, \begin{array}{l} k \equiv c \ (p-1) \text{ si } p \neq 2 \\ k \equiv c \ (2) \ \ldots \end{array}\right)$$

La formule (*) est une caractérisation de $L_K(s, \psi)$ comme fonction analytique en s.

<u>Démonstration</u>

D'après (4.18), (4.7), et le fait que l'ensemble des valeurs k décrit dans la formule (*) est dense dans Z_p.

5. La transformée de Kubota-Leopold

Définissons les composants du diggramme ci-dessous:

$$
\begin{tikzcd}
\mathbb{Z}_p[q] \arrow[rr, "\Gamma'_c"] \arrow[dd, "\subseteq"'] & & D[[q]] \arrow[d] \\
& & \Lambda_s \arrow[d] \\
\mathbb{Z}_p\{\{\bar{q}\}\} \arrow[rr, dashed] & & C_s
\end{tikzcd}
$$

Remarque : [illegible] & D quelconque [illegible]

(i) $Z_p[q]$: l'anneau des polynomes en q

(ii) $\bar{q} = q-1$

(iii) $Z_p\{\{\bar{q}\}\}$: l'anneau des séries formelles divisées en $\bar{q}$ à coefficients dans Z_p. C'est le sous-anneau de $Q_p[[\bar{q}]]$ des éléments de la forme

$$A = \sum_{0}^{\infty} a_n \gamma_n(\bar{q}) \qquad \gamma_n = \text{n-ième puissance divisée} \qquad a_n \in \mathbb{Z}_p.$$

tels que $\lim_{n\to\infty} a_n = 0$.

On met la norme suivante sur $Z_p\{\{\bar{q}\}\}$: Si $A \in Z_p\{\{\bar{q}\}\}$ est une série formelle divisée,

$$\|A\| = \sup_n |a_n| .$$

Alors $Z_p\{\{\bar{q}\}\}$ est un anneau complet par rapport à la norme.

(iv) C_s: l'anneau des fonctions continues en s à valeurs dans D_p. C'est un anneau complet pour la norme

$$\|f\| = \sup_{s \in Z_p} |f(s)| .$$

(v) Les morphismes verticals sont les morphismes naturels. L'application Γ est un homomorphisme de Z_p-<u>modules</u> (<u>pas</u> d'algèbres) défini par

$$\Gamma(q^n) = \begin{cases} \langle n \rangle & \text{si } (n,p)=1 \\ 0 & \text{sinon.} \end{cases}$$

Pour la proposition suivante je donne l'énoncé pour $p \neq 2$. Il n'y a pas beaucoup de changements nécessaire pour $p = 2$ mais ....

(5.2) <u>Proposition</u> : (i) Soit $p \neq 2$. L'homomorphisme Γ se prolonge à un homomorphisme continu de Z_p-modules

$$\Gamma : Z_p\{\{\bar{q}\}\} \rightarrow C_s$$

rendant le diagramme ci-dessus commutatif. On a

$$\|\Gamma A\| \leq \|A\| .$$

(2) Si $A(\bar{q}) \in Z_p\{\{\bar{q}\}\}$, substituons $\bar{q} = e^t - 1$, la série formelle en t. Ecrivons

$$A(e^t-1) = \Sigma\, B_k(A)\gamma_k(t).$$

Par $\operatorname{Lim}_{k \to s} B_k(A)$ pour $s \in Z_p$ on entend la limite prise pour n'importe quelle suite (strictement croissante) d'entiers k positifs tels que

$$k \equiv 0 \mod p-1$$

$$k \to s \quad \text{dans } Z_p .$$

Alors, $\lim\limits_{k \to s^*} B_k(A)$ existe pour $A \in Z_p\{\{\bar{q}\}\}$ et $s \in Z_p$

et

$$A(s) = \lim_{k \to s^*} B_k(A).$$

<u>Démonstration</u>:

On garde la terminologie de l'énoncé de la proposition et on se prépare en considérant la fonction

$$A_n(\bar{q}) = \bar{q}^n \qquad n \text{ entier.}$$

$$A_n(e^t-1) = (e^t-1)^n = \Sigma\, B_k(A_n)\, t^k/k!$$

où $B_k(A_n) = \sum\limits_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^k.$ (1)

Puisque,

$$B_k(A_n) = \left[\frac{d^k}{dt^k} (e^t-1)^n\right]_{t=0}$$

$$= \left[\frac{d^{k-1}}{dt^{k-1}} \left(n(e^t-1)^n + n(e^t-1)^{n-1}\right)\right]_{t=0}$$

$$= nB_{k-1}(A_n) + nB_{k-1}(A_{n-1}),$$

on voit par récurrence que $B_k(A_n)$ est un entier divisible par $n!$.

