ACTA ARITHMETICA
XVII (1970)

Sommes de puissances d-ièmes dans un anneau commutatif

par

JEAN-RENÉ JOLY (Grenoble)

INTRODUCTION

Indiquons tout d'abord quelques conventions et notations.

Conventions générales

(1) Les symboles $\boldsymbol{F}_q$, $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$, $\boldsymbol{Z}_p$, $\boldsymbol{Q}_p$, ... auront leur signification habituelle: corps fini à q éléments, anneau des entiers rationnels, corps des nombres rationnels, corps des nombres réels, corps des nombres complexes, anneau des entiers rationnels p-adiques, corps des nombres rationnels p-adiques, ...

(2) *Anneau* signifiera toujours *anneau commutatif à élément unité*; *homomorphisme* (d'anneaux) signifiera de même *homomorphisme unitaire*; *module* signifiera *module unitaire*; *sous-anneau* (d'un anneau donné) signifiera *sous-anneau contenant l'élément unité de l'anneau en question*; etc...

(3) Si A est un anneau, A^* désignera le groupe multiplicatif des éléments inversibles de A. Si A est un anneau local et si x est un élément de A, $\overline{x}$ désignera l'image canonique de x dans le corps résiduel de A.

Conventions particulières

(4) La lettre d représentera en principe un exposant entier $\geqslant 1$. Si A est un anneau, on utilisera alors les notations suivantes:

A^d désignera l'ensemble des éléments de A de la forme a^d, avec $a \in A$;

A_d^+ désignera l'ensemble des éléments de A de la forme

$$(*) \qquad a_1^d + a_2^d + \ldots + a_n^d,$$

avec $n \geqslant 1$ quelconque et $a_1, a_2, \ldots, a_n \in A$;

A_d désignera l'ensemble des éléments de A de la forme

$$(**) \qquad e_1 a_1^d + e_2 a_2^d + \ldots + e_n a_n^d,$$

avec $n \geqslant 1$ quelconque, $e_1 = \pm 1$, $e_2 = \pm 1$, ..., $e_n = \pm 1$, et $a_1, a_2, \ldots, a_n \in A$.

On a évidemment $A^d \subset A_d^+ \subset A_d \subset A$, et A_d est le sous-anneau de A engendré par A^d.

(5) Soit x un élément de A_d^+; si, pour un entier n donné, x est de la forme (*), on dira qu'*il est somme de n puissances d-ièmes*; de même, si x est un élément de A_d et si, pour un entier n donné, x est de la forme (**), on dira qu'*il s'exprime* (ou qu'*il est représentable*) *à l'aide de n puissances d-ièmes*.

(6) Soient toujours A un anneau et d un entier $\geqslant 1$.

On désignera par $w(d; A)$ le plus petit entier n (s'il en existe) tel que tout élément de A_d^+ soit somme de n puissances d-ièmes; sinon, on posera $w(d; A) = \infty$.

On désignera de même par $v(d; A)$ le plus petit entier n (s'il en existe) tel que tout élément de A_d s'exprime à l'aide de n puissances d-ièmes; sinon, on posera $v(d; A) = \infty$.

Enfin, si, dans l'anneau A, -1 appartient à A_d^+, on désignera par $u(d; A)$ le plus petit entier n tel que -1 soit somme de n puissances d-ièmes; sinon, on conviendra de poser $u(d; A) = \infty$.

Le nombre $w(d; A)$ étend à un anneau commutatif quelconque A la notion de *constante de Waring*; de même, le nombre $v(d; A)$ généralise la notion de *constante de Waring "facile"*: les Anglo-Saxons appellent en effet "Easier Waring Problem" l'étude de la constante $v(d; A)$ lorsque A est un anneau d'entiers algébriques (voir par exemple [25]).

Ces conventions et notations étant fixées, décrivons maintenant le contenu de ce travail; il se décompose en deux parties d'égale importance:

La première partie (chapitres 1 à 5) est l'étude des relations existant entre un anneau quelconque A et son sous-anneau A_d (d étant supposé fixé). Les résultats les plus typiques nous semblent être les théorèmes (2.8), (2.13) et (2.19), au chapitre 2, et les théorèmes (4.8) et (4.11), au chapitre 4; pour plus amples détails, voir le texte.

La deuxième partie (chapitres 6 et 7) est l'étude des constantes $u(d; A)$, $v(d; A)$ et $w(d; A)$ (d étant également supposé fixé). Les résultats les plus dignes d'intérêt nous paraissent être les théorèmes (6.15) et (6.16), au chapitre 6, et les théorèmes (7.23), (7.25), (7.26), (7.30) et (7.32), au chapitre 7; ici encore, pour plus amples détails, voir le texte.

Ces deux parties ne sont naturellement pas indépendantes; ainsi, si pour un anneau A et un entier d donnés, on sait d'après la première partie que $A = A_d$, et d'après la deuxième que $u(d; A) < \infty$, c'est-à-dire que -1 est somme de puissances d-ièmes dans A, alors on pourra conclure que $A = A_d^+$, c'est-à-dire que tout élément de A est somme de puissances d-ièmes: c'est là un type de résultat que nous conviendrons de considérer comme intéressant.

Les chapitres 1 à 7 sont suivis d'un appendice: il contient quelques identités algébriques dont nous faisons un usage constant au cours de ce travail, et que nous avons préféré dégager du corps même du texte; le lecteur aura néanmoins intérêt à y jeter un coup d'oeil avant de s'attaquer au chapitre 1.

Les résultats obtenus dans ce travail sont pour la plupart nouveaux: en ce qui concerne la première partie, cela tient à ce que l'étude systématique de l'anneau A_d dans le cadre le plus général n'avait pas été entreprise jusqu'à présent, à notre connaissance du moins; en ce qui concerne la deuxième partie, cela provient du fait que nous nous sommes placés dans une situation où le recours aux méthodes analytiques de la Théorie des Nombres n'est plus possible: or, la majeure partie des résultats relatifs au Problème de Waring a été obtenue précisément à l'aide de techniques analytiques dérivées des travaux de Hardy et Littlewood. A ce propos, indiquons que la plupart de nos démonstrations s'appuient

d'une part, sur les identités données en appendice;

d'autre part et surtout, sur les résultats les plus classiques de l'Algèbre Commutative, telle qu'elle est exposée dans [5] ou dans [28] (dépendance intégrale, localisation, ...); en fait (voir par exemple la démonstration du théorème (4.11) par passage du local au global, ou celle du théorème (7.36) par application du théorème de structure des anneaux artiniens), il apparaît que les techniques de l'Algèbre Commutative sont particulièrement bien adaptées aux problèmes étudiés dans ce travail.

Signalons également ici que nous avons tiré le plus grand profit de la lecture des articles [2], [3], [6], [23] et [26], dont l'objet est très voisin de celui de ce travail.

Toutes les fois qu'un résultat est cité dans le texte, ou qu'un théorème plus ou moins connu est utilisé au cours d'une démonstration, une référence aussi précise que possible est donnée: un numéro entre crochets renvoie le lecteur à la bibliographie, placée à la fin du texte, après l'appendice. D'autre part, pour faciliter le repérage des divers éléments de ce travail, nous avons tout numéroté (ou presque), exemples et remarques aussi bien que théorèmes et propositions: les numéros sont du type (a.b), a désignant le chapitre (ou, pour a = 8, l'appendice), et b désignant la proposition, remarque, ..., à l'intérieur de ce chapitre.

Paris–Orsay, avril 1968

Un incident imprévisible, d'ordre matériel, a retardé de plusieurs mois la publication de ce travail; pour éviter une perte de temps supplémentaire, nous avons laissé le manuscrit tel qu'il était: signalons seulement que nous avons eu connaissance, dans l'intervalle, d'un article de Bhaskaran (*Sums of m-th powers of algebraic integers*, Archiv der Mathematik, 17 (1966), p. 497–504) où l'auteur donné une démonstration (d'ailleurs complétement différente de celle proposée ici) du théorème (4.11), ainsi que d'un article de Pfister (*Zur Darstellung definiter Funktionen als Summe von Quadraten*, Inventiones mathematicae, 4 (1967), p. 229–237) où l'auteur prouve que si L est le corps des fractions rationnelles à n indéterminées sur un corps réel maximal, alors $w(2; L) \leqslant 2^n$; indiquons aussi que nous avons, pendant cette période, donné une démonstration du résultat suivant: quels que soient A, anneau d'entiers algébriques, et d, exposant positif, on a la majoration $v(d; A) \leqslant 2^d + 8d^5$ (*Sommes de puissances dans les anneaux P-adiques et dans les anneaux d'entiers algébriques*, L'Enseignement mathématique, à paraître); comblons enfin une lacune dans la bibliographie en signalant que les résultats de Pfister relatifs aux sommes de carrés dans un corps commutatif, exposés par Cassels en 1964 au Colloque C.N.R.S. de Clermont–Ferrand (voir [6]) ont été publiés par Pfister lui-même en 1965 dans les deux articles suivants:

Darstellung von -1 *als Summe von Quadraten in einem Körper*, Journal London Mathematical Society 40 (1965), p. 159–165;

Multiplikative quadratische Formen, Archiv der Mathematik 16 (1965), p. 363–370.

Grenoble, mars 1969

TABLE DES MATIÈRES

I. Chapitre 1. Généralités relatives à A_d (p 41).
1. Quelques propriétés évidentes. 2. Le foncteur $A \mapsto A_d$.

Chapitre 2. Détermination de A_d dans certains cas importants (p. 44).
1. Détermination de k_d lorsque k est un corps fini. 2. Détermination de A^d lorsque A est une algèbre sur un corps infini K. 3. Etude de la condition $A_d = A$ pour un anneau local A.

Chapitre 3. Stabilité de la finitude de A/A_d (p. 50).
1. Passage à une extension de type fini. 2. Passage à un localisé ou à un complété.

Chapitre 4. Localisation et globalisation (p. 57).
1. Généralités; passage à un anneau de fractions. 2. Le théorème de globalisation. 3. Le cas intègre. 4. Application: condition $A = A_d$ pour un anneau d'entiers algébriques A.

Chapitre 5. Correspondance entre idéaux de A et de A_d (p. 62).
1. Généralités. 2. Correspondance entre idéaux premiers. 3. Correspondance entre modules projectifs de rang 1. 4. Cas intègre: correspondance entre idéaux inversibles. 5. Cas d'un anneau de Dedekind.

II. Chapitre 6. Représentation de -1 comme somme de puissances d-ièmes (p. 75).
1. Généralités sur $u(d; A)$. 2. Résultats relatifs au cas d'un corps K et de l'exposant $d = 2$. 3. Etude de $u(d; K)$ pour un corps de nombres algébriques K. 4. Etude de $u(d; K)$ pour un corps K quelconque de caractéristique 0. 5. Etude de $u(d; A)$ pour un anneau local hensélien A.

Chapitre 7. Problème de Waring généralisé (p. 87).
1. Généralités relatives à $v(d; A)$ et $w(d; A)$. 2. Le problème de Waring généralisé. 3. Etude de $v(d; K)$ et $w(d; K)$ pour un corps K tel que $(K^* : K^{*d}) < \infty$. 4. Etude de $v(d; A)$ et $w(d; A)$ pour une algèbre A sur un corps infini. 5. Etude de $w(d; A)$ pour un anneau local hensélien A. Applications.

Appendice. Trois identités fondamentales (p. 111).

Bibliographie (p. 113).

PREMIÈRE PARTIE

Chapitre 1

GÉNÉRALITÉS RELATIVES À A_d

1. Quelques propriétés évidentes. Nous donnons, dans ce paragraphe, une liste de propriétés très simples, mais dont nous servirons presque constamment dans la suite de ce travail, en les qualifiant d'ailleurs d'évidentes.

