Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Jean-René Joly

Sommes de puissances m-ièmes dans les anneaux β-adiques et les anneaux d'entiers algébriques

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 10, n° 2 (1968-1969), exp. n° 16, p. 1-8

<http://www.numdam.org/item?id=SDPP_1968-1969__10_2_A3_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
10e année, 1968/69, n° 16

5 mai 1969

SOMMES DE PUISSANCES m-ièmes DANS LES ANNEAUX $\mathfrak{P}$-ADIQUES ET LES ANNEAUX D'ENTIERS ALGÉBRIQUES

par Jean-René JOLY

1. Introduction.

Pour tout anneau commutatif et unitaire A et tout entier positif m, nous désignerons par A_m^+ l'ensemble des éléments de A de la forme

$$a_1^m + a_2^m + \dots + a_s^m \tag{1}$$

(s positif quelconque, $a_1, a_2, \dots, a_s \in A$), et par A_m l'ensemble des éléments de A de la forme

$$\pm a_1^m \pm a_2^m \pm \dots \pm a_s^m \tag{2}$$

(avec également s positif quelconque, et $a_1, a_2, \dots, a_s \in A$) ; il est clair que A_m est le sous-anneau de A engendré par les puissances m-ièmes des éléments de A. Nous désignerons d'autre part par $w(m ; A)$ le plus petit entier s tel que tout élément de A_m^+ puisse se mettre sous la forme (1), et par $v(m ; A)$ le plus petit entier s tel que tout élément de A_m puisse se mettre sous la forme (2) (bien entendu, il n'est pas exclu a priori que $w(m ; A)$ ou $v(m ; A)$ soit infini ; voir par exemple dans [8], théorème (7.30), la construction d'un corps L tel que $w(m ; L)$ soit infini pour tout exposant pair m).

L'étude par des méthodes purement algébriques des constantes $w(m ; A)$ et $v(m ; A)$, et la recherche de conditions permettant d'affirmer que $A = A_m$, ont été entreprises notamment par BIRCH, RAMANUJAM et nous-mêmes (voir respectivement [3], [9], [7]) dans le cas où A est un anneau $\mathfrak{P}$-adique, et par SIEGEL, BATEMAN, STEMMLER, BHASKARAN et nous-mêmes dans le cas où A est un anneau d'entiers algébriques (voir respectivement [10], [1], [11], [2], [6]). Naturellement, l'étude de $w(m ; A)$ lorsque A est un anneau d'entiers algébriques (ou un corps de nombres algébriques) est étroitement apparentée au problème de Waring, qui a fait depuis une cinquantaine d'années l'objet de travaux fort nombreux ; mais ces travaux reposent presque exclusivement sur l'application de techniques analytiques et, faute de compétence suffisante en ce domaine, nous nous abstiendrons de les envisager ici.

En fait, le but de cet exposé est de résumer les résultats actuellement connus (connus de l'auteur, bien entendu) relatifs à $w(m ; A)$, $v(m ; A)$, et A_m , dans le cas où A est un anneau $\mathfrak{P}$-adique (paragraphe 2) et dans le cas où A est un anneau d'entiers algébriques (paragraphe 3), puis de les compléter en donnant de $v(m ; A)$ une majoration explicite et indépendante de A , toujours dans le cas où A est un anneau d'entiers algébriques (théorème (3.3), démontré au paragraphe 4) ; ce dernier résultat est une conséquence presque immédiate d'un résultat de RAMANUJAM (théorème (2.3)), dont la démonstration, donnée dans [9], est d'ailleurs longue et délicate.

2. Sommes de puissances m-ièmes dans un anneau $\mathfrak{P}$-adique.

Pour des raisons de commodité, adoptons une notation : si p est un nombre premier, si $q = p^f$ $(f \geqslant 1)$ est un nombre p-primaire, et si m est un entier positif quelconque, nous désignerons par le symbole $[q ; m]$ le plus petit nombre p-primaire p^g ayant les deux propriétés suivantes :

- L'exposant g divise l'exposant f ;
- Le quotient $(p^f - 1)/(p^g - 1)$ divise l'entier m .

On a alors ce résultat élémentaire (pour une démonstration, voir par exemple [8], théorème (2.3)) :

LEMME (2.1). - *Soit $k = \mathbb{F}_q$ le corps fini à $q = p^f$ éléments. Si m est un entier positif, k_m est égal au sous-corps de k contenant exactement $[q ; m]$ éléments :*

$$k_m = \mathbb{F}_{[q;m]} .$$

Ces préliminaires étant posés, désignons par A un anneau $\mathfrak{P}$-adique (c'est-à-dire un anneau de valuation discrète complet d'inégales caractéristiques à corps résiduel fini), et soient k le corps résiduel de A , $q = p^f$ le nombre d'éléments de k , et e l'indice de ramification absolu de A .