Nous appliquons ce qui précède ~~à~~ pour montrer

$$\|\Gamma_s(\bar{q}^n)\| = \|\Gamma A_n\| \leqslant |n!|$$

En effet,

$$\Gamma(\bar{q}^n) = \Gamma((q-1)^n) = \sum_{j=0}^{n} (-1)^{n-j}\binom{n}{j}\Gamma_s(q^j)$$

$$= \sum_{\substack{j=0\\(j,p)=1}}^{n} (-1)^{n-j}\binom{n}{j}\langle j\rangle^s \quad \in C_s^1 .$$

et par conséquent,

$$\|\Gamma(\bar{q}^n)\| \leqslant \max \left| \sum_{\substack{j=0\\(j,p)=1}}^{n} (-1)^{n-j}\binom{n}{j}\langle j\rangle^N \right|$$

ou N parcourt les entiers qui sont

(a) supérieur à un entier N_0 donne

(b) congrus à 0 mod p-1

parce que l'ensemble de tels entiers est dense dans Z_p.

Mais pour un tel N,

$$\sum_{\substack{j=0\\(j,p)=1}}^{n} (-1)^{n-j}\binom{n}{j}\langle j\rangle^N \equiv \sum_{j=0}^{n}(-1)^{n-j}\binom{n}{j}\, j^N = B_N(A_n) \quad \text{mod } p^{N_0}.$$

Puisque $B_N(A_u)$ est divisible par n!, la formule ci-dessus démontre bien l'inégalité

$$\| \Gamma(\bar{q}^u) \| < |n!|$$

si l'on prend N_o suffisament grand tel que $|p^N q| < |n!|$.

Définissons

$$\Gamma(\gamma_n(\bar{q})) = \Gamma(\bar{q}^u)/n! \quad \varepsilon\ C_s$$

et c'est immédiat que Γ s'étend par continuité à $Z_p\{\{\bar{q}\}\}$, satisfaisant à l'inégalité de normes énoncée.

Afin de démontrer la deuxième partie de la proposition, considérons n'importe quelle série

$$A(\bar{q}) = \sum_0^\infty a_n \gamma_u(\bar{q}) \varepsilon \quad Z_p\{\{\bar{q}\}\}.$$

C'est clair que.

$$B_k(A) = \sum_{n=0}^{\infty} a_n . B_k(A_u)/n!$$

où la convergence est assurée d'après ce qui précède. On en tire

$$| B_k(A) | \leq \| A \| .$$

La démonstration ~~est~~ sera conclue en deux étapes:

1. Lorsque $A = q^u$, , $B_k(A) = n^k$, et

$$\lim_{k \to s} B_k(A) = \begin{cases} \langle n \rangle^s & (u,p)=1 \\ 0 & p \mid u \end{cases} = \Gamma(A)(s)$$

Alors on a

$$\lim_{k \to s} B_k(A) = \Gamma A(s)$$

pour tout $A \in Z_p[q]$.

2. Pour n'importe quel $A \in Z_p\{\{q\}\}$ et $\varepsilon > 0$ prenons un polynome $A' \in Z_p[q]$ tel que

$$\|A'-A\| < \varepsilon$$

Alors

$$\|\Gamma A' - \Gamma A\| \leq \|\Gamma(A'-A)\| \leq \|A'-A\| < \varepsilon$$

$$\|B_k(A') - B_k(A)\| \leq \|B_k(A'-A)\| \leq \|A'-A\| < \varepsilon$$

et on obtient

$$\lim_{k \to s} B_k(A) = \Gamma A(s).$$

c.q.f.d.

L'application Γ s'étend aussi à l'espace vectoriel sur Q_p, $Q_p \otimes_{Z_p} Z_p\{\{\bar{q}\}\} \to Q_p \otimes_{Z_p} C_s$. Elle est appelée <u>la transformée de Kubota-Leopold</u>.

Q_p K quelconque

Soit $\theta : Z_p\{\{\bar{q}\}\} \to Z_p\{\{\bar{q}\}\}$ la dérivation définie par $\theta = q \cdot \log q \cdot d/dq$. Pour $A(\bar{q}) \in Z_p\{\{\bar{q}\}\}$ on a la formule

$$(\theta A)(e^t-1) = t\cdot d/dt\left[A(e^t-1)\right].$$

Il s'ensuit que

$$B_k(\theta A) = k\cdot B_k(A)$$

et, d'après la deuxième partie de la proposition ci-dessus, si $p \neq 2$,

(I) $\Gamma\theta A(s) = s.\Gamma A(s)$.

