

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

GERMAINE REVUZ

Ordre et indice modulo les puissance d'un idéal premier

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 15, n° 2 (1973-1974),
exp. n° G8, p. G1-G4

http://www.numdam.org/item?id=SDPP_1973-1974__15_2_A5_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1973-1974, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

ORDRE ET INDICE MODULO LES PUISSANCE D'UN IDÉAL PREMIER

par Germaine REVUZ

1. Ordre.

1° Dans $\underline{\mathbb{Z}}$. - Soient p un nombre premier, a un entier naturel, différent de ± 1 , non divisible par p . L'ordre $\omega(h)$ de a dans le groupe multiplicatif $(\mathbb{Z}/p^h \mathbb{Z})^*$ peut être donné par la formule

$$\omega(h) = \omega(h_0) p^{h-h_0} \text{ avec } \omega(h_0) \neq \omega(h_0 + 1), \quad h_0 > \frac{1}{p-1}$$

(la restriction $h_0 > 1/(p-1)$ n'intervenant que dans le cas $p = 2$).

2° Dans l'anneau A des entiers d'un corps de nombre L . - Soit \mathfrak{p} un idéal premier de A au-dessus de l'entier naturel p , l'indice de ramification étant e et le degré résiduel de l'extension f . Soit $a \in A$, $a \notin \mathfrak{p}$ et a non racine de 1. L'ordre $\omega(h)$ de a dans le groupe multiplicatif $(A/\mathfrak{p}^h)^*$ est donné par la formule

$$\omega(h) = \omega(h_1) p^{\lfloor (h-h_1)/e \rfloor} \text{ pour } h \geq h_1,$$

avec $h_1 = h_0 + 1$, $\omega(h_0) \neq \omega(h_0 + 1)$, $h_0 > e/(p-1)$.

Sur cette formule on voit que a est générateur de $(A/\mathfrak{p}^h)^*$ si, et seulement si, il est générateur de $(A/\mathfrak{p}^{h_0})^*$, et si $e = f = 1$. Il en résulte que $(A/\mathfrak{p}^h)^*$ est cyclique si, et seulement si, $e = f = 1$, $p \neq 2$.

2. Indice d'un élément relativement à un autre.

1° Dans $\underline{\mathbb{Z}}$. - Soit, avec les mêmes notations que ci-dessus, un autre élément c , non divisible par p , et soit $\alpha(h)$ le plus petit entier tel que $a^{\alpha(h)} \equiv c \pmod{p^h}$. Posons, pour simplifier l'écriture, $\omega(h_0) = \omega_0$, $\alpha(h_0) = \alpha_0$.

PROPOSITION 1. - Si $\alpha(h_0)$ existe, alors $\alpha(h)$ existe pour tout h , et est donné par la formule

$$\alpha(h) = \alpha_0 + \omega_0 \beta_{h-h_0-1} \text{ pour } h \geq h_0 + 1,$$

où β_n désigne le développement de Hensel p -adique limité au terme en p^n de $\beta = (\log ca^{-\alpha_0}) / (\log a^{\omega_0})$ ces logarithmes étant pris au sens p -adique.

Exemple de calcul.

$$p = 5, \quad a = 2, \quad c = 3$$

$$h_0 = 1, \quad \omega_0 = 4, \quad \alpha_0 = 3$$

$$\beta = \frac{\log 3/8}{\log 16} = \frac{\log(1 - 5/8)}{\log(1 + 5 \times 3)} = \frac{\overline{03331} \dots}{\overline{03300} \dots} = \overline{1011} \dots \quad (\text{Développements } 5\text{-adique}).$$

On en déduit

$$\begin{aligned}\alpha(2) &= \alpha(1) + \omega_0 \times 5^0 = 7 \\ \alpha(3) &= \alpha(2) \\ \alpha(4) &= \alpha(3) + \omega_0 \times 5^2 = 107 \\ \alpha(5) &= \alpha(4) + \omega_0 \times 5^3 = 607, \text{ etc.}\end{aligned}$$

2° Dans l'anneau A des entiers d'un corps de nombre L. - Soit, avec les mêmes notations qu'au §1, 2°, $c \in A$, $c \notin p$, et soit encore $\alpha(h)$ le plus petit entier naturel tel que

$$a^{\alpha(h)} \equiv c \pmod{p^h}.$$

(a) Cas $e = f = 1$. - L peut être plongé dans $\underline{\mathbb{Q}}_p$.

La proposition 1 reste valable. (Le calcul de β se faisant sur les éléments de $\underline{\mathbb{Q}}_p$, images des éléments de L dans le plongement.)

Exemple de calcul.

$$\begin{aligned}L &= \underline{\mathbb{Q}}(i\sqrt{5}), \quad p = 3, \quad \mathfrak{p} = (3, 2 + i\sqrt{5}), \\ a &= 2i\sqrt{5}, \quad c = i\sqrt{5}, \quad h_0 = 1, \quad \omega_0 = 2, \quad \alpha_0 = 2,\end{aligned}$$

$i\sqrt{5}$ s'identifiant à $\overline{12021} \dots$

$$\beta = \frac{\log(-i\sqrt{5}/20)}{\log(-20)} = \frac{\log(1 + \overline{00002} \dots)}{\log(1 - \overline{012})} = \overline{0001} \dots \quad (\text{Développements } 3\text{-adiques}).$$

On en déduit

$$\begin{aligned}\alpha(1) &= \alpha(2) = \alpha(3) = \alpha(4) = 2 \\ \alpha(5) &= \alpha(4) + 2 \times 3^3 = 56 \dots \text{ etc.}\end{aligned}$$

(b) Cas e ou $f \neq 1$. - Le processus de calcul de $\alpha(h)$ peut s'arrêter même si $\alpha(h_0)$ existe.