THÉORÈME (2.2) (voir [8], théorème (2.19)). - *Les deux assertions suivantes sont équivalentes :*

(a) $A = A_m$;
(b) $k = k_m$, *et de plus, si p divise m , A est absolument non ramifié.*

Compte tenu du lemme (2.1), l'égalité $A = A_m$ équivaut donc à la condition "numérique" ci-dessous :

(c) $[q\ ;\ m] = q$, et de plus, si p divise m , $e = 1$.

Ajoutons deux choses : tout d'abord, dans un anneau $\mathfrak{P}$-adique, -1 est toujours somme de puissances m-ièmes (voir par exemple [8], théorème (6.19)) : l'égalité $A = A_m$ implique donc, en fait, que tout élément de A est somme de puissances m-ièmes ; par ailleurs, même lorsque $A \neq A_m$, A_m est un anneau local, séparé, complet, de dimension 1 (mais non intégralement clos), et A est un A_m-module de type fini (voir [8], prop. (3.14)).

THÉORÈME (2.3) (voir [9], prop. 3). - On a la majoration suivante, indépendante de l'anneau ($\mathfrak{P}$-adique) A :

$$w(m\ ;\ A) \leqslant 8m^5 \ .$$

Signalons que BIRCH a donné, par une méthode complètement différente, la majoration (également indépendante de A) $w(m\ ;\ A) \leqslant m^{16m^2}$; par ailleurs, nous avons prouvé nous-mêmes que si m est premier impair, on a la majoration plus précise $w(m\ ;\ A) \leqslant 2m - 1$ (voir respectivement [3], théorème 1, et [8], théorème (7.34)).

3. Sommes de puissances m-ièmes dans un anneau d'entiers algébriques.

Soient maintenant A un anneau d'entiers algébriques, K le corps des fractions de A , et d le discriminant de K ; pour tout idéal premier non nul p de A , convenons de désigner par c_p la caractéristique de $A/p = A_p/pA_p$, par e_p et f_p l'indice de ramification absolu et le degré résiduel absolu de A_p , et par Np le nombre d'éléments de $A/p = A_p/pA_p$; on a donc $Np = c_p^{f_p}$.

THÉORÈME (3.1) (voir [2], théorème 1, d'une part ; et [6], théorème 5, ou [8], théorème (4.11), d'autre part). - Les deux assertions suivantes sont équivalentes :

(a) $A = A_m$;

(b) Pour tout idéal premier non nul p de A , on a $A/p = (A/p)_m$, et de plus, si c_p divise m , on a $e_p = 1$.

Notons que, compte tenu du lemme (2.1) et du lien entre discriminant et ramification, l'égalité $A = A_m$ équivaut ici encore à une condition "numérique" :

(c) Pour tout idéal premier non nul p de A , on a l'égalité $[Np\ ;\ m] = Np$, et, de plus, m est étranger au discriminant d .

(La condition $[Np\ ;\ m] = Np$ est d'ailleurs automatiquement vérifiée dès que $c_p > m$; il n'y a donc, en fait, qu'un nombre fini de vérifications numériques à effectuer, pour voir si un couple $(A\ ,\ m)$ satisfait à la condition (c).)

Le théorème (3.1) a été démontré pour la première fois par SIEGEL pour $m = 2$ (voir [10], théorème V), et par BATEMAN et STEMMLER pour m premier quelconque (voir [1], théorème 3). En ce qui concerne le cas général, la démonstration donnée par BHASKARAN est de type arithmétique en ce sens qu'elle s'appuie sur des calculs de congruences modulo des puissances d'idéaux premiers ; elle utilise d'ailleurs certains des résultats obtenus par BATEMAN et STEMMLER dans [1] et [11] ; la démonstration du théorème (3.1) que nous donnons nous-mêmes dans [6] est au contraire de type algébrique : elle consiste à noter que $A = A_m$ si, et seulement si, $A_\mathfrak{p} = (A_\mathfrak{p})_m$ pour tout idéal premier $\mathfrak{p}$ non nul de A, puis que $A_\mathfrak{p} = (A_\mathfrak{p})_m$ si, et seulement si, $\hat{A}_\mathfrak{p} = (\hat{A}_\mathfrak{p})_m$; comme $\hat{A}_\mathfrak{p}$ est un anneau $\mathfrak{P}$-adique, il suffit alors d'utiliser le théorème (2.2). Naturellement, les deux démonstrations sont essentiellement équivalentes ; remarquons simplement que les techniques de l'algèbre commutative (localisation, complétion, etc.) sont particulièrement bien adaptées au type de problème envisagé ici ; nous aurons d'ailleurs une nouvelle occasion de le constater au paragraphe suivant.