Proposition (1.1). *Soient* $h\colon A \to B$ *un homomorphisme d'anneaux et* d *un entier* $\geqslant 1$. *Alors*

(i) *sans autre hypothèse, on a* $h(A_d) \subset B_d$;

(ii) *si* h *est surjectif (autrement dit, si* B *est un quotient de* A*), on a* $h(A_d) = B_d$;

(iii) *en particulier, si* h *est surjectif et si de plus* $A = A_d$, *on a aussi* $B = B_d$.

Démonstration. Elle découle immédiatement des définitions de A_d et de B_d (voir l'introduction).

Proposition (1.2). *Soient* K *un corps et* d *un entier* $\geqslant 1$. *Alors* K_d *est lui-même un corps.*

Démonstration. K_d est un sous-anneau de K; reste à vérifier que si x est un élément non nul de K_d, alors $x^{-1} \in K_d$; mais ceci résulte immédiatement de l'égalité $x^{-1} = (x^{-1})^d \cdot x^{d-1}$, et du fait que K_d, sous-anneau de K, est stable pour la multiplication.

On démontre sans plus de peine les résultats suivants:

PROPOSITION (1.3). *Soient A un anneau intègre, K son corps des fractions, et d un entier $\geqslant 1$. Alors A_d, sous-anneau de A, est évidemment intègre, et admet K_d comme corps des fractions.*

PROPOSITION (1.4). *Soit A un anneau local d'idéal maximal $\mathfrak{m}$ et de corps résiduel k, et soit d un entier $\geqslant 1$. Alors A_d est lui-même un anneau local, d'idéal maximal $\mathfrak{m} \cap A_d$, et il admet k_d comme corps résiduel.*

PROPOSITION (1.5). *Soient $A^{(1)}, A^{(2)}, \ldots, A^{(u)}$ une famille finie d'anneaux, B l'anneau produit $\prod A^{(i)}$, et d un entier $\geqslant 1$. On a alors $B_d = \prod A_d^{(i)}$ (autrement dit, la formation de A_d commute aux produits directs finis; en ce qui concerne les produits directs quelconques, voir le paragraphe suivant).*

Signalons encore un résultat immédiat, mais qui sera d'une importance capitale pour la suite:

PROPOSITION (1.6). *Quels que soient A et d, l'anneau A est entier sur son sous-anneau A_d.*

Démonstration. Si $a \in A$, a est racine de $X^d - a^d$, polynôme unitaire à coefficients dans A_d.

2. Le foncteur $A \mapsto A_d$. Soit d un entier $\geqslant 1$. La correspondance $A \mapsto A_d$ peut être considérée comme un foncteur covariant de la catégorie des anneaux dans elle-même: en effet, la proposition (1.1), (i) montre que si $h: A \to B$ est un homomorphisme d'anneaux, il en résulte canoniquement, par restriction de h à A_d, un homomorphisme $h_d: A_d \to B_d$. Ce foncteur $A \mapsto A_d$ transforme évidemment tout homomorphisme injectif (resp. surjectif) en un homomorphisme injectif (resp. surjectif). Le but de ce paragraphe est d'étudier le comportement du foncteur $A \mapsto A_d$ vis-à-vis des opérations de passage à la limite inductive ou projective. Les résultats obtenus étant surtout négatifs, et de toute façon sans utilité pour la suite, le lecteur pourra sans inconvénient sauter directement au chapitre 2.

PROPOSITION (1.7). *Le foncteur $A \mapsto A_d$ commute aux limites inductives filtrantes.*

Démonstration. Compte tenu de la proposition (1.1), il suffit de montrer que si un anneau A est réunion d'une famille filtrante $(A^{(i)})$ de sous-anneaux, alors l'anneau A_d est lui-même réunion de la famille $(A_d^{(i)})$; or, ceci est évident.

REMARQUE (1.8). En revanche, le foncteur $A \mapsto A_d$ ne commute pas, en général, aux sommes directes, même finies, ni a fortiori aux limites inductives quelconques; on peut le voir sur l'exemple suivant (rappelons que dans la catégorie des anneaux, somme directe = produit tensoriel sur $\mathbf{Z}$): prenons $A = \mathbf{Z}[X]$, $B = \mathbf{Z}[Y]$, et $d = 2$; un calcul facile montre que $A_2 = \mathbf{Z}[X^2, 2X]$, que $B_2 = \mathbf{Z}[Y^2, 2Y]$, et que $A_2 \otimes B_2 = \mathbf{Z}[X^2, Y^2, 2X, 2Y]$. L'anneau $A_2 \otimes B_2$ s'identifie alors à un sous-anneau de $A \otimes B = \mathbf{Z}[X, Y]$ (à cause de l'absence de torsion, par exemple); et cependant

$$2XY = (X+Y)^2 - X^2 - Y^2 \in (A \otimes B)_2,$$

mais

$$2XY \notin A_2 \otimes B_2.$$

D'où effectivement

$$A_2 \otimes B_2 \neq (A \otimes B)_2.$$

Venons-en maintenant aux limites projectives; d'après la proposition (1.5), le foncteur $A \mapsto A_d$ commute aux produits directs finis; commute-t-il aux produits directs quelconques? Indiquons d'abord un résultat:

PROPOSITION (1.9). *Etant donné $d \geqslant 1$, les deux assertions suivantes sont équivalentes:*

(a) *le foncteur $A \mapsto A_d$ commute aux produits directs quelconques;*

(b) *quand A décrit la classe de tous les anneaux, le nombre $v(d; A)$ reste borné.*

(Noter que l'assertion (b) implique en particulier ceci: quel que soit A, $v(d; A) < \infty$.)

Démonstration. Prouvons d'abord que (b) entraîne (a). Posons $h = \sup_A v(d; A)$. Soit $(A^{(i)})$ une famille d'anneaux et posons $A = \prod A^{(i)}$; il est bien clair que

$$A_d \subset \prod A_d^{(i)}.$$

Prouvons l'inclusion inverse: soit $x = (x_i)$ un élément du second membre; par définition de h, il est possible, pour tout $i \in I$, d'écrire une relation de la forme

$$x_i = x_{i,1}^d + \ldots + x_{i,h}^d - x_{i,h+1}^d - \ldots - x_{i,2h}^d \tag{1.9.1}$$

avec des $x_{i,j} \in A$. Posons, pour tout j tel que $1 \leqslant j \leqslant 2h$, $x_j = (x_{i,j}) \in A$. La collection des égalités (1.9.1) équivaut alors à

$$x = x_1^d + \ldots + x_h^d - x_{h+1}^d - \ldots - x_{2h}^d,$$

et ceci montre bien que $x \in A_d$.

Prouvons maintenant que non (b) implique non (a). Si non (b) est vraie, il existe une famille d'anneaux $(A^{(i)})$ (indexée par les entiers $\geqslant 1$) et ayant la propriété suivante:

(1.9.2) Pour tout $i \geqslant 1$, il existe un élément $x_i \in A_d^{(i)}$ qui ne peut pas s'exprimer à l'aide de moins de i puissances d-ièmes.

Posons alors $x = (x_i) \in \prod A_d^{(i)}$: montrons que $x \notin (\prod A^{(i)})_d$ (d'où évidemment non (a), ce qu'il faut démontrer). En effet, dans le cas contraire, on pourrait écrire une relation de la forme

$$x = e_1 y_1^d + e_2 y_2^d + \ldots + e_m y_m^d \tag{1.9.3}$$

(les $e_j = \pm 1$, les $y_j \in \prod A^{(i)}$). Soit alors i un entier strictement supérieur à m: par projection des deux membres de (1.9.3) sur $A^{(i)}$, on obtiendrait une égalité de la forme

$$x_i = e_1 y_{1,i}^d + e_2 y_{2,i}^d + \ldots + e_m y_{m,i}^d,$$

(les $y_{i,j} \in A_i$); mais alors x_i pourrait s'exprimer à l'aide de $m < i$ puissances d-ièmes, ce qui contredirait (1.9.2).

La proposition (1.9) étant établie, la question relative aux produits directs équivaut à celle-ci: *quand A décrit la classe de tous les anneaux, $v(d; A)$ reste-t-il borné?* La réponse est positive quand $d = 2$: nous verrons en effet au chapitre 7 que quel que soit A, $v(d; A) \leqslant 3$; ainsi, le foncteur $A \mapsto A_2$ commute aux produits directs quelconques. En revanche, pour $d > 2$, nous ignorons la réponse: pour plus amples renseignements concernant $v(d; A)$, se reporter au chapitre 7.

Quant à la question plus générale de savoir si le foncteur $A \mapsto A_d$ commute aux limites projectives quelconques, elle demeure a fortiori en suspens.

Chapitre 2

DÉTERMINATION DE A_d DANS CERTAINS CAS IMPORTANTS

1. Détermination de k_d lorsque k est un corps fini. Pour des raisons de commodité, nous adopterons une notation qui nous resservira par la suite:

DÉFINITION (2.1). Soient d un entier $\geqslant 1$, p un nombre premier, et $q = p^f$ ($f \geqslant 1$) un nombre p-primaire. Nous désignerons par le symbole $[q; d]$ le plus petit nombre p-primaire p^g ayant les deux propriétés suivantes:

(i) l'exposant g divise l'exposant f;

(ii) le quotient $(p^f-1)/(p^g-1)$ divise l'entier d.

(Rappelons en effet que les assertions g divise f et p^g-1 divise p^f-1 sont équivalentes.)

Nous aurons besoin d'autre part de ce résultat bien connu:

LEMME (2.2). *Soient k un corps fini à q éléments, et d un exposant $\geqslant 1$. Alors, l'indice $(k^*: k^{*d})$ est égal à $(q-1, d)$, et l'ordre de k^{*d} est donc égal à*

$$(q-1)/(q-1, d).$$

Dans ces conditions:

THÉORÈME (2.3). *Soient k un corps fini à q éléments, et d un entier $\geqslant 1$. Alors, k_d est égal au sous-corps de k contenant exactement $[q; d]$ éléments, ce qu'on peut écrire*

$$k_d = \boldsymbol{F}_{[q;d]}.$$

Démonstration. k^* est un groupe cyclique d'ordre $q-1$, et ses sous-groupes correspondent bijectivement aux diviseurs de $q-1$. Par ailleurs, si $q = p^f$, les sous-corps de k correspondent bijectivement aux diviseurs de f. Les assertions g divise f et p^g-1 divise p^f-1 étant équivalentes, on voit donc que, pour qu'un sous-groupe G de k^* soit de la forme k'^* (k' étant un sous-corps de k), il faut et il suffit que l'ordre de G soit de la forme p^g-1, g étant un diviseur de f. Comme k^{*d} est d'ordre $(p^f-1)/(p^f-1, d)$ (lemme (2.2)) et que k_d est le plus petit sous-corps de k contenant k^{*d}, on a évidemment $k_d = \boldsymbol{F}_{p^s}$, s étant le plus petit diviseur g de f tel que

$$(p^f-1)/(p^f-1, d) \text{ divise } p^g-1,$$

ou encore, tel que

$$(p^f-1)/(p^g-1) \text{ divise } (p^f-1, d),$$

ce qui équivaut à

$$(p^f-1)/(p^g-1) \text{ divise } d.$$

D'où le théorème.

REMARQUE (2.4). La condition $[p^f; d] \neq p^f$ est assez rarement vérifiée; elle ne l'est en effet que s'il existe deux entiers g et h ($h \neq 1$) tels que $gh = f$ et que l'entier

$$p^{(h-1)g} + p^{(h-2)g} + \ldots + p^g + 1$$

divise d. Or, ceci implique évidemment les deux inégalités

$$p < d, \tag{2.4.1}$$

$$p^f < d^2, \tag{2.4.2}$$

ce qui, pour d donné, n'est possible que dans un nombre fini de cas. Cette remarque conduit d'ailleurs au résultat suivant (démontré différemment par Tornheim (voir [26], p. 361), qui ne donne pas la détermination de k_d):

PROPOSITION (2.5). *Pour d donné, il n'existe qu'un nombre fini de corps finis k tels que $k_d \neq k$.*

Voici la situation la plus simple où l'on ait $k_d \neq k$:

Exemple (2.6). Prenons $k = \boldsymbol{F}_4$ et $d = 3$. On a alors $[4;3] = 2$, donc $k_3 = \boldsymbol{F}_2 \neq k$. Et en effet, dans k, tout élément x non nul vérifie la relation

$$x^{4-1} = x^3 = 1;$$

d'où $k^{*3} = \{1\}$ et $k_3 = \{0, 1\} = \boldsymbol{F}_2$.

