Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Jean Fresnel

Applications arithmétiques de la formule p-adique des résidus

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 8, n° 2 (1966-1967), exp. n° 18, p. 1-8

<http://www.numdam.org/item?id=SDPP_1966-1967__8_2_A8_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
8e année. 1966/67, n° 18

17 avril 1967

APPLICATIONS ARITHMÉTIQUES DE LA FORMULE p-ADIQUE DES RÉSIDUS

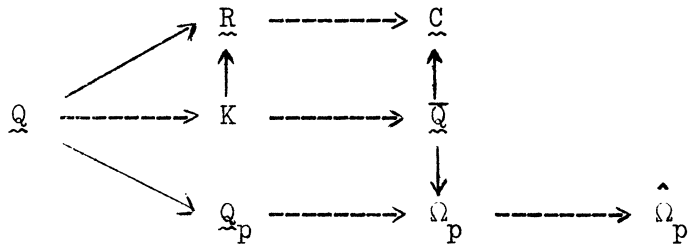
par Jean FRESNEL

1. Introduction.

Le but de cet exposé est de montrer comment interviennent les fonctions L p-adiques dans le calcul du nombre de classes d'idéaux (§ 2), et comment la théorie de ces fonctions éclaire certains résultats déjà connus sur le nombre de classes d'idéaux et en simplifie considérablement la démonstration (§ 3 et 4).

2. Formule des résidus.

Soient $\underset{\sim}{R}$ le corps des réels, $\underset{\sim}{C}$ le corps des nombres complexes, $\overline{\underset{\sim}{Q}}$ une clôture algébrique du corps $\underset{\sim}{Q}$ des nombres rationnels, K une extension abélienne réelle de $\underset{\sim}{Q}$, $\underset{\sim}{Q}_p$ le corps p-adique élémentaire, Ω_p une clôture algébrique de $\underset{\sim}{Q}_p$, et $\hat{\Omega}_p$ un complété de Ω_p avec les inclusions suivantes (les flèches signifient les inclusions) :



D'autre part, soit $\hat{A}_p$ (resp. $\hat{\mathfrak{M}}_p$) l'anneau (resp. l'idéal) de valuation de $\hat{\Omega}_p$. Notons par $\log_\infty$ la fonction logarithme de $\underset{\sim}{R}$, et par $\log_p$ le prolongement fonctionnel [6] à $\hat{A}_p - \hat{\mathfrak{M}}_p$ du logarithme p-adique défini sur $1 + \hat{\mathfrak{M}}_p$. Soient $|\ |_\infty$ la valeur absolue de $\underset{\sim}{C}$ et $|\ |_p$ la valeur absolue de $\hat{\Omega}_p$.

Soient A la clôture intégrale de $\underset{\sim}{Z}$ dans K, et U le groupe des unités de A. Si $n = [K : \underset{\sim}{Q}]$, nous savons que U est le produit direct du sous-groupe cyclique $U_0 = \{1, -1\}$ d'ordre 2 par le sous-groupe libre U_1 de rang $r = n - 1$. Soient G le groupe de Galois de K sur $\underset{\sim}{Q}$, $G^* = G - \{e\}$ (e est l'élément neutre de G), $(e_i)_{1\leq i\leq r}$ une base du U_1, nous savons que l'expression

$$\det(\log_\infty |e_i^\sigma|_\infty)_{1\leq i\leq r,\, \sigma\in G^*} \tag{1}$$

est indépendante, au signe près, du choix de la base.

Le régulateur p-adique $R_p(K)$ est défini par

$$R_p(K) = \det(\log_p e_i^{\sigma})_{1\leqslant i\leqslant r,\sigma\in G^*} \ .$$

On choisit la base $(e_i)_{1\leqslant i\leqslant r}$ et l'ordre des (σ) de façon que l'expression (1) soit positive.

A. BRUMER vient récemment de montrer le résultat suivant [3] :

THÉORÈME. - Le régulateur p-adique de toute extension abélienne réelle est non nul.

Ce problème avait été soulevé par H.-W. LEOPOLDT [9] dans un contexte que nous allons brièvement rappeler.