THÉORÈME (3.2) (voir [2], théorème 1). - *Pour tout entier positif* m, *il existe un entier* $b(m)$ *tel qu'on ait la majoration*

$$v(m\ ;\ A) \leqslant b(m)\ ,$$

pour tout anneau d'entiers algébriques A.

Ce théorème est tout-à-fait analogue au théorème (2.3), à ceci près qu'il ne nous donne pas d'ordre de grandeur pour la quantité majorante. Nous allons combler cette lacune en démontrant le résultat suivant :

THÉORÈME (3.3). - *Quels que soient l'entier positif* m *et l'anneau d'entiers algébriques* A, *on a l'inégalité*

$$v(m\ ;\ A) \leqslant 2^m + 8m^5\ .$$

Le théorème (3.3) généralise l'inégalité

$$v(m\ ;\ A) \leqslant 2^{m-1} + (m-1)/3 + 1\ ,$$

obtenue par STEMMLER (voir [11]), dans le cas où l'exposant m est premier ; l'ordre de grandeur est seulement un peu moins bon : 2^m au lieu de 2^{m-1} (ceci tient au fait qu'on est obligé, dans le cas général, d'envisager les valeurs paires de m).

4. Démonstration du théorème (3.3).

LEMME (4.1). - Soient A un anneau, m un entier positif, et B un anneau quotient de A . On a alors l'inégalité

$$v(m ; B) \leqslant v(m ; A) \quad .$$

LEMME (4.2). - Soient A_1 , A_2 , ... , A_r des anneaux en nombre fini, et soit B leur produit. On a alors l'inégalité

$$w(m ; B) \leqslant \sup_{1 \leqslant i \leqslant r} w(m ; A_i) \quad .$$

La démonstration de ces deux lemmes est immédiate ; signalons seulement que le lemme (4.2) devient faux si on y remplace w par v (comme on le voit sur l'exemple suivant : $r = 2$, $m = 2$, et $A_1 = A_2 = \underset{\sim}{R}$).

LEMME (4.3). - Soient A un anneau, m et s deux entiers positifs, et α un idéal de A ayant la propriété suivante : Tout élément de α est de la forme

(3) $$\pm a_1 \pm a_2 \pm \ldots \pm a_s \qquad (a_1 , a_2 , \ldots , a_s \in A) \ ;$$

on a alors l'inégalité

$$v(m ; A) \leqslant s + v(m ; A/\alpha) \quad .$$

Il suffit pour le voir d'appliquer la définition de $v(m ; A)$.

LEMME (4.4). - Soient A un anneau d'entiers algébriques, m et n deux entiers positifs, et p un idéal premier non nul de A . On a alors l'inégalité

$$w(m ; A/p^n) \leqslant 8m^5 \quad .$$

Prouvons ce lemme : p étant en fait un idéal maximal de A , on a un isomorphisme canonique

$$A/p^n \simeq A_p/p^n A_p$$

(voir [4], chap. II, § 3, n° 3, prop. 9) ; mais on a également un isomorphisme canonique

$$A_p/p^n A_p \simeq \hat{A}_p/p^n \hat{A}_p$$

(voir [4], chap. III, § 2, n° 12, formules (21), et n° 13, prop. 19). A/p^n est donc isomorphe à un quotient de $\hat{A}_p$, d'où, en appliquant le lemme (4.1),

$$w(m\ ;\ A/p^n) \leqslant w(m\ ;\ \hat{A}_p) \quad ;$$

le lemme (4.4) résulte alors du théorème (2.3), et du fait que $\hat{A}_p$ est un anneau $\mathfrak{P}$-adique.

Venons-en alors à la démonstration du théorème (3.3). Soient A un anneau d'entiers algébriques, et m un entier positif ; l'identité bien connue (voir par exemple [5], théorème 402)

$$(4) \qquad m!\ a = \sum_{h=0}^{m-1} \binom{m-1}{h} (-1)^{m-1-h}((a+h)^m - h^m)$$

montre que tout élément de l'idéal $\alpha = m!\ A$ est de la forme (3) (voir lemme (4.3)) avec

$$s = 2 \sum_{h=0}^{m-1} \binom{m-1}{h} = 2.2^{m-1} = 2^m \quad ;$$

le lemme (4.3) donne donc l'inégalité

$$v(m\ ;\ A) \leqslant 2^m + v(m\ ;\ A/\alpha) \quad .$$

D'autre part, dans A/α, qui est un anneau fini, -1 est somme de puissances m-ièmes, d'où évidemment l'inégalité