2. Détermination de A_d lorsque A est une algèbre sur un corps infini K.

Lemme (2.7). *Soient K un corps (fini ou non) de caractéristique $p > 0$, A une K-algèbre (commutative et unitaire, bien entendu) et e un exposant ≥ 1 et non divisible par p. Désignons par φ la fonction indicatrice d'Euler, et posons*

$$t = \varphi(e), \qquad m = p^t - 1.$$

Alors, si le groupe multiplicatif K^{*m} est d'ordre $\geq m-1$, on a l'égalité

$$A_e = A.$$

Démonstration. e n'étant pas divisible par p, m est multiple de e. Ceci implique l'inclusion $A_m \subset A_e$, et il suffit par conséquent de prouver l'égalité $A_m = A$. Soit alors x un élément quelconque de A. Choisissons des éléments $u_1, u_2, \ldots, u_{m-1}$ de K^* tels que $u_1^m, u_2^m, \ldots, u_{m-1}^m$ soient des éléments distincts de K^{*m}: c'est possible, par hypothèse sur l'ordre de K^{*m}; dans l'identité du théorème (8.4) (appendice), faisons alors $X = x$, $U_j = u_j$ $(j = 1, 2, \ldots, m-1)$; l'égalité obtenue prouve que $x \in A_m$, et le lemme est démontré.

Théorème (2.8). *Soient K un corps infini d'exposant caractéristique (quelconque) p, A une K-algèbre, et d un exposant (divisible ou non par p). Ecrivons $d = p^r \cdot e$ avec $(p, e) = 1$. Dans ces conditions, on a l'égalité*

$$A_d = A^{p^r}.$$

Démonstration. Si $p = 1$, l'égalité à prouver se réduit à $A_d = A$, ce qui résulte immédiatemment de (8.3) (appendice), puisque $d!$ est inversible dans K et donc aussi dans A. Si $p > 1$, on a évidemment $A_d = (A_e)^{p^r}$; il suffit alors de prouver que $A_e = A$, ce qui résulte du lemme (2.7), puisque K est maintenant supposé infini.

Corollaire (2.9). *Si K est un corps infini d'exposant caractéristique p, et si $d = p^r \cdot e$ avec $(p, e) = 1$, on a l'égalité*

$$K_d = K^{p^r}.$$

En particulier, si K est parfait infini, on a, quel que soit l'exposant d,

$$K_d = K.$$

Remarque (2.10). Il est clair que (2.8) et (2.9) restent vrais lorsque K est un corps fini, mais "suffisamment grand".

Le théorème (2.8) permet l'étude de la conservation de certaines propriétés d'un anneau intègre A par passage à A_d.

Proposition (2.11). *Soient A un anneau intègre infini, K son corps des fractions, p l'exposant caractéristique de K, et d un entier ≥ 1. Posons $d = p^r \cdot e$ avec $(p, e) = 1$. Si l'anneau A est intégralement clos, les deux assertions suivantes sont équivalentes:*

(a) *A_d est lui-même intégralement clos;*

(b) *A_d est égal à A^{p^r}.*

Démonstration. L'application $x \mapsto x^{p^r}$ est un isomorphisme du triplet (A_e, A, K) sur le triplet (A_d, A^{p^r}, K^{p^r}). D'après le corollaire (2.9), on a $K^{p^r} = K_d$; mais K_d est le corps des fractions de A_d et A est entier sur A_e. L'isomorphisme en question montre donc que A^{p^r} est entier sur A_d et qu'il est intégralement clos (dans $K^{p^r} = K_d$): le reste de la démonstration est alors évident.

Corollaire (2.12). *Mêmes données et notations. Si A est un anneau de valuation (resp. de valuation discrète, de Dedekind, factoriel, principal), les deux assertions suivantes sont équivalentes:*

(a) *A_d est lui-même de valuation (resp. de valuation discrète, de Dedekind, factoriel, principal);*

(b) *A_d est égal à A^{p^r}.*

Démonstration. Il suffit de remarquer que chacune des assertions A de valuation, de valuation discrète, etc. ..., implique l'assertion A intégralement clos.

3. Etude de la condition $A_d = A$ pour un anneau local A.

Théorème (2.13). *Soient A un anneau local, $\mathfrak{m}$ son idéal maximal, k son corps résiduel, p la caractéristique de k, et soit d'autre part d un entier ≥ 1.*

(i) *Si A est séparé et si p divise d, les deux assertions suivantes sont équivalentes:*

(a) *$A_d = A$;*

(b) *$k_d = k$, et $\mathfrak{m} = pA$.*

(ii) *Si A est hensélien et si p ne divise pas d, les deux assertions suivantes sont équivalentes:*

(a) *$A_d = A$;*

(b) *$k_d = k$.*

Démonstration. Prouvons la première partie du théorème, et montrons d'abord que (a) implique (b). L'égalité de A_d et A implique évidemment celle de k_d et k; reste à prouver l'égalité $\mathfrak{m} = pA$: or, consi-

dérons l'anneau local $B = A/pA$; il est séparé, il a pour corps résiduel k et, d'après la proposition (1.1), il satisfait à l'égalité $B_d = B$; a fortiori puisque p divise d, on a $B_p = B$, et même, puisque B est de caractéristique p, $B^p = B$ (B^p désigne l'ensemble des x^p pour $x \in B$; notons qu'on a nécessairement $p > 0$, puisque p divise d; p est donc l'exposant caractéristique de k). Désignons alors par $\mathfrak{n}$ l'idéal maximal $\mathfrak{m}/pA$ de B: si $\mathfrak{n}^p$ est la puissance p-ième (au sens habituel) de l'idéal $\mathfrak{n}$, la relation $B^p = B$ montre immédiatement que $\mathfrak{n}^p = \mathfrak{n}$; par itération, on déduit de là que, pour tout entier positif h, on a également $\mathfrak{n}^{p^h} = \mathfrak{n}$; d'où l'égalité

$$\bigcap_{h>0} \mathfrak{n}^{p^h} = \mathfrak{n}.$$

Mais comme B est séparé, ceci implique $\mathfrak{n} = 0$, donc $\mathfrak{m} = pA$, C.Q.F.D.

Montrons maintenant que (b) implique (a). On peut écrire $d! = p^n \cdot e$ avec $(p, e) = 1$; comme l'entier e est inversible dans l'anneau A, ceci implique l'égalité

$$(*) \qquad d!\,A = p^n A.$$

Soit alors x un élément quelconque de A; $\bar{x}$ désignant son image dans le corps résiduel k, on a par hypothèse $\bar{x} \in k_d$; donc il existe $y_1 \in A_d$ tel que $x - y_1 \in pA = \mathfrak{m}$; ou encore, il existe $y_1 \in A_d$ et $x_1 \in A$ tels que $x = y_1 + px_1$. Maintenant, on peut recommencer pour x_1 ce qu'on a fait pour x, et itérer $n-1$ fois ce raisonnement. On arrive en définitive à une décomposition

$$x = y_1 + py_2 + p^2 y_3 + \ldots + p^{n-1} y_n + p^n x_n,$$

avec $y_1, y_2, \ldots, y_n \in A_d$ et $x_n \in A$. Mais chacun des p^h ($= 1^d + 1^d + \ldots + 1^d$ (p^h fois)) appartient à A_d. De plus, d'après (*) et (8.3) (appendice), on a également $p^n x_n \in A_d$. D'où finalement $x \in A_d$, et $A_d = A$. (On notera que l'hypothèse de séparation n'est pas intervenue dans cette partie de la démonstration.)

Venons-en à la deuxième partie du théorème: le fait que (a) implique (b) est évident, k étant un quotient de A; et le fait que (b) implique (a) résulte du second des deux lemmes suivants:

LEMME (2.14). *Soit A un anneau local hensélien d'idéal maximal $\mathfrak{m}$ et de corps résiduel k. Soient p la caractéristique de k, et d un entier non divisible par p. Alors, toute égalité*

$$\bar{x} = e_1 \xi_1^d + e_2 \xi_2^d + \ldots + e_m \xi_m^d,$$

où x est un élément inversible de A, où m est un entier $\geqslant 1$ quelconque, où les e_i sont des coefficients égaux à ± 1, et où les ξ_i sont des éléments quelconques de k, peut se relever dans A en une égalité

$$x = e_1 x_1^d + e_2 x_2^d + \ldots + e_m x_m^d,$$

avec $\bar{x}_1 = \xi_1, \bar{x}_2 = \xi_2, \ldots, \bar{x}_m = \xi_m$.

Démonstration. Puisque x est inversible dans A, $\bar{x}$ n'est pas nul, et on peut toujours supposer que ξ_1, par exemple, est lui-même différent de zéro. Soient alors $x_2, x_3, \ldots, x_m$ des éléments de A tels que $\bar{x}_2 = \xi_2$, $\bar{x}_3 = \xi_3, \ldots, \bar{x}_m = \xi_m$, et considérons dans $A[X]$ le polynôme

$$F(X) = e_1 X^d + e_2 x_2^d + e_3 x_3^d + \ldots + e_m x_m^d - x.$$

Réduit modulo $\mathfrak{m}$, ce polynôme admet ξ_1 pour racine, et cette racine est simple: car $\bar{F}'(\xi_1) = de_1 \xi_1^{d-1}$, et $\xi_1 \neq 0$, $p \nmid d$. A étant hensélien, il existe donc x_1 tel que $\bar{x}_1 = \xi_1$ et que $F(x_1) = 0$, ce qu'il fallait justement démontrer.

LEMME (2.15). *Mêmes hypothèses qu'au lemme précédent; désignons par π l'homomorphisme canonique $A \to k$. On a alors l'égalité*

$$A_d = \pi^{-1}(k_d).$$

Démonstration. Soit x un élément de A tel que $\pi(x) \in k_d$. Si x est inversible, le lemme (2.14) montre immédiatement que $x \in A_d$. Sinon, $1-x$ est inversible dans A, et $\pi(1-x) = 1 - \pi(x) \in k_d$; donc $1-x \in A_d$, et ici encore $x = 1-(1-x) \in A_d$.

REMARQUE (2.16). Conservons les hypothèses et notations du lemme (2.15); le type de démonstration employé montre également que

$$u(d; A) = u(d; k);$$

$$v(d; k) \leqslant v(d; A) \leqslant v(d; k) + 1;$$

$$w(d; k) \leqslant w(d; A) \leqslant w(d; k) + 1.$$

REMARQUE (2.17). Il est facile de voir que le théorème (2.13) reste vrai si on y remplace les assertions $A_d = A$ et $k_d = k$ par les assertions *A est de type fini sur A_d* et *k est de dimension finie sur k_d*.

REMARQUE (2.18). Si un anneau local séparé A de caractéristique résiduelle $p > 0$ satisfait à la condition $\mathfrak{m} = pA$ qui intervient dans la première partie du théorème (2.13), A possède les propriétés suivantes:

c'est un anneau noethérien, de dimension de Krull $\leqslant 1$; tout idéal non nul de A est de la forme $p^n A$, pour n convenable; si A est sans torsion, A est un anneau de valuation discrète absolument non-ramifié; sinon, A est un anneau artinien (un corps si $pA = 0$).