Définition. - Nous appelons couple privilégié d'éléments de A un couple (a, c) tel que $\alpha(h)$ existe pour tout h.

Nous remarquons que, cette fois, L est plongé dans une extension \hat{L} de $\underline{\mathbb{Q}}_p$ et nous avons le résultat suivant.

PROPOSITION 2. - Pour que (a, c) soit un couple privilégié, il est nécessaire que $\alpha(h_0)$ existe, et que $\beta = (\log ca^{-\alpha_0}) / (\log a^{\omega_0})$ soit dans $\underline{\mathbb{Q}}_p$.

Remarque 1. - En fait, $v_p(\beta) \geq 0$ et, si $\beta \in \underline{\mathbb{Q}}_p$, alors $\beta \in \underline{\mathbb{Z}}_p$.

Remarque 2. - Dans le cas où L est galoisien sur $\underline{\mathbb{Q}}$, la condition $\beta \in \underline{\mathbb{Q}}_p$, peut être mise sous la forme : β est invariant par les automorphismes prolongeant à \hat{L} ceux du groupe de décomposition de p dans L. En particulier si p est inerte dans L, β doit être invariant par tous les automorphismes prolongeant ceux du

groupe de Galois de L sur $\underline{\mathbb{Q}}$.

PROPOSITION 3. - Les conditions de la proposition 2 sont suffisantes pour que (a, c) soit privilégié si L ne contient pas de zéros de la fonction logarithme p -adique et on a alors, pour tout $h \geq h_1$,

$$\alpha(h) = \alpha_0 + \omega_0 \beta_n \text{ avec } \left[\frac{h - h_1}{e} \right] = n$$

où β_n est le développement limité à la puissance n -ième de β .

Cette proposition s'applique en particulier quand $e = 1$, ou plus généralement quand e n'est pas divisible par $p - 1$.

(c) Cas où a et c sont multiplicativement dépendants sur $\underline{\mathbb{Z}}$.

$$a^r = c^s, \quad r \in \underline{\mathbb{Z}}, \quad s \in \underline{\mathbb{Z}}.$$

Si α_0 existe, alors $\beta = ((r - \alpha_0 s) / (\omega_0 s)) \in \underline{\mathbb{Q}} \cap \underline{\mathbb{Z}}_p$, et β a un développement périodique.

PROPOSITION 4. - Si a et c sont $\underline{\mathbb{Z}}$ -multiplicativement dépendants et si $\alpha(h_0)$ existe, le couple (a, c) est privilégié sauf, peut-être, si L contient des zéros de la fonction logarithme p -adique et si r et s sont divisibles par p .

Question : Dans ce cas exceptionnel ($p|r$, $p|s$, L contient des racines p -ièmes de l'unité), α_0 peut-il exister ?

Remarque. - Dans le cas où s'applique la proposition 4, on obtient une expression explicite de $\alpha(h)$.

Exemple dans $\underline{\mathbb{Z}}$:

$$p = 5, \quad a = 8, \quad c = 4, \quad a^2 = c^3,$$

$$h_0 = 1, \quad \omega_0 = 4, \quad \alpha_0 = 2,$$

$$\beta = -\frac{1}{3} = \overline{31313} \dots \text{ (Développement 3-adique).}$$

D'où

$$\text{pour } h \text{ impair, } \alpha(h) = \frac{2 + 4 \times 5^{h-1}}{3},$$

$$\text{pour } h \text{ pair, } \alpha(h) = \frac{2 + 8 \times 5^{h-1}}{3}.$$

Exemple dans $L = \underline{\mathbb{Q}}(\sqrt{3})$:

$$p = \sqrt{3}A, \quad a = (1 + \sqrt{3})^2, \quad c = (1 + \sqrt{3})^3,$$

$$e = 2, \quad h_0 = 3, \quad \omega_0 = 3, \quad \alpha_0 = 3,$$

$$\beta = -\frac{1}{2} = \overline{1111} \dots \text{ (Développement tri-adique).}$$

D'où

$$\alpha(h) = \alpha_0 + \omega_0 \beta_{\left[\frac{h-4}{2}\right]} = \frac{3 + 3^{\left[\frac{h}{2}\right]}}{2} \text{ pour } h \geq 2.$$

Notons qu'on peut retrouver, à partir de là, le résultat suivant qui est un cas particulier d'un théorème de Gelfond ([1], th. II') : si a et c sont des entiers algébriques multiplicativement dépendants, si p est un idéal premier de l'anneau des entiers de leur corps, auquel ils n'appartiennent pas, et si la congruence

$$a^x \equiv c \pmod{p^y}$$

a une infinité de solutions en (x, y) , alors il existe une constante $\tau(p, a, c)$ telle que

$$y < \tau \log x$$

(ce qui, avec nos notations, signifie $((\log \alpha(h))/h) > \frac{1}{\tau}$).

BIBLIOGRAPHIE

- [1] GELFOND (A.). - Sur la divisibilité de la différence des puissances de deux nombres entiers par les puissances d'un idéal premier, Mat. Sbornik, Nouv. Série, t. 7, 1940, p. 7-25.

(Texte reçu le 19 février 1974)

Mme Germaine REVUZ
 Mathématiques
 Université de Poitiers
 40 avenue du Recteur Pineau
 86022 POITIERS