$$v(m\ ;\ A/\alpha) \leqslant w(m\ ;\ A/\alpha) \quad .$$

Il suffit donc en fait de prouver l'inégalité

$$(5) \qquad w(m\ ;\ A/\alpha) \leqslant 8m^5 \quad ;$$

or, dans A, qui est un anneau de Dedekind, l'idéal α se décompose en facteurs premiers :

$$\alpha = p_1^{n_1}\ p_2^{n_2} \dots\ p_r^{n_r}$$

(les p_i premiers non nuls et deux à deux distincts, les $n_i > 0$), et le "théorème chinois" (voir par exemple [4], chap. II, § 1, n° 2, prop. 5) donne un isomorphisme canonique

$$A/\alpha \simeq (A/p_1^{n_1}) \times (A/p_2^{n_2}) \times \dots \times (A/p_r^{n_r}) \quad ;$$

l'inégalité (5) résulte alors immédiatement des lemmes (4.2) et (4.4). Et le théorème (3.3) se trouve démontré.

Deux remarques pour terminer :

(a) Tout d'abord, si l'exposant m est <u>impair</u>, on peut, au lieu de (4), utiliser l'identité

$$(6) \qquad m!\,(a + (m-1)/2) = \sum_{h=0}^{m-1} \binom{m-1}{h} (-1)^{m-1-h}(a+h)^m \quad ,$$

qui n'en est d'ailleurs qu'une écriture différente ; la démonstration ci-dessus mène alors à la majoration plus précise

$$v(m\ ;\ A) \leqslant 2^{m-1} + 8m^5 \quad .$$

(b) Si maintenant l'exposant m est <u>premier impair</u>, l'inégalité (5) peut être remplacée par celle-ci :

$$(7) \qquad w(m\ ;\ A/\alpha) \leqslant 2m - 1 \quad ;$$

il suffit pour le voir d'appliquer le résultat signalé dans les dernières lignes du paragraphe 2. Remplaçant dans la démonstration ci-dessus l'identité (4) par l'identité (6) et la majoration (5) par la majoration (7), on obtient alors l'inégalité

$$v(m\ ;\ A) \leqslant 2^{m-1} + 2m - 1 \quad ,$$

toujours pour un anneau d'entiers algébriques A, bien entendu.

BIBLIOGRAPHIE

[1] BATEMAN (P. T.) and STEMMLER (R. M.). - Waring's problem for algebraic number fields and primes of the form $(p^r - 1)/(p^d - 1)$, Illinois J. of Math., t. 6, 1962, p. 142-156.

[2] BHASKARAN (M.). - Sums of m^{th} powers of algebraic and abelian number fields, Arch. der Math., t. 17, 1966, p. 497-504.

[3] BIRCH (B. J.). - Waring's problem for $\mathfrak{P}$-adic number fields, Acta Arithm., Warszawa, t. 9, 1964, p. 169-176.

[4] BOURBAKI (N.). - Algèbre commutative. Chap. 1-2, 3-4, 5-6, 7. - Paris, Hermann, 1961-1965 (Act. scient. et ind., 1290, 1293, 1303, 1314 ; Bourbaki, 27, 28, 30, 31).

[5] HARDY (G. H.) and WRIGHT (E. M.). - The theory of numbers. 3rd edition. - Oxford, Clarendon Press, 1954.

[6] JOLY (J.-R.). - Sur les puissances d-ièmes des éléments d'un anneau commutatif, C. R. Acad. Sc. Paris, t. 261, 1965, p. 3259-3262.

[7] JOLY (J.-R.). - Sur le problème de Waring pour un exposant premier dans certains anneaux locaux, C. R. Acad. Sc. Paris, t. 262, 1966, Série A, p. 1438-1441.

[8] JOLY (J.-R.). - Etude des sommes de puissances dans les anneaux commutatifs, Thèse Sc. math. Orsay, 1968.

[9] RAMANUJAM (C. P.). - Sums of m^{th} powers in $\mathfrak{P}$-adic rings, Mathematika, London, t. 10, 1963, p. 137-146.

[10] SIEGEL (C. L.). - Sums of m^{th} powers of algebraic integers, Annals of Math., Series 2, t. 46, 1945, p. 313-339.

[11] STEMMLER (R. M.). - The easier Waring problem in algebraic number fields, Acta Arithm., Warszawa, t. 6, 1961, p. 447-468.

(Texte reçu le 5 mai 1969)

Jean-René JOLY
Faculté des Sciences de Grenoble
Institut de Mathématiques pures
Boîte postale 116
38 - SAINT-MARTIN-d'Hères