Venons-en au résultat le plus important de ce paragraphe:

THÉORÈME (2.19). *Soient A un anneau de valuation discrète, K son corps des fractions, $\mathfrak{m}$ son idéal maximal, k son corps résiduel, et p la carac-*

téristique de k. Supposons K de caractéristique 0. Alors, quel que soit l'exposant $d \geqslant 1$, les deux assertions suivantes sont équivalentes:

(a) $A_d = A$;

(b) $k_d = k$, *et de plus, si p divise d, A est absolument non-ramifié* (*c'est-à-dire* $\mathfrak{m} = pA$).

Démonstration. Si $p = 0$, ou bien si $p > 0$, mais si $d < p$, $d!$ est inversible à la fois dans A et dans k; compte tenu de (8.3), on a donc alors $A_d = A$ et $k_d = k$; comme de plus il est impossible dans ce cas que p divise d, il n'y a en fait rien à démontrer.

Supposons donc maintenant $p > 0$ et $d \geqslant p$. Alors $d!$ est divisible par p, donc $d!\,A \subset \mathfrak{m}$, et comme par ailleurs $d!\,A \subset A_d$ (toujours d'après (8.3)), il suffit visiblement de démontrer l'équivalence de (a) et (b) pour l'anneau quotient $A' = A/d!\,A$, qui est local, d'idéal maximal $\mathfrak{m}' = \mathfrak{m}/d!\,A$, et de corps résiduel k. Mais A' est séparé et hensélien (par exemple, parce que l'idéal $\mathfrak{m}'$ est nilpotent); de plus, les conditions $\mathfrak{m} = pA$ et $\mathfrak{m}' = pA'$ sont équivalentes; l'équivalence de (a) et (b) résulte alors de (2.13) (i), si p divise d, et de (2.13) (ii), si p ne divise pas d.

Le théorème (2.19) nous permettra de donner, par globalisation, une condition nécessaire et suffisante pour qu'un anneau d'entiers algébriques A satisfasse à l'égalité $A_d = A$ (chapitre 4, théorème (4.11.)).

Chapitre 3

STABILITÉ DE LA FINITUDE DE A/A_d

1. Passage à une extension de type fini. Si A est un anneau, et d un entier $\geqslant 1$, nous avons déjà noté que A est entier sur A_d: les conditions *A est une A_d-algèbre de type fini* et *A est un A_d-module de type fini* sont donc équivalentes, et l'assertion *A est de type fini sur A_d* ne présente donc aucune ambiguïté. Notons d'autre part que s'il existe une forme diagonale

$$a_1 X_1^d + a_2 X_2^d + \ldots + a_m X_m^d \qquad (a_1, a_2, \ldots, a_m \in A)$$

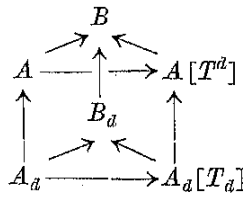
universelle pour A, c'est-à-dire représentant tout élément de A, alors A est de type fini sur A_d: car $(a_1, a_2, \ldots, a_m)$ est évidemment un système générateur de A sur A_d; inversement, il est facile de voir que si A est de type fini sur A_d et si de plus $v(d; A) < \infty$, il existe une forme diagonale de degré d universelle pour A.

Proposition (3.1). *Soient A un anneau et d un entier $\geqslant 1$. Soit d'autre part B une algèbre de type fini sur A. Alors*

(i) *Si A est de type fini sur A_d, B est de type fini sur B_d.*

(ii) *Si de plus l'anneau A_d est noethérien, B_d est une algèbre de type fini sur A_d, donc un anneau noethérien.*

Démonstration. La proposition est évidente si B est un quotient de A; on peut donc se ramener au cas où B est une algèbre de polynômes sur A, et même, par récurrence, au cas où $B = A[T]$. On a alors le diagramme ci-contre, où les flèches représentent des inclusions. $B = A[T]$ est un module de type fini sur $A[T^d]$, il est engendré par $1, T, \ldots, T^{d-1}$;



de même $A[T^d]$ est un module de type fini sur $A_d[T^d]$, il est engendré par n'importe quel système générateur fini de A sur A_d. Mais dans ces conditions, B est un module de type fini sur $A_d[T^d]$ et a fortiori sur B_d, ce qui prouve (i).

Passons à (ii): A_d est noethérien par hypothèse, donc $A_d[T^d]$ est noethérien, et B, de type fini sur $A_d[T^d]$, est un $A_d[T^d]$-module noethérien. Son sous-module B_d est donc de type fini sur $A_d[T^d]$, comme module et a fortiori comme algèbre: mais ceci implique évidemment que B_d est une A_d-algèbre de type fini, et en particulier, A_d étant noethérien, que B_d est lui-même noethérien.

Remarque (3.2). On se servira le plus souvent de (3.1) dans le cas où A est noethérien et où $A_d = A$.

Exemples.

1) $A = \mathbf{Z}$;

2) $A =$ un corps premier;

3) $A =$ un corps algébriquement clos;

4) plus généralement, $A =$ un corps parfait infini;

5) $A = \mathbf{Z}_p$.

Tous ces anneaux sont noethériens; la condition $A_d = A$ est satisfaite en 1) et 2) parce que A ne contient aucun sous-anneau distinct de lui-même; en 3), parce que tout élément de A est une puissance d-ième. L'égalité $A_d = A$ pour 4) et 5) a été prouvée au chapitre 2 ((2.9) et (2.13)).

Cela étant, la proposition (3.1) donne par exemple les résultats suivants (d est un entier quelconque $\geqslant 1$):

Corollaire (3.3). *Si A est un ordre d'entiers algébriques, A_d est noethérien, et A est de type fini sur A_d.*

(Naturellement, il est plus facile de le voir directement; en fait, A_d est lui-même un ordre d'entiers algébriques, qui a même corps des fractions que A.)

COROLLAIRE (3.4). *Soient k un corps parfait et A une algèbre de type fini sur k. Alors l'anneau A_d est noethérien, A est de type fini sur A_d, et A_d est une k_d-algèbre de type fini.*

(La conclusion $A_d = A$ est en fait valable même si k n'est pas parfait: car K est alors infini, et dans ce cas, $A_d \cong A$ (en tant qu'anneau) quoique, en général, $A_d \neq A$ (voir théorème (2.8).)

COROLLAIRE (3.5). *Si A est un anneau $\mathfrak{P}$-adique, A_d est un anneau noethérien, et un A_d-module de type fini.*

(On en dira davantage sur A_d, dans le cas $\mathfrak{P}$-adique, au paragraphe suivant.)

Insérons ici un résultat très particulier:

PROPOSITION (3.6). *Soient p un nombre premier, $k = \boldsymbol{F}_p$ le corps premier à p éléments, A l'anneau de polynômes $k[X]$, et d un entier non divisible par p. Alors, A_d est un sous-espace vectoriel de A (sur k) de codimension finie:*

$$\dim_k(A/A_d) \leqslant (d-1)^2.$$

Démonstration. Le fait que A_d soit un espace vectoriel sur k tient à ce que $k = k_d \subset A_d$. Donnons un lemme:

LEMME (3.7). *Avec les hypothèses ci-dessus, tout polynôme appartenant à A est congru (modulo A_d) à un polynôme de degré $< d(d-1)$.*

Prouvons le lemme; quels que soient les entiers m et n satisfaisant à $n \geqslant 0$, $1 \leqslant m \leqslant d-1$, on peut écrire, par la formule du binôme,

$$(1+X^m)^d X^{nd} = X^{nd} + dX^{m+nd} + \ldots + dX^{m(d-1)+nd} + X^{md+nd};$$

mais $(1+X^m)^d X^{nd} - X^{md+nd} \in A_d$; comme d, non divisible par p, est inversible dans $k_d = k$, et que $m(d-1)+nd = (m+n)d-m$, on déduit de là un premier résultat:

(*) Il existe un polynôme $P_{(m+n)d-m-1}(X)$, de degré $\leqslant (m+n)d-m-1$, et tel que

$$X^{(m+n)d-m} \equiv P_{(m+n)d-m-1}(X) \pmod{A_d}.$$

Pour démontrer le lemme, il suffit alors de prouver que, quel que soit $q \geqslant d(d-1)$, il existe un polynôme $G_{q-1}(X)$ de degré $\leqslant q-1$ et tel que

$$X^q \equiv G_{q-1}(X) \pmod{A_d}.$$

Si q est multiple de d, il suffit de faire $G_{q-1} = 0$. Sinon, écrivons $q = bd+r$ $(1 \leqslant r \leqslant d-1)$, et posons

$$m = d-r, \qquad n = b+r+1-d.$$

On a bien $1 \leqslant m \leqslant d-1$, et $n \geqslant 0$ (à cause de l'hypothèse $q \geqslant d(d-1)$), et on constate immédiatement que

$$(m+n)d-m = bd+r = q.$$

Compte tenu de (*), il suffit alors de faire

$$G_{q-1} = P_{q-1}.$$

Le lemme est démontré; il prouve que l'espace-quotient A/A_d est engendré par les images de $1, X, X^2, \ldots, X^{d(d-1)-1}$. Mais $X^d, X^{2d}, \ldots, X^{(d-2)d}$ sont dans A_d et ont donc une image nulle dans A/A_d. Finalement, A/A_d est engendré par les images des $(d-1)^2$ monômes $X, X^2, \ldots, X^{d-1}, X^{d+1}, \ldots$ $\ldots, X^{2d-1}, X^{2d+1}, \ldots, X^{d(d-1)-1}$, C.Q.F.D.

EXEMPLE (3.8). Supposons $p = 2$ et $d = 3$. Nous nous intéressons aux sommes de cubes dans $\boldsymbol{F}_2[X] = A$. La méthode exposée ci-dessus donne le résultat suivant:

pour que le polynôme $P(X) = \sum_{i \geqslant 0} a_i X^i$ appartienne à A_3, il faut et il suffit que

$$\sum_{3 \nmid i} a_i = a_1 + a_2 + a_4 + a_5 + \ldots = 0.$$

Notons que $P \mapsto \sum_{3 \nmid i} a_i$ est une forme k-linéaire non nulle sur A. L'énoncé ci-dessus équivaut à dire que A_3 est le noyau de cette forme linéaire. Dans ce cas particulier, on a donc $\dim_k(A/A_3) = 1 \leqslant (3-1)^2 = 4$.

REMARQUE (3.9). Si, dans (3.7), on supprime l'hypothèse *p ne divise pas d*, et si on suppose seulement *k fini*, on voit facilement qu'on obtient l'énoncé suivant:

posons $d = p^r \cdot q$, avec $(p, q) = 1$; alors A_d est un sous-k_d-espace vectoriel de codimension finie dans $k_d[X^{p^r}]$.

Si au contraire on suppose *k infini*, le théorème (2.8) montre que $k_d = k^{p^r}$ et $A_d = k^{p^r}[X^{p^r}]$.

2. Passage à un localisé ou à un complété.

PROPOSITION (3.10). *Soient A un anneau, d un entier $\geqslant 1$ et S une partie multiplicative de A. Si A est de type fini sur A_d, $S^{-1}A$ est de type fini sur $(S^{-1}A)_d$.*

Démonstration. Si $(a_i)_{1 \leqslant i \leqslant n}$ est un système générateur de A sur A_d, $(a_i/1)_{1 \leqslant i \leqslant n}$ est un système générateur de $S^{-1}A$ sur $(S^{-1}A)_d$.

Ce résultat s'applique en particulier à un localisé.

En ce qui concerne le passage à un complété, nous nous limiterons au cas local. Nous prendrons les notations suivantes:

A, anneau local; d, entier $\geqslant 1$;

$\mathfrak{m}$, idéal maximal de A;

$\mathfrak{n}$, idéal maximal de A_d (donc $\mathfrak{n} = \mathfrak{m} \cap A_d$);

k et k_d, corps résiduels de A et A_d.

Par *topologie de* A (resp. A_d), nous entendrons la topologie naturelle d'anneau local, donc la topologie $\mathfrak{m}$-adique (resp. $\mathfrak{n}$-adique).