A tout caractère primitif χ nous associons la quantité $L_p(\chi)$ définie de la façon suivante :

Si $f(\chi) \neq p^e$, $\forall\ e \in \mathbb{N}$ ($f(\chi)$ est le conducteur du caractère χ) ,

$$L_p(\chi) = -\frac{\tau(\chi)}{f(\chi)} \sum_{a=1}^{f(\chi)} \overline{\chi}(a) \log_p(1 - Z_{f(\chi)}^a) \ .$$

Si $f(\chi) = p$,

$$L_p(\chi) = -\frac{\tau(\chi)}{f(\chi)} \frac{1}{p-1} \sum_{a=1}^{p} \overline{\chi}(a) \log_p\left(\frac{(1 - Z_p^a)^{p-1}}{-p}\right) \ .$$

Si $f(\chi) = p^e$, avec $e \geqslant 2$,

$$L_p(\chi) = \frac{\tau(\chi)}{f(\chi)} \frac{1}{p} \sum_{a=1}^{p^e} \overline{\chi}(a) \log_p\left[\frac{(1 - Z_{p^e}^a)^p}{(1 - Z_{p^{e-1}}^a)}\right] \ .$$

Nous désignons par $Z_{f(\chi)}$ une racine primitive $f(\chi)$-ième de l'unité, et par $\tau(\chi)$ la somme de Gauss définie par

$$\tau(\chi) = \sum_{a=1}^{f(\chi)} \chi(a)\, Z_{f(\chi)}^a \ .$$

H.-W. LEOPOLDT [9] a montré que si K est un corps abélien réel, le nombre de classes, le régulateur p-adique et les quantités $L_p(\chi)$ sont reliées par la formule

$$(2) \qquad \frac{2^{n-1}\, h_K\, R_p(K)}{\sqrt{d_K}} = \prod_{\chi\in\mathfrak{X}} L_p(\chi) \ .$$

Le discriminant du corps K est d_K, et $\sqrt{d_K}$ est parfaitement déterminé par les inclusions $\underset{\sim}{Q} \to \underset{\sim}{R}$ et $\overline{\underset{\sim}{Q}} \to \Omega_p$. D'autre part, h_K est le nombre de classes de K (c'est-à-dire l'indice du sous-groupe des idéaux principaux de A dans le groupe des idéaux de A). Le problème posé par H.-W. LEOPOLDT [9] était le suivant :

Existe-t-il des couples (χ , p) pour lesquels $L_p(\chi) = 0$?

Le théorème de Brumer permet immédiatement de dire que :

$$L_p(\chi) \neq 0 \quad \text{quels que soient} \quad \chi \neq \varepsilon \quad \text{et} \quad p \quad \text{premier} .$$

Soit $L(. , \chi)$ la fonction de Dirichlet complexe, nous voyons alors que $L_p(\chi)$ n'est autre que le pendant p-adique de la valeur $L(1 , \chi)$. Nous avons une relation analogue avec les fonctions $L_p(. , \chi)$.

THÉORÈME. - Quels que soient le caractère $\chi \neq \varepsilon$, et le nombre premier p, nous avons

$$L_p(1 , \chi) = (1 - \frac{\chi(p)}{p}) L_p(\chi) .$$

Ce théorème fut annoncé par H. W. LEOPOLDT [7] ; pour une démonstration, on peut consulter [1], et aussi [5] dans un cas particulier.

Ce résultat permet d'écrire la formule (2) sous la forme

$$(3) \qquad \frac{2^{n-1} h_K R_p(K)}{\sqrt{d_K}} = \prod_{\chi \neq \varepsilon} (1 - \frac{\chi(p)}{p})^{-1} L_p(1 , \chi) .$$

Le résidu de la fonction zêta p-adique du corps K peut être exprimé par la formule (3)

$$(4) \qquad \frac{2^{n-1} h_K R_p(K)}{\sqrt{d_K}} = \Big(\prod_{\mathfrak{P} | p} (1 - N(\mathfrak{P})^{-1}) \Big) \Big(\lim_{s \to 1} (s - 1) \zeta_p(s , K) \Big) .$$

Le théorème de Brumer montre alors que le résidu de la fonction $\zeta_p(. , K)$, en $s = 1$, est non nul, par suite cette fonction admet, pour $s = 1$, un pôle simple.

