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

ristiques 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], th. (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^{iemes} (voir par exemple [8], th. (6.19)): l'égalité $A = A_m$ implique donc en fait que tout élément de A est somme de puissances m^{iemes}; 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:

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

Signalons que Birch a donné, par une méthode complètement différente, la majoration (également indépendante de A) $w(m; A) \leqq m^{16m2}$; par ailleurs, nous avons prouvé nous-même que si m est *premier impair*, on a la majoration plus précise $w(m; A) \leqq 2m-1$ (voir respectivement [3], th. 1, et [8], th. (7.34)).

3. Sommes de puissances m^{iemes} 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 $\mathfrak{p}$ de A, convenons de désigner par c_p la caractéristique de $A/\mathfrak{p} = A_p/\mathfrak{p}A_p$, par e_p et f_p l'indice de ramification absolu et le degré résiduel absolu de A_p, et par $N\mathfrak{p}$ le nombre d'éléments de $A/\mathfrak{p} = A_p/\mathfrak{p}A_p$; on a donc $N\mathfrak{p} = c_p{}^f p$.

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

(a) $A = A_m$;

(b) Pour tout idéal premier non nul $\mathfrak{p}$ de A, on a $A/\mathfrak{p} = (A/\mathfrak{p})_m$, 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 $\mathfrak{p}$ de A, on a l'égalité $[N\mathfrak{p}; m] = N\mathfrak{p}$, et *de plus*, m est étranger au discriminant d.

(La condition $[N\mathfrak{p}; m] = N\mathfrak{p}$ 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], th. V) et par Bateman et Stemmler pour m premier quelconque (voir [1], th. 3). En ce qui concerne le cas général, la démonstration donnée dans [2] 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-même dans [6] est au contraire de type *algébrique*: elle consiste à noter que $A = A_m$ si et seulement si $A_p = (A_p)_m$ pour tout idéal premier $\mathfrak{p}$ non nul de A, puis que $A_p = (A_p)_m$ si et seulement si $\hat{A}_p = (\hat{A}_p)_m$; comme $\hat{A}_p$ 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, ...) 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], th. 1). Pour tout entier positif m, il existe un entier $b(m)$ tel qu'on ait la majoration

$$v(m; A) \leqq b(m)$$

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:

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

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

Le théorème (3.3) généralise l'inégalité

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

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

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

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

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

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 $A_1 = A_2 = \mathbf{R}$).

Lemme (4.3.) Soient A un anneau, m et s deux entiers positifs et $\mathfrak{a}$ un idéal de A ayant la propriété suivante:

tout élément de $\mathfrak{a}$ est de la forme

$$\pm a_1^m \pm a_2^m \pm \ldots \pm a_s^m \qquad (a_1, a_2, \ldots, a_s \in A); \tag{4}$$

on a alors l'inégalité

$$v\,(m; A) \leqq s + v\,(m; A/\mathfrak{a}).$$