PROPOSITION (3.11). (i) *La topologie de A_d est plus fine que la topologie induite sur A_d par celle de A;*

(ii) *Si ces deux topologies sont égales, on peut (en identifiant $\hat{A}_d$ à l'adhérence de A_d dans $\hat{A}$) écrire l'inclusion*

$$(\hat{A})_d \subset \hat{A}_d;$$

(iii) *Si de plus k est un corps fini, si A est séparé, si $\mathfrak{m}$ est de type fini et si $v(d; A) < \infty$, on a plus précisément*

$$(\hat{A})_d = \hat{A}_d.$$

Démonstration. (i) résulte de l'inclusion évidente

$$\mathfrak{n}^h \subset \mathfrak{m}^h \cap A_d.$$

Prouvons (ii): si $a \in (\hat{A})_d$, il existe $e_1, e_2, \ldots, e_m$, égaux à ± 1, et $a_1, a_2, \ldots, a_m \in \hat{A}$, tels que

$$a = e_1 a_1^d + e_2 a_2^d + \ldots + e_m a_m^d.$$

A étant dense dans $\hat{A}$, on peut, pour tout j de 1 à m, écrire

$$a_j = \lim_{\nu \to \infty} a_{j,\nu} \qquad (\text{les } a_{j,\nu} \in A).$$

Alors

$$a = \lim_{\nu \to \infty} (e_1 a_{1,\nu}^d + \ldots + e_m a_{m,\nu}^d);$$

a est limite d'une suite d'éléments de A_d, et appartient donc bien à l'adhérence $\hat{A}_d$ de A_d.

Démontrons (iii). Je dis d'abord que A est *précompact*. En effet, A est séparé par hypothèse; de plus, quel que soit $h \geqslant 0$, $\mathfrak{m}^h$ est un idéal de type fini, donc $\mathfrak{m}^h/\mathfrak{m}^{h+1}$ est un espace vectoriel de dimension finie sur $A/\mathfrak{m} = k$, corps fini; l'indice $(\mathfrak{m}^h : \mathfrak{m}^{h+1})$ est donc fini; et par conséquent, quel que soit $n \geqslant 1$, $A/\mathfrak{m}^n$ est fini, d'ordre égal à

$$\prod_{h=0}^{n-1} (\mathfrak{m}^h : \mathfrak{m}^{h+1}).$$

Ceci implique que, si grand que soit n, A est recouvert par un nombre

fini de translatés de $\mathfrak{m}^n$, donc que A est précompact. Soit alors $a \in A_d$; si l'on pose $q = v(d; A)$, on a, par définition, une relation du type

$$a = \lim_{\nu \to \infty} (e_{1,\nu} a_{1,\nu}^d + \ldots + e_{q,\nu} a_{q,\nu}^d),$$

les $e_{j,\nu} = \pm 1$, les $a_{j,\nu} \in A$. Mais le groupe discret $D = \{-1, 1\}$ est compact, ainsi que $\hat{A}$, puisque A est précompact. L'espace produit $D^q \times (A)^q$ est donc compact, et on peut extraire de la suite

$$\big((e_{1,\nu}, e_{2,\nu}, \ldots, e_{q,\nu}), (a_{1,\nu}, a_{2,\nu}, \ldots, a_{q,\nu})\big)_{\nu \geqslant 0}$$

une sous-suite convergeant vers une limite

$$\big((e_1, e_2, \ldots, e_q), (a_1, a_2, \ldots, a_q)\big)$$

(les $e_j = \pm 1$, les $a_j \in A$). Mais alors, par passage à la limite,

$$a = e_1 a_1^d + e_2 a_2^d + \ldots + e_q a_q^d,$$

c'est-à-dire $a \in (\hat{A})_d$, C.Q.F.D.

Notons que, avec les hypothèses de (iii), on a

$$v(d; \hat{A}) \leqslant v(d; A).$$

PROPOSITION (3.12). *Si l'anneau A_d est noethérien, et si A est de type fini sur A_d, la topologie de A_d (la $\mathfrak{n}$-adique) est égale à la topologie induite par la topologie de A (la $\mathfrak{m}$-adique).*

Démonstration. Prenons pour anneau de base A_d (noethérien) et considérons A, module de type fini sur A_d, et A_d, sous-module de A. D'après le lemme d'Artin–Rees, il existe h tel que, pour tout $q \geqslant h$, on ait

$$(\mathfrak{n}^q A) \cap A_d \subset \mathfrak{n}^{q-h}\big((\mathfrak{n}^h A) \cap A_d\big)$$

(voir par exemple [28], Vol. 2, p. 255, th. 4'), et en particulier

$$(\mathfrak{n}A)^q \cap A_d \subset \mathfrak{n}^{q-h}.$$

Comme $\mathfrak{n}A$ est $\mathfrak{m}$-primaire et est donc un idéal de définition de la topologie $\mathfrak{m}$-adique, ceci prouve que la topologie $\mathfrak{n}$-adique est moins fine que celle induite sur A_d par la topologie $\mathfrak{m}$-adique, d'où la proposition.

Remarquons que les hypothèses A_d noethérien et A de type fini sur A_d impliquent A noethérien, ce qui implique A séparé et $\mathfrak{m}$ de type fini (soit deux sur quatre des hypothèses faites dans (iii)). Les propositions (3.11) et (3.12) admettent donc le corollaire suivant:

COROLLAIRE (3.13). *Gardons toujours les mêmes notations. Supposons*

A_d noethérien;

A de type fini sur A_d;

k fini, et $v(d; A) < \infty$.

Alors

(i) *On a l'identification* $(\hat{A})_d = \hat{A}_d$, *et de plus* $v(d;\hat{A}) = v(d;A)$.

(ii) *En particulier, si* A *est supposé complet,* A_d *est lui-même complet (pour sa structure uniforme naturelle d'anneau local).*

Voici une autre proposition qui, dans une certaine mesure, apporte un complément à la précédente:

Théorème (3.14). Mêmes notations: *Supposons* A *de valuation discrète, d'inégales caractéristiques* 0 *et* $p>0$, *et supposons* k *parfait. Alors*

(i) A_d *est un anneau local séparé de dimension de Krull égale à* 1.

(ii) A_d *est un sous-anneau à la fois ouvert et fermé de* A.

(iii) *Si* A *est complet,* A_d *est noethérien, et* A *est de type fini sur* A_d *(donc, d'après* (3.12), *la topologie de* A_d *est induite par la topologie de* A).

(iv) *Si de plus* k *est fini (autrement dit, si* A *est un anneau* $\mathfrak{P}$*-adique), on a*

$$v(d;A)<\infty,$$

(donc, d'après (2.13), A_d *est un anneau local noethérien complet de dimension* 1).

Démonstration. (i) Il suffit de noter que A est entier sur A_d et que A est lui-même local séparé de dimension 1.

(ii) Soit e l'indice de ramification absolu de A, et soit p^n la plus haute puissance de p divisant $d!$. La relation $d!\,A\subset A_d$ s'écrit ici

$$p^n\cdot A=\mathfrak{m}^{en}\subset A_d;$$

elle prouve que 0 est un point intérieur de A_d: le groupe additif A_d (et par conséquent l'anneau A_d) est donc à la fois ouvert et fermé dans A.

(iii) Posons

$$k_0=\begin{cases} k & \text{si } k \text{ est infini;}\\ \text{le corps premier } \boldsymbol{F}_p \text{ sinon.}\end{cases}$$

Désignons par W_0 (resp. W) l'anneau des vecteurs de Witt sur k_0 (resp. k) (voir par exemple [24], p. 49). A étant maintenant supposé complet, W_0 et W s'identifient à des sous-anneaux de A, et on peut écrire $W_0\subset W\subset A$. Or, W est de type fini sur W_0 (et même libre, de rang $[k:k_0]$); A est lui-même de type fini sur W (et même libre, de rang e). Ainsi, A est un W_0-module de type fini. D'autre part, on a $(k_0)_d=k$: c'est évident si k_0 est le corps premier; sinon, $k_0=k$, parfait infini, et cela résulte alors de (2.9). De plus, W_0 est absolument non-ramifié; le théorème (2.19) nous permet alors d'écrire $(W_0)_d=W_0$. Enfin, W_0 est évidemment noethérien; nous pouvons donc appliquer la proposition (3.1) à A, W_0-algèbre de type fini, et l'assertion (iii) se trouve démontrée.

(iv) L'identité (8.2) (appendice)montre que tout élément de l'idéal $d!\,A=\mathfrak{m}^{en}$ (voir la démonstration de (ii)) s'exprime à l'aide de

$$2\sum_{h=0}^{d-1}\binom{d-1}{h}=2^d$$

puissances d-ièmes. On en déduit facilement que

$$v(d;A)\leqslant 2^d+v(d;A/\mathfrak{m}^{en}).$$

Mais $A/\mathfrak{m}^{en}$ est un anneau fini, d'où évidemment $v(d;A/\mathfrak{m}^{en})<\infty$; donc aussi $v(d;A)<\infty$, C.Q.F.D.

Le théorème (3.14) nous renseigne assez bien sur la structure de A_d lorsque A est un anneau $\mathfrak{P}$-adique: notons que si $A_d\neq A$ (ce qui peut se produire: voir (2.19)), A_d n'est pas un anneau $\mathfrak{P}$-adique, faute d'être intégralement clos.

Chapitre 4

LOCALISATION ET GLOBALISATION

1. Généralités; passage à un anneau de fractions. Notons d'abord un résultat déjà vu, mais qui nous sera particulièrement utile dans ce chapitre et le suivant:

Théorème (4.1). *Soient* A *un anneau, et* d *un entier* $\geqslant 1$; *l'anneau* A *est entier sur son sous-anneau* A_d.

Démonstration. Si $a\in A$, a est racine de X^d-a^d, polynôme unitaire à coefficients dans l'anneau A_d.

Corollaire (4.2). *Si* A *est un anneau local (resp. semi-local), l'anneau* A_d *est lui-même un anneau local (resp. semi-local); en particulier, si* A *est un corps,* A_d *est également un corps.*

Démonstration. Voir par exemple [5], chapitre 5, § 2, n° 1, proposition 1 et lemme 2.

On retrouve ainsi, sans calculs, certains résultats du chapitre 1 (où de toute façon les calculs étaient restés implicites).

Venons-en à l'étude du passage aux anneaux de fractions; dans tout ce paragraphe, nous utiliserons les notations suivantes:

Notations (4.3). A désigne un anneau, d un entier $\geqslant 1$, et S une partie multiplicative de A; on pose

$$T=S\cap A_d;$$

$$S^d=\{s^d \mid s\in S\}.$$

Il est clair alors qu'on a la double inclusion $S^d \subset T \subset S$, et que S^d et T sont des parties multiplicatives, à la fois de A_d et de A. En outre, si $t \in T$, on peut écrire

$$t^{d-1} \cdot t = t^d \in T^d \subset S^d,$$

d'où un isomorphisme canonique

$$(S^d)^{-1} A_d \simeq T^{-1} A_d,$$

(voir [5], chapitre 2, § 2, n°3, proposition 8); de même, on peut écrire les isomorphismes canoniques suivants:

$$(S^d)^{-1} A \simeq T^{-1} A \simeq S^{-1} A.$$

Cela étant:

THÉORÈME (4.4). *Avec les notations* (4.3):

(i) *Pour tout élément $x = a/t$ de $T^{-1}A_d$, appelons $f(x)$ l'élément a/t de $S^{-1}A$; alors $f(x)$ ne dépend effectivement que de x, et non du couple (a, t) servant à représenter x.*

(ii) *L'application f est un homomorphisme injectif de l'anneau $T^{-1}A_d$ dans l'anneau $S^{-1}A$.*

(iii) *L'image de f est égale à $(S^{-1}A)_d$, de sorte que f définit un isomorphisme canonique*

$$T^{-1}A_d \simeq (S^{-1}A)_d.$$

(*Le plus souvent, nous identifierons purement et simplement ces deux anneaux.*)

Démonstration. (i) et (ii) se vérifient par un simple calcul à la main; on peut également utiliser les résultats de [5], loc. cit.; prouvons maintenant (iii); tout d'abord, on a

$$f(T^{-1}A_d) \subset (S^{-1}A)_d;$$

soit en effet $x = a/t$ ($a \in A_d$, $t \in T$) un élément de $T^{-1}A_d$; on peut l'écrire $x = at^{d-1}/t^d$, et comme $a \in A_d$, $t \in A_d$ et que A_d est un anneau, on a $at^{d-1} \in A_d$; d'où une écriture

$$at^{d-1} = \sum e_j a_j^d \quad (\text{les } e_j = \pm 1, \text{ les } a_j \in A).$$

Et on constate alors que $f(x) = \sum e_j (a_j/t)^d$, donc que $f(x) \in (S^{-1}A)_d$.