Il y a une deuxième formule utile:

(II) (<u>Évaluation à s=0</u>)

$$\Gamma A(0) = A(0) - 1/p \sum_{\zeta_p} A(\zeta_p-1)$$

ou $A(\bar{q}) \in Z_p\{\{\bar{q}\}\}$ et ζ_p parcourt les racines p-ième de l'unité. La serie $A(\zeta_p-1) = \sum_e a_n\gamma_n(\zeta_p-1)$ est convergente puisque la valeur absolue $\gamma_n(\zeta_p-1)$ est bornée (Exercise facile: $v_p(n!) < n/p-1$

$v_p(\zeta_p-1) \geq 1/p-1$)

Donc l'expression à gauche dans la formule (II) est définie. Puisque les deux côtés de (II) sont linéaires est continus en A il suffira de considérer $A(\bar{q}) = \bar{q}^n$ afin d'établir (II). Mais en ce cas on calcul les deux côtés de (II) et on obtient qu'ils sont 0 ou 1 suivant les cas $p \mid m$ ou $p \nmid m$.

Je termine ce rapport en ~~obtenant~~ [illegible] la série L de Kubota-Leopold comme la transformée de Kubota-Leopold de quelque chose ΓH. La série H est bien explicite et on en tirera la formule analytique de Leopold. Je travail toujours dans le cas $p \neq 2$, et on va restreindre la généralité un peu en plus.

Si un caractère $\chi : Z/m^* \to D^*$ ne se factorise pas à travers un quotient propre de Z/m^* on dit χ est primitif sur Z/m^* et on dit que m est la conducteur de χ.

Soit $m = m_\mu = m_0 p^\mu$ pour $n \geq 1$ et χ un caractère à valeurs dans D de conducteur m. Supposons que les racines m-ièmes de l'unité dans $\mathbb{Q}_p$ sont contenues dans D

On définit la somme de Gauss

$$\tau(\chi) = \sum_{a=0}^{m-1} \chi(a) \zeta^a$$

où ζ^a parcourt les racines m-ièmes de l'unité.

Ecrivons

$$G(\bar{q}, \chi) = G(\bar{q}) = \sum_{a=0}^{m-1} \frac{\chi(a) q^{a-1}}{q^m - 1}$$

Lemme 1:

$$G(\bar{q}) = \frac{\tau(\chi)}{m} \sum_{(a,m)=1} \frac{\chi(a^{-1})}{q - \zeta^a}$$

Démonstration:

Si $g(q) = \sum_{\substack{0 \\ (a,m)=1}}^{m-1} \chi(a) q^{a-1}$

est la numérateur de G, on démontre facilement

$$G(\overline{q}) = \frac{g(q)}{q^m - 1} = \sum_{0}^{m} \frac{\zeta^a}{m} \cdot \frac{g(\zeta^a)}{q - \zeta^a}$$

et puisque $\zeta^a g(\zeta^a) = \sum \chi(b) \zeta^{ab} = \chi(a^{-1}) \tau(\chi)$

on a gagné.

cqfd

Lemme 2:

Il existe une série $H(\overline{q}) \in K \otimes_{Z_p} Z_p \{\{ q \}\}$ satisfaisant les propriétés suivantes:

(i) $dH/dq = -G(\overline{q}, \chi)$.

(ii) $\Gamma H(s) = L(1-s, \chi)$

Corollaire:

$$L(1,\chi) = -\frac{\tau(\chi)}{m} \sum_{\substack{0 \\ (a,m)=1}}^{m-1} \chi(a^{-1}) \log_p(1-\zeta^a)$$

où $\log_p$ = le logarithme p-adique.

Esquisse de la démonstration du lemme:

On emploie l'expression pour G donnée dans le lemme 1 et la formule

$$d/dq(\log(q-\zeta^a)) = d/dq(\log(1-\zeta^a + \bar{q}) = 1/(q-\zeta^a).$$

Puisque $1-\zeta^a$ est une unité p-adique lorsque $(a,m)=1$,

$$\log(1-\zeta^a + \bar{q}) \in D\{\{\bar{q}\}\}$$

et on prend

$$(*) \quad H = -\frac{\tau(\chi)}{m} \Sigma \chi(a^{-1})\log(q-\zeta^a) .$$

Maintenant il faut démontrer (ii). On a

$$(\theta H)(e^t-1) = -te^tG(e^t-1) = -\Sigma \frac{\chi(a)t.e^{at}}{e^{mt}-1}$$

$$= -\Sigma\, b_k(\chi)\gamma_k(t)$$

et alors $B_k(H) = -b_k(\chi)/k$ ~~d'après (I)~~ et

$$\Gamma H(s) = \lim_{k \to s} -b_k(\chi)/k = L(1-s,\chi).$$

c.q.f.d.

<u>Esquisse de la démonstration du corollaire</u>:

Appliquons la formule (II) et (*) ci-dessus afin d'évaluer $\Gamma H(0)$.

FIN