Nous allons donner deux applications de la formule du résidu.

3. Première application [8].

Les notations étant les mêmes qu'au § 2, nous supposons que $p \neq 2$, et que p n'est pas ramifié (c'est-à-dire que $p \nmid d_K$).

Exprimons la formule (3) modulo p . Il nous suffit donc d'évaluer $L_p(1 , \chi)$ mod p , évaluation qui nous est donnée par les nombres de Bernoulli [4]. Nous avons

$$L_p(1 , \chi) \equiv - \frac{B^{p-1}(\chi\omega^0)}{p - 1} \mod p \ ;$$

Soit

$$L_p(1 , \chi) \equiv - \frac{B^{p-1}(\chi)}{p - 1} \mod p \ .$$

Par suite, la formule (3) s'écrit

$$(5) \qquad \frac{2^{n-1} h_K R_p(K)}{\sqrt{d_K}} \prod_{\chi \neq \varepsilon} \left(1 - \frac{\chi(p)}{p}\right) \equiv \prod_{\chi \neq \varepsilon} \frac{B^{p-1}(\chi)}{1 - p} \mod p \ .$$

Puisque p n'est pas ramifié

$$\left|\frac{\mathrm{Log}_\omega e^\sigma}{p}\right|_p \leqslant 1 \quad \text{si} \quad \sigma \in G \quad \text{et si} \quad e \in U \ .$$

Ainsi $\left|\frac{R_p(K)}{p^{n-1}}\right| \leqslant 1$, et la formule (5) s'écrit

$$\frac{2^{n-1} h_K}{\sqrt{d_K}} \frac{R_p(K)}{p^{n-1}} \prod_{\chi \neq \varepsilon} \chi(p) \equiv \prod_{\chi \neq \varepsilon} \frac{B^{p-1}(\chi)}{p - 1} \mod p \ ,$$

or $\prod_{\chi \neq \varepsilon} \chi(p) = \pm 1$, et par suite

$$2^{n-1} h_K \frac{R_p(K)}{p^{n-1}} \equiv \pm \prod_{\chi \neq \varepsilon} B^{p-1}(\chi) \mod p \ .$$

Cette congruence nous donne la proposition suivante

PROPOSITION. - Soient K une extension abélienne réelle dans laquelle l'idéal (p) ($p \neq 2$) n'est pas ramifié, h_K le nombre de classes d'idéaux, nous avons alors l'implication suivante :

$$(p \mid h_K) \implies (p \mid \prod_{\chi \neq \varepsilon} B^{p-1}(\chi)) \ .$$

On voit que la réciproque est vraie si

$$(6) \qquad p \nmid \frac{R_p(K)}{p^{n-1}} \ .$$

Nous allons énoncer des conditions sous lesquelles (6) est satisfaite. Soient φ la surjection canonique de A sur $A/p^2 A$

$$B = \{x \in A \mid (x , p) = 1\}$$

$$C = \{x \in A \mid x \equiv 1 \mod p\}$$

$$C^* = \{x \in C \mid N_{K|Q}(x) = 1\} .$$

Nous avons les inclusions suivantes des groupes multiplicatifs :

$$\varphi(C^*) \subset \varphi(C) \subset \varphi(B) \quad \text{et} \quad \varphi(U) \subset \varphi(B) .$$

THÉORÈME [8]. - Soit K une extension abélienne réelle dans laquelle l'idéal (p) $(p \neq 2)$ n'est pas ramifié. Si $p \nmid [K : Q]$ et si $\varphi(C^*) \subset \varphi(U)$, alors

$$p \nmid \frac{R_p(K)}{p^{n-1}} .$$

Preuve. - Soit $C_0 = \{x \in C \mid (\exists\, \alpha \in \mathbb{N}) x \equiv (1 + p)^{\alpha} \mod p^2\}$. Nous avons

$$\varphi(C) = \varphi(C^*) \times \varphi(C_0) . \tag{7}$$

Posons par définition,

$$R_p(a_1 , \ldots , a_n) = \det(\log_p a_i^{\sigma})_{1 \leq i \leq n, \sigma \in G} ,$$

$a_i \in K$, $|a_i|_p = 1$ et $n = [K : Q]$.