Inversement, on a l'inclusion

$$(S^{-1}A)_d \subset f(T^{-1}A_d);$$

en effet, soit $y = \sum e_j (a_j/s_j)^d$ (les $e_j = \pm 1$, les $a_j \in A$, les $s_j \in S$) un élément de $(S^{-1}A)_d$; quitte à opérer une réduction au même dénominateur, on peut supposer tous les s_j égaux à un même s: mais y s'écrit alors sous la

forme $(\sum e_j a_j^d)/s^d$, et comme le numérateur appartient à A_d et le dénominateur à $S^d \subset T$, y est bien de la forme $f(x)$ pour un $x \in T^{-1}A_d$.

COROLLAIRE (4.5). *Soient $\mathfrak{P}$ un idéal premier de A, et $\mathfrak{p}$ l'idéal premier $\mathfrak{P} \cap A_d$ de A_d au-dessous de $\mathfrak{P}$. Il existe alors un isomorphisme canonique*

$$(A_{\mathfrak{P}})_d \simeq (A_d)_{\mathfrak{p}}.$$

Conservons les notations (4.3); comme T est une partie multiplicative de l'*anneau* A, on peut envisager l'*anneau de fractions* $T^{-1}A$. Mais d'autre part, A peut être considéré comme une A_d-algèbre, et on peut, par l'opération de passage au *module de fractions*, en déduire une $T^{-1}A_d$-*algèbre* $T^{-1}A$. En fait, les deux anneaux $T^{-1}A$ ainsi obtenus sont canoniquement isomorphes (ou même égaux: tout dépend de la définition choisie pour la notion de module de fractions) et il n'y a donc aucun risque de confusion. Et on peut énoncer:

PROPOSITION (4.6). *Avec les notations* (4.3), *il existe un isomorphisme canonique*

$$S^{-1}A \simeq (T^{-1}A_d) \underset{A_d}{\otimes} A.$$

Démonstration. Nous venons en effet de remarquer implicitement que

$$T^{-1}A \simeq (T^{-1}A_d) \underset{A_d}{\otimes} A,$$

et nous avions noté précédemment que $T^{-1}A \simeq S^{-1}A$.

COROLLAIRE (4.7). *Mêmes notations qu'au corollaire* (4.5). *Il existe alors un isomorphisme canonique*

$$A_{\mathfrak{P}} \simeq (A_d)_{\mathfrak{p}} \underset{A_d}{\otimes} A.$$

2. Le théorème de globalisation.

THÉORÈME (4.8). *Soient A un anneau, et d un entier $\geqslant 1$. Les trois assertions suivantes sont équivalentes*:

(a) $A_d = A$;

(b) *Quel que soit l'idéal premier $\mathfrak{P}$ de A, on a l'égalité*

$$(A_{\mathfrak{P}})_d = A_{\mathfrak{P}};$$

(c) *Quel que soit l'idéal maximal $\mathfrak{M}$ de A, on a l'égalité*

$$(A_{\mathfrak{M}})_d = A_{\mathfrak{M}}.$$

(*En d'autres termes, la condition $A_d = A$ passe du local au global.*)

Démonstration. (a) implique (b) en raison du corollaire (4.5). (b) implique (c) parce que tout idéal maximal est premier. Reste à montrer que (c) implique (a). Pour cela, désignons par u l'homomorphisme d'inclusion

$A_d \to A$, que nous considérerons comme un *homomorphisme de A_d-modules*: il s'agit de prouver que u est bijectif, ce que nous allons faire par passage du local au global. Notons d'abord qu'en vertu de la théorie du relèvement des idéaux premiers (voir par exemple [5], chapitre 5, § 2), le fait que A est entier sur A_d prouve que tout idéal maximal $\mathfrak{m}$ de A_d est de la forme $\mathfrak{M} \cap A_d$, où $\mathfrak{M}$ désigne un idéal maximal de A; et on a, $A_{\mathfrak{m}}$ désignant la localisée de la A_d-algèbre A par rapport à l'idéal maximal $\mathfrak{m}$ de A_d,

$$A_{\mathfrak{M}} \simeq A_{\mathfrak{m}},$$

(cas particulier de l'isomorphisme $T^{-1}A \simeq S^{-1}A$ vu plus haut). L'hypothèse (c) implique alors ceci: quel que soit $\mathfrak{m}$, idéal maximal de A_d, l'homomorphisme canonique $(A_d)_{\mathfrak{m}} \to A_{\mathfrak{m}}$ est un isomorphisme (noter que d'après le corollaire (4.5), l'anneau $(A_{\mathfrak{M}})_d$ s'identifie à l'anneau $(A_d)_{\mathfrak{m}}$). Avec les notations de [5], chapitre 2, § 3, n°3, ceci peut encore se dire: quel que soit $\mathfrak{m}$, idéal maximal de A_d, l'homomorphisme $u_{\mathfrak{m}}$ est bijectif; il suffit alors d'appliquer le théorème 1 (loc. cit.) pour conclure que u lui-même est bijectif. C.Q.F.D.

Ce théorème (4.8) sera utilisé au paragraphe 4 pour déterminer à quelles conditions un anneau d'entiers algébriques A satisfait à la relation $A_d = A$.

3. Le cas intègre. Supposons maintenant A intègre, de corps des fractions K; les divers anneaux envisagés ci-dessus: A_d, $S^{-1}A$, $T^{-1}A_d$, etc..., sont alors des sous-anneaux de K, et les isomorphismes de la théorème (4.4) et du corollaire (4.5) sont des égalités de sous-anneaux de K. En particulier, faisons, dans (4.5), $\mathfrak{P} = (0)$; nous obtenons

PROPOSITION (4.9). *Si A est un anneau intègre, de corps des fractions K, le corps K_d coïncide avec le corps des fractions de l'anneau A_d.*

On retrouve ainsi un résultat déjà noté au chapitre 1.

De même, le théorème (4.8) devient, dans cette situation particulière

PROPOSITION (4.10). *Soient A un anneau intègre et d un entier $\geqslant 1$. On a la double égalité*

$$A_d = \bigcap_{\mathfrak{P}} A_{\mathfrak{P}} = \bigcap_{\mathfrak{M}} A_{\mathfrak{M}},$$

$\mathfrak{P}$ et $\mathfrak{M}$ décrivant respectivement l'ensemble des idéaux premiers et l'ensemble des idéaux maximaux de l'anneau A.

4. Application: condition $A = A_d$ pour un anneau d'entiers algébriques A. Soient K un corps de nombres algébriques, A l'anneau des entiers de K et D le discriminant de K. Pour tout idéal premier $\mathfrak{P}$ non nul de A, désignons

par $p_{\mathfrak{P}}$ la caractéristique du corps résiduel $A/\mathfrak{P}$,

par $e_{\mathfrak{P}}$ l'indice de ramification $e(\mathfrak{P}|p_{\mathfrak{P}})$,

par $f_{\mathfrak{P}}$ le degré résiduel $f(\mathfrak{P}|p_{\mathfrak{P}})$,

par $N\mathfrak{P}$ le nombre d'éléments du corps résiduel $A/\mathfrak{P}$;

on a alors évidemment $N\mathfrak{P} = p_{\mathfrak{P}}^{f_{\mathfrak{P}}}$.

THÉORÈME (4.11). *Soit d un entier $\geqslant 1$. Avec les conventions ci-dessus, les trois conditions suivantes sont équivalentes:*

(a) $A = A_d$.

(b) *Pour tout idéal premier $\mathfrak{P}$ non nul, on a $A/\mathfrak{P} = (A/\mathfrak{P})_d$, et de plus si $p_{\mathfrak{P}}$ divise d, on a $e_{\mathfrak{P}} = 1$.*

(c) *D et d sont premiers entre eux, et de plus, si $p_{\mathfrak{P}} \leqslant d$, on a $[N\mathfrak{P}; d] = N\mathfrak{P}$.*

(Pour la notation utilisée à la dernière ligne, voir chapitre 2, définition (2.1).)

Démonstration. L'équivalence entre (b) et (c) résulte

— du lien entre discriminant et ramification (voir par exemple [28], tome 1, chapitre V, § 11);

— du théorème (2.3), et du fait que $A/\mathfrak{P} = \boldsymbol{F}_{N\mathfrak{P}}$;

— enfin, de la remarque suivante: si $p > d$ et si q est une puissance quelconque de p, alors $[q; d] = d$.

L'équivalence entre (a) et (b) résulte

— du théorème (4.8);

— du théorème (2.19);

— enfin, du fait que, pour tout idéal premier non nul $\mathfrak{P}$ de A, le localisé $A_{\mathfrak{P}}$ est un anneau de valuation discrète d'inégales caractéristiques, de corps résiduel isomorphe à $A/\mathfrak{P}$, et d'indice de ramification absolu égal à $e_{\mathfrak{P}}$.

Ce théorème résout complètement un problème posé par Siegel, et auquel Bateman et Stemmler avaient donné une réponse dans le cas d'un exposant d premier (voir [2]).

Illustrons ce résultat par deux exemples très simples.

EXEMPLE (4.12). Posons $A = \boldsymbol{Z}[i]$ et $d = 2$; on a alors $D = 4$, divisible par 2, de sorte que $A_2 \neq A$; et on vérifie effectivement sans peine que $A_2 = \boldsymbol{Z}[2i]$.

EXEMPLE (4.13). Posons encore $A = \boldsymbol{Z}[i]$, mais prenons maintenant $d = 3$; on a toujours $D = 4$, de sorte que d et D sont premiers entre eux; il y a deux idéaux premiers de A à envisager: d'une part $\mathfrak{P} = (1+i)A$, le seul pour lequel on ait $p_{\mathfrak{P}} = 2$; mais on a $N\mathfrak{P} = 2$, donc $[N\mathfrak{P}; d] = [2; 3] = 2 = N\mathfrak{P}$; et d'autre part $\mathfrak{P} = 3A$, le seul pour lequel on ait $p_{\mathfrak{P}} = 3$; mais on a alors $N\mathfrak{P} = 9$, donc $[N\mathfrak{P}; d] = [9; 3] = 9 = N\mathfrak{P}$. Le théorème (4.11) montre ainsi que $A = A_3$; et de fait, on a $-i = i^3 \in A_3$, d'où évidemment $A_3 = \boldsymbol{Z}[i] = A$.

Chapitre 5

CORRESPONDANCE ENTRE IDÉAUX DE A ET DE A_d

1. Généralités. Soient A un anneau, et d un entier $\geqslant 1$. La question suivante se pose: *existe-t-il une correspondance simple entre l'ensemble* $\mathrm{Id}(A)$ *des idéaux de l'anneau* A, *et l'ensemble* $\mathrm{Id}(A_d)$ *des idéaux du sous-anneau* A_d?

A priori, on peut définir de façon naturelle deux applications h et j de $\mathrm{Id}(A)$ dans $\mathrm{Id}(A_d)$:

l'application h: $\mathrm{Id}(A) \to \mathrm{Id}(A_d)$, sera celle qui, à tout idéal $\mathfrak{a}$ de A, fait correspondre son intersection $\mathfrak{a} \cap A_d$ avec A_d;

l'application j: $\mathrm{Id}(A) \to \mathrm{Id}(A_d)$, sera celle qui, à tout idéal $\mathfrak{a}$ de A, fait correspondre l'ensemble des éléments de A_d de la forme

$$e_1 a_1^d + e_2 a_2^d + \ldots + e_m a_m^d$$

avec $m \geqslant 1$ quelconque, les $e_j = \pm 1$, les $a_j \in \mathfrak{a}$; cet ensemble est effectivement un idéal de A_d, comme on le voit sans peine.

Notons que $h \neq j$ en général: si $d \geqslant 2$ et si A est un anneau de valuation discrète d'uniformisante π, tel que $A = A_d$ (voir le théorème (2.19)), on aura évidemment $h(\pi A) = \pi A$, mais $j(\pi A) = \pi^d A$, donc $h(\pi A) \neq j(\pi A)$.

Il se trouve malheureusement que les applications h et j ne sont en général ni injectives ni surjectives. Nous allons le voir sur des exemples:

L'application h n'est pas surjective en général.

Démonstration. Remarquons que si $\mathfrak{a} \in \mathrm{Id}(A_d)$ est de la forme $\mathfrak{A} \cap A_d$, $(\mathfrak{A} \in \mathrm{Id}(A))$, on a

$$\mathfrak{a} \subset (A\mathfrak{a}) \cap A_d \subset \mathfrak{A} \cap A_d = \mathfrak{a};$$

il suffit donc de trouver un exemple où l'on ait

$$(*) \qquad (A\mathfrak{a}) \cap A_d \neq \mathfrak{a}.$$

Voici comment on peut procéder: A étant un anneau intègre infini de corps des fractions K parfait, et d un entier $\geqslant 2$, on a vu au chapitre 2 que $K_d = K$, mais on sait bien qu'en général, $A_d \neq A$. Supposons ces conditions réalisées: il existe alors $a \in A$ tel que $a \notin A_d$; comme K est le corps des fractions de A_d, on peut néanmoins écrire

$$a = b/q \quad \text{avec} \quad b, q \in A_d,\ q \neq 0.$$

Je dis que l'idéal $\mathfrak{a} = A_d \cdot q \in \mathrm{Id}(A_d)$ satisfait à l'inégalité (*): en effet, comme $a \in A$, que $q \in \mathfrak{a}$ et que $aq = b \in A_d$, on a

$$aq \in (A\mathfrak{a}) \cap A_d.$$

Mais $aq \notin \mathfrak{a}$: l'assertion $aq \in \mathfrak{a}$ impliquerait en effet l'existence de $a' \in A_d$ tel que $a'q = aq$, soit $a' = a$, puisque A est intègre et que $q \neq 0$; mais on aurait alors $a = a' \in A_d$, contrairement aux hypothèses.

Exemple explicite. Prenons $A = \boldsymbol{Z}[i]$, anneau des entiers de Gauss, $K = \boldsymbol{Q}(i)$, $d = 2$ (exposant) et $q = 2$ (élément de K). Alors $A_2 = \boldsymbol{Z}[2i]$; on a bien $2 \in A_2$, et on voit que $\mathfrak{a} = \{2a + 4bi \mid a, b \in \boldsymbol{Z}\}$. De là la relation $2i \notin \mathfrak{a}$, alors que cependant $2i = i \cdot 2 \in (A\mathfrak{a}) \cap A_2$.

L'application h n'est pas injective en général.

Démonstration. L'idée est la suivante: trouver un anneau A, un entier $d \geqslant 2$ et un idéal maximal $\mathfrak{M}$ de A tels que $\mathfrak{M} \neq \mathfrak{M}^2$, mais que $\mathfrak{M} \cap A_d = \mathfrak{M}^2 \cap A_d$. C'est possible:

Exemple explicite. Prenons encore $A = \boldsymbol{Z}[i]$, $d = 2$, et faisons $\mathfrak{M} = (1+i)A$. Alors $\mathfrak{M}^2 = 2A$, et on a $\mathfrak{M}^2 \subset A^2$ (cas particulier de $d!\, A \subset A_d$); donc

$$\mathfrak{M}^2 = \mathfrak{M}^2 \cap A_2 \subset \mathfrak{M} \cap A_2.$$

Maintenant, $\mathfrak{M} \cap A_2$ est un idéal maximal de A_2: pour prouver que $\mathfrak{M} \cap A_2 = \mathfrak{M}^2 \cap A_2$, il suffit de montrer que $\mathfrak{M}^2$ est un idéal maximal de A_2, autrement dit, que $A_2/\mathfrak{M}^2$ est un corps. Mais

$$A_2 = \{a + bi \mid a \text{ quelconque},\ b \text{ pair}\},$$

$$\mathfrak{M}^2 = \{a + bi \mid a \text{ et } b \text{ tous deux pairs}\};$$

l'anneau $A_2/\mathfrak{M}^2$ est donc réduit à deux éléments: c'est le corps premier à deux éléments, ce qui achève la démonstration.

L'application j n'est pas surjective en général.

Exemple. Prenons $d \geqslant 2$, et soit A un anneau de valuation discrète d'uniformisante π, tel que $A = A_d$ (voir théorème (2.19)). On a alors $\mathrm{Id}(A) = \mathrm{Id}(A_d) =$ l'ensemble des $\pi^n A$ $(n \geqslant 0)$. Mais $j(\mathrm{Id}(A))$ est constitué seulement de l'ensemble des idéaux $\pi^n A$ avec n divisible par d.

L'application j n'est pas injective en général.

Exemple. Prenons $d \geqslant 2$, et posons

$B = \boldsymbol{Q}[X, Y, U, V]$, anneau des polynômes à quatre indéterminées sur le corps $\boldsymbol{Q}$;

$\mathfrak{b}$ = l'idéal de B engendré par les polynômes $X^d - UY^d$, $Y^d - VX^d$, $UV - 1$;

A = l'anneau quotient $B/\mathfrak{b}$, que l'on peut écrire $\boldsymbol{Q}[x, y, u, v]$ (x, y, u, v, images canoniques de X, Y, U, V dans A).

On a alors $A = A_d$, puisque A est une algèbre sur $\boldsymbol{Q}$, corps de caractéristique 0 (voir théorème (2.8)). De plus les éléments x^d et y^d sont associés, puisque $x^d = uy^d$ et $y^d = vx^d$. Mais du fait que $j(xA) = x^d A$

et $j(yA) = y^d A$, on voit alors que xA et yA, idéaux distincts, donnent par j le même idéal: j n'est pas injective, C.Q.F.D.

Remarquons d'autre part que, alors que l'application h transforme évidemment les idéaux premiers en idéaux premiers, ce n'est pas le cas pour l'application j: dans l'exemple de l'anneau de valuation discrète donné plus haut, l'idéal πA est premier, mais l'idéal $j(\pi A) = \pi^d A$ ne l'est pas, puisqu'on a choisi $d \geqslant 2$. De ce fait, nous abandonnons désormais l'application j, et nous nous intéresserons seulement à l'application h, qui a le mérite d'établir une bijection entre l'ensemble des idéaux premiers de A et celui des idéaux premiers de A_d, ainsi que nous le verrons au paragraphe 2.

Notons enfin qu'on peut se poser le problème suivant: *si l'anneau A est noethérien, l'anneau A_d est-il également noethérien?* Dans la plupart des cas usuels, la réponse est positive, comme le montrent les résultats du chapitre 3, et aussi du chapitre 2, paragraphe 2. Toutefois, dans le cas général, nous ne savons pas répondre; l'absence de bijection naturelle entre $\mathrm{Id}(A)$ et $\mathrm{Id}(A_d)$ conduirait à penser que l'on peut avoir simultanément A noethérien et A_d non noethérien, mais nous n'avons su construire aucun exemple d'une telle situation.

2. Correspondance entre idéaux premiers.

THÉORÈME (5.1). *L'application $\mathfrak{P} \mapsto \mathfrak{P} \cap A_d$ est une bijection de l'ensemble des idéaux premiers de A sur l'ensemble des idéaux premiers de A_d.*

Démonstration. Pour tout idéal premier $\mathfrak{p}$ de A_d, notons $g(\mathfrak{p})$ l'ensemble des $x \in A$ tels que $x^d \in \mathfrak{p}$. Nous allons montrer que $g(\mathfrak{p})$ est un idéal premier de A au-dessus de $\mathfrak{p}$, et que c'est le seul. En tout cas (voir [5], chapitre 5, § 2, n° 1, théorème 1) il existe un idéal premier $\mathfrak{P}$ de A tel que $\mathfrak{P} \cap A_d = \mathfrak{p}$. Je dis que $g(\mathfrak{p}) \subset \mathfrak{P}$: car si $x \in A$ et si $x^d \in \mathfrak{p}$, on a a fortiori $x^d \in \mathfrak{P}$, donc $x \in \mathfrak{P}$, puisque $\mathfrak{P}$ est premier. Je dis qu'inversement, $\mathfrak{P} \subset g(\mathfrak{p})$: car si $x \in \mathfrak{P}$, on a à la fois $x^d \in \mathfrak{P}$ et $x^d \in A_d$, donc $x^d \in \mathfrak{P} \cap A_d = \mathfrak{p}$, et par suite $x \in g(\mathfrak{p})$, par définition de $g(\mathfrak{p})$. Ainsi, $g(\mathfrak{p}) = \mathfrak{P}$ (ce qui prouve que $g(\mathfrak{p})$ est un idéal premier) et $\mathfrak{P} = g(\mathfrak{p})$ (ce qui prouve, $g(\mathfrak{p})$ ne dépendant que de $\mathfrak{p}$, qu'il n'y a qu'un seul $\mathfrak{P}$ au-dessus de $\mathfrak{p}$). $\mathfrak{P} \mapsto \mathfrak{P} \cap A_d$ est donc bien bijective, et g est la bijection inverse.

REMARQUE (5.2). Rappelons qu'un idéal est dit semi-premier s'il est intersection d'idéaux premiers, autrement dit, s'il est égal à sa racine; la démonstration ci-dessus prouve plus généralement que

$$\mathfrak{J} \mapsto \mathfrak{J} \cap A_d \quad \text{et} \quad \mathfrak{i} \mapsto \{x \mid x \in A \text{ et } x^d \in \mathfrak{i}\}$$

sont deux bijections réciproques l'une de l'autre entre l'ensemble des idéaux semi-premiers de A et l'ensemble des idéaux semi-premiers de A_d.

Revenons au théorème (5.1): les applications $\mathfrak{P} \mapsto \mathfrak{P} \cap A_d$ et $\mathfrak{p} \mapsto g(\mathfrak{p})$ sont manifestement croissantes, ce qui permet de le reformuler ainsi:

THÉORÈME (5.3). *Soit u l'injection canonique $A_d \to A$. Alors l'application continue*

$$\mathrm{Spec}(u) : \mathrm{Spec}(A) \to \mathrm{Spec}(A_d)$$

est un homéomorphisme, dont g est l'homéomorphisme inverse.

Le théorème (4.8) montre toutefois que $v = \mathrm{Spec}(u)$ n'est pas un isomorphisme d'espaces annelés (sauf évidemment si $A = A_d$).

3. Correspondance entre modules projectifs de rang 1. Donnons-nous toujours un anneau A et un entier $d \geqslant 1$; le théorème (5.3) nous autorise à faire les conventions suivantes, qui seront valables dans toute la suite de ce chapitre:

CONVENTIONS (5.4). Nous identifierons $\mathrm{Spec}(A)$ et $\mathrm{Spec}(A_d)$ et nous poserons pour simplifier

$$X = \mathrm{Spec}(A) = \mathrm{Spec}(A_d).$$

Si x est un point de X, nous noterons respectivement $\mathfrak{J}_x$ et $\mathfrak{j}_x = \mathfrak{J}_x \cap A_d$ les idéaux premiers de A et A_d auxquels x s'identifie.