Soient $(e_i)_{1 \leq i \leq n-1}$ un système générateur de U_1, et $e_n = 1 + p$ alors,

$$\frac{1}{p^n} R_p(e_1 , \ldots , e_n) \equiv \pm \frac{n}{p^{n-1}} R_p(K) \mod p .$$

Soient $(\omega_i)_{1 \leq i \leq n}$ une base du $\mathbb{Z}$-module A et $C_i = 1 + p\omega_i$, $1 \leq i \leq n$. Ainsi

$$\frac{1}{p^n} R_p(C_1 , \ldots , C_n) \equiv \det(\omega_i^{\sigma})_{1 \leq i \leq n, \sigma \in G} = \pm \sqrt{d_K} \mod p .$$

D'après la décomposition (7), il existe $(a_i^j)_{1 \leq i \leq n, 1 \leq j \leq n}$, $a_i^j \in \mathbb{Z}$ tel que

$$\varphi(C_i) = \prod_{j=1}^{m} \varphi(e_j)^{a_i^j} \qquad 1 \leq i \leq n$$

et par suite

$$\frac{1}{p}\log_p C_i \equiv \sum_{j=1}^{n} a_i^j \frac{1}{p}\log_p e_j \mod p \qquad 1 \leqslant i \leqslant n$$

$$\frac{1}{p^n} R_p(C_1, \ldots, C_n) \equiv \det(a_i^j)\frac{1}{p^n} R_p(e_i) \equiv \pm \frac{n}{p^{n-1}} R_p(K) \mod p$$

Soit

$$\pm\sqrt{d_K} \equiv n \det(a_i^j) \frac{R_p(K)}{p^{n-1}} \mod p \ .$$

Ce qui prouve que $p \nmid \dfrac{R_p(K)}{p^{n-1}}$.

4. Deuxième application [10].

Les notations étant les mêmes qu'au § 2, nous supposons de plus que $K = \mathbb{Q}(\sqrt{d})$ est une extension quadratique réelle de discriminant d, avec $d = pn$, $p \neq 2$.

Soient

$$e = \frac{t + u\sqrt{d}}{2} \qquad t, u \in \mathbb{Z}$$

une unité fondamentale telle que $|e|_\infty > 1$, et χ le caractère primitif, quadratique modulo n .

La formule (3) s'écrit

$$\frac{2h_K \log_p e}{\sqrt{d_K}} = L_p(1, \theta^{(p-1)/2}\chi) .$$

Nous avons les égalités évidentes

$$e = \frac{t + u\sqrt{d}}{2} = \frac{t}{2}\left(1 + \frac{u}{t}\sqrt{d}\right) ,$$

$$\frac{t^2}{4} - d\frac{u^2}{4} = \varepsilon = \pm 1 \qquad (t, p) = 1 ,$$

$$\frac{t^2}{4} = \varepsilon\left(1 + \varepsilon d \frac{u^2}{4}\right) ,$$

et par suite

$$\log_p e = \frac{1}{2}\log_p\left(1 + \varepsilon\frac{du^2}{4}\right) + \log_p\left(1 + \frac{u}{t}\sqrt{d}\right)$$

$$\omega\left(\frac{2h_K \log_p e}{\sqrt{d}}\right) = \omega(h_K u) \quad ,$$

ω étant la valuation p-adique.

Posons

$$\ell = \omega(h_K u) = \omega(L_p(1 , \theta^{(p-1)/2} \chi)) \quad .$$

D'après [4],

$$L_p(1 , \chi\theta^{(p-1)/2}) \equiv - \frac{B^n(\chi\theta^{(p-1)/2} \theta^{-n})}{n} \mod p^{\ell} \text{ si } p^{\ell-1} | n \quad .$$

Ainsi

$$L_p(1 , \chi\theta^{(p-1)/2}) \equiv - \frac{B^{((p-1)/2)p^{\ell-1}}(\chi\theta^{C})}{\frac{p-1}{2} p^{\ell-1}} \mod p^{\ell} \quad ,$$

nous avons alors le résultat suivant :

THÉORÈME. - Soient $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique réel, de discriminant d, avec $d = pn$, χ le caractère quadratique primitif modulo n, h_K le nombre de classes d'idéaux de K et

$$e = \frac{u + t\sqrt{d}}{2} \quad ,$$

une unité fondamentale, alors

$$(p^{\ell} | h_K u) \iff \left(p^{\ell} \mid \frac{B^{((p-1)/2)p^{\ell-1}}}{\frac{p-1}{2} p^{\ell-1}}\right) \quad .$$

Remarquons que le nombre de Bernoulli peut être explicité par la congruence [4] :

$$\frac{B^{((p-1)/2)p^{\ell-1}}(\chi)}{\frac{p-1}{2} p^{\ell-1}} \equiv \frac{1}{\frac{p-1}{2} p^{\ell-1} p^{\nu} n} \sum_{a=1}^{p^{\ell} n} \chi(a) a^{((p-1)/2)p^{\ell-1}} \mod p^{\ell} \quad .$$

Si $p \nmid h_K$ (ce que l'on sait en particulier si $n < p$ puisque $h_K < \sqrt{d}$), alors

$$(p^{\ell} | u) \iff \left(p^{\ell} \mid \frac{B^{((p-1)/2)p^{\ell-1}}(\chi)}{\frac{p-1}{2} p^{\ell-1}}\right) .$$

Dans ce cas,

$$\frac{2h_K \log_p e}{\sqrt{d}} \equiv 2h_K \frac{u}{t} \mod p^{2\ell+1/2} \quad .$$

or

$$L_p(1 , \chi\theta^{(p-1)/2}) \equiv - \frac{B^{((p-1)/2)p^{2\ell}}(\chi)}{(\frac{p-1}{2})\, p^{2\ell}} \mod p^{2\ell+1} \quad .$$

Puisque $2h_K \frac{u}{t}$ et $B^{((p-1)/2)p^{2\ell}}(\chi)$ sont rationnels, nous avons

$$2h_K \frac{u}{t} \equiv - \frac{B^{((p-1)/2)p^{2\ell}}(\chi)}{(\frac{p-1}{2})\, p^{2\ell}} \mod p^{2\ell+1} \quad ,$$

quel que soit $\ell \geq 0$.

En particulier si $\ell = 0$, nous retrouvons le résultat [2].

$$h_K \frac{u}{t} \equiv B^{(p-1)/2}(\chi) \mod p \quad .$$

BIBLIOGRAPHIE

[1] AMICE (Yvette). - Sur un résultat de Léopoldt, Acta Arithm., Warszawa (à paraître).

[2] ANKENY (N. C.), ARTIN (E.) and CHOWLA (S.). - The Class-number of real quadratic number field, Annals of Math., Series 2, t. 56, 1952, p. 479-493.

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

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

[5] FRESNEL (J.). - Fonctions zeta p-adique des corps de nombres abéliens réels, Conférence prononcée en 1967, aux Journées arithmétiques de Grenoble.

[6] KRASNER (Marc). - Prolongement analytique uniforme et multiforme dans les corps valués complets, Colloques internationaux du C. N. R. S. : Les tendances géométriques en algèbre et théorie des nombres [143. 1964. Clermont-Ferrand], p. 91-141. - Paris, Centre national de la Recherche scientifique, 1966.

[7] KUBOTA (Tomio) und LEOPOLDT (Heinrich-Wolfgang). - Eine p-adische Theorie der Zetawerte, I : Einführung der p-adischen Dirichletschen L-Funktionen, J. für reine und angew. Math., t. 214-215, 1964, p. 328-339.

[8] LEOPOLDT (Heinrich-Wolfgang). - Über Fermatquotienten von Kreiseinheiten und Klassenzahlformeln modulo p , Rend. Cir. mat. Palermo, Serie 2, t. 9, 1960, p. 39-50.

[9] LEOPOLDT (Heinrich-Wolfgang). - Zur Aritmetik in abelschen Zahlkörpern, J. für reine und angew. Math., t. 209, 1962, p. 54-71.

[10] SLAVUTSKY (I. S.). - On Mordell's theorem, Acta Arithm., Warszawa, t. 11, 1965/66, p. 57-56.