L'espace X est alors muni de deux faisceaux:

le faisceau structural de $\mathrm{Spec}(A)$, que nous noterons $\mathscr{O}$, et dont la fibre en tout $x \in X$ est

$$\mathscr{O}_x = A_{\mathfrak{J}_x};$$

le faisceau structural de $\mathrm{Spec}(A_d)$ que nous noterons $\mathscr{O}_d$, et dont la fibre en tout $x \in X$ est

$$(\mathscr{O}_d)_x = (A_d)_{\mathfrak{j}_x}.$$

Enfin, nous noterons $\mathscr{A}$ et $\mathscr{A}_d$ les faisceaux constants sur X égaux respectivement à A et A_d.

Cela étant:

PROPOSITION (5.5). *Avec les conventions* (5.4):

(i) *$\mathscr{O}_d$ un sous-faisceau de $\mathscr{O}$.*

(ii) *Les faisceaux $\mathscr{O}$, $\mathscr{O}_d$, $\mathscr{A}$ et $\mathscr{A}_d$ sont liés par un isomorphisme canonique*

$$\mathscr{O} \simeq \mathscr{A} \underset{\mathscr{A}_d}{\otimes} \mathscr{O}_d$$

(noter que $\mathscr{O}$, $\mathscr{A}$ et $\mathscr{O}_d$ sont des faisceaux de $\mathscr{A}_d$-modules).

Démonstration. L'assertion (i) est évidente. Quant à (ii), c'est une reformulation globale de (4.7).

Nous allons appliquer ce qui précède à l'étude de la correspondance entre *modules projectifs de rang* 1 sur A et sur A_d. Rappelons que si A est un anneau, on appelle *groupe de Picard de* A (notation: $\mathrm{Pic}(A)$; voir [5], chapitre 2, § 5, n° 4) le groupe des classes de A-modules projectifs de rang 1.

THÉORÈME (5.6). *Désignons par u l'homomorphisme canonique d'inclusion $A_d \to A$, et par*

$$\bar{u} : \mathrm{Pic}(A_d) \to \mathrm{Pic}(A)$$

l'homomorphisme correspondant, pour les groupes de Picard. Dans ces conditions, le noyau et le conoyau de $\bar{u}$ sont des groupes de torsion d'exposant d.

Démonstration. Sur $X = \mathrm{Spec}(A_d) = \mathrm{Spec}(A)$, considérons $\mathcal{O}^*$ et $\mathcal{O}_d^*$, faisceaux des unités de $\mathcal{O}$ et $\mathcal{O}_d$ respectivement. On sait (voir [5], loc. cit.) qu'on a des identifications

$$(5.6.1) \qquad \begin{cases} \mathrm{Pic}(A) = H^1(X, \mathcal{O}^*), \\ \mathrm{Pic}(A_d) = H^1(X, \mathcal{O}_d^*). \end{cases}$$

Soit alors $\mathcal{G}$ le faisceau quotient $\mathcal{O}^*/\mathcal{O}_d^*$. La fibre de $\mathcal{G}$ au-dessus de tout $x \in X$ peut s'écrire, compte tenu de (4.5),

$$\mathcal{G}_x = A^*_{\mathfrak{I}_x}/(A_{\mathfrak{I}_x})^*_d;$$

c'est un groupe de torsion d'exposant d, car $(A_{\mathfrak{I}_x})^*_d \supset (A^*_{\mathfrak{I}_x})^d$. Le fait que l'élévation à la puissance d-ième commute à la cohomologie prouve alors que, quel que soit l'entier $q \geqslant 0$, le groupe $H^q(X, \mathcal{G})$ est un groupe de torsion d'exposant d. Ecrivons maintenant la suite exacte de cohomologie associée à la suite $1 \to \mathcal{O}_d \to \mathcal{O} \to \mathcal{G} \to 1$. On peut en extraire le tronçon suivant

$$H^0(X, \mathcal{G}) \xrightarrow{\delta} H^1(X, \mathcal{O}_d^*) \xrightarrow{u_1} H^1(X, \mathcal{O}^*) \xrightarrow{v_1} H^1(X, \mathcal{G}),$$

qui s'écrit aussi, compte tenu de (5.6.1),

$$H^0(X, \mathcal{G}) \xrightarrow{\delta} \mathrm{Pic}(A_d) \xrightarrow{\bar{u}} \mathrm{Pic}(A) \xrightarrow{v_1} H^1(X, \mathcal{G}).$$

Or, on vient de voir que les termes extrêmes de cette suite sont des groupes de torsion d'exposant d: il en résulte immédiatement que $\ker(\bar{u})$ et $\mathrm{coker}(\bar{u})$ sont également des groupes de torsion d'exposant d, C.Q.F.D.

4. Cas intègre: correspondance entre idéaux inversibles. Dans ce paragraphe et dans le suivant, A désigne un anneau *intègre infini* (si A, intègre, est fini, c'est un corps, ainsi que A_d, et l'étude des idéaux inversibles est triviale); K désigne le corps des fractions de A et p l'*exposant caractéristique* de K; les conventions (5.4) restent en vigueur.

Ecrivons $d = p^r \cdot d_1$ avec $(p, d_1) = 1$. Il est clair alors que $x \mapsto x^{p^r}$ définit un isomorphisme de K_{d_1} sur $(K_{d_1})^{p^r} = K_d$, isomorphisme qui applique A_{d_1} sur A_d; comme K_{d_1} (resp. K_d) est le corps des fractions de A_{d_1} (resp. A_d), l'étude des idéaux inversibles de A_d équivaut donc à celle des idéaux inversibles de A_{d_1}, ce qui nous permet de supposer désormais l'entier d *étranger à* p. Or, nous avons vu au chapitre 2, corollaire (2.9), que si K est infini et si $(p, d) = 1$, $K_d = K$. Nous nous sommes donc ramenés sans restriction de la généralité, à une situation où les anneaux A et A_d ont le même *corps des fractions* K.

Ces hypothèses et remarques étant faites, rappelons (voir [5], chapitre 2, § 5, n° 6) que dans le cas intègre, le groupe de Picard $\mathrm{Pic}(A)$ s'identifie au groupe $\mathscr{C}(A)$ des classes d'idéaux (fractionnaires) inversibles de A; et de même pour A_d. L'homomorphisme $\bar{u} : \mathrm{Pic}(A_d) \to \mathrm{Pic}(A)$ déduit de l'inclusion $u : A_d \to A$, s'identifie alors à l'homomorphisme $\mathscr{C}(A_d) \to \mathscr{C}(A)$ obtenu de la façon suivante: à tout idéal inversible $\mathfrak{i}$ de A_d, on associe $A \cdot \mathfrak{i}$, idéal inversible de A; d'où, entre groupes d'idéaux inversibles, un homomorphisme $\tilde{u}$, qui applique en particulier le groupe des idéaux principaux de A_d dans celui des idéaux principaux de A; on prend alors l'homomorphisme $\mathscr{C}(A_d) \to \mathscr{C}(A)$ coïnduit par $\tilde{u}$.

Conservons pour cet homomorphisme la notation $\bar{u}$. Le théorème (5.6) donne alors l'énoncé suivant:

PROPOSITION (5.7). *Avec les hypothèses et notations ci-dessus, le noyau et le conoyau de l'homomorphisme*

$$\bar{u} : \mathscr{C}(A_d) \to \mathscr{C}(A)$$

sont des groupes de torsion d'exposant d.

Dans ce qui suit, nous garderons la notation $\mathrm{Pic}(A)$, car il nous arrivera, dans un même diagramme, de rencontrer des anneaux intègres et des anneaux non intègres.

Aux hypothèses A intègre infini et d étranger à p faites au début de ce paragraphe, nous en ajouterons une, valable également dans ce paragraphe et dans le suivant: A sera supposé *intégralement clos*. Nous utiliserons en outre les notations et conventions suivantes qui complètent (5.4):

CONVENTIONS (5.8). $\mathfrak{f}$ désignera le *conducteur* de A_d dans A; $\mathfrak{b}$ désignera un idéal (quelconque) de A contenu dans $\mathfrak{f}$; $\mathfrak{b}$ sera donc aussi un idéal de A_d; B désignera l'anneau quotient $A/\mathfrak{b}$; on aura alors évidemment $B_d = A_d/\mathfrak{b}$.

Les conventions (5.4) resteront en vigueur; en particulier, X désignera toujours l'espace $\mathrm{Spec}(A)$ $(= \mathrm{Spec}(A_d))$; toutefois, on notera $\mathcal{O}_X$, $(\mathcal{O}_d)_X$ et $\mathcal{G}_X$ les faisceaux sur X notés précédemment $\mathcal{O}$, $\mathcal{O}_d$ et $\mathcal{G}$ $(= \mathcal{O}^*/\mathcal{O}_d^*)$.

De plus, Y désignera l'espace $\mathrm{Spec}(B)$ $(= \mathrm{Spec}(B_d))$ que l'on identifiera au sous-espace fermé $V(\mathfrak{b})$ de X (voir [5], chapitre 2, § 4, n° 3). Enfin, $\mathscr{O}_Y$, $(\mathscr{O}_d)_Y$ et $\mathscr{G}_Y$ auront, relativement à Y, les significations correspondant à celles qu'ont $\mathscr{O}_X$, $(\mathscr{O}_d)_X$ et $\mathscr{G}_X$ relativement à X.

Cela étant:

THÉORÈME (5.9). *Le faisceau $\mathscr{G}_X$ est trivial en dehors du fermé $Y \subset X$. De plus, sa restriction à Y est égale au faisceau $\mathscr{G}_Y$.*

Démonstration. Soit $x \in X$; supposons d'abord $x \notin Y$. Cela signifie $\mathfrak{b} \not\subset \mathfrak{j}_x$ et a fortiori $\mathfrak{f} \not\subset \mathfrak{j}_x$; le conducteur $\mathfrak{f}$ rencontre la partie multiplicative $A_d \setminus \mathfrak{j}_x$ de A_d; comme A est la clôture intégrale de A_d, ceci implique (voir [5], chapitre 5, p. 23, corollaire 4, (ii)) que le localisé $(A_d)_{\mathfrak{j}_x}$ est intégralement clos. Mais $(A_d)_{\mathfrak{j}_x}$ a même corps des fractions K que $A_{\mathfrak{J}_x}$, qui est entier sur $(A_d)_{\mathfrak{j}_x}$. Finalement,

$$(A_d)_{\mathfrak{j}_x} = A_{\mathfrak{J}_x},$$

et $\mathscr{G}_{X,x} = 1$; $\mathscr{G}_X$ est effectivement concentré sur Y.

Supposons maintenant $x \in Y$, donc $\mathfrak{b} \subset \mathfrak{j}_x$. Il est clair que

$$\mathfrak{b} A_{\mathfrak{J}_x} = \mathfrak{b}(A_d)_{\mathfrak{j}_x},$$

$$B_{(\mathfrak{J}_x/\mathfrak{b})} \simeq A_{\mathfrak{J}_x}/\mathfrak{b} A_{\mathfrak{J}_x},$$

$$(B_d)_{(\mathfrak{j}_x/\mathfrak{b})} \simeq (A_d)_{\mathfrak{j}_x}/\mathfrak{b}(A_d)_{\mathfrak{j}_x}.$$

(Rappelons que $B = A/\mathfrak{b}$). On a donc un diagramme commutatif de A_d-modules, à lignes et colonnes exactes:

$$\begin{array}{ccccccc}
0 & \to & \mathfrak{b} A_{\mathfrak{J}_x} & \longrightarrow & A_{\mathfrak{J}_x} & \longrightarrow & B_{(\mathfrak{J}_x/\mathfrak{b})} \to 0 \\
 & & \| & & \uparrow & & \uparrow \\
0 & \to & \mathfrak{b}(A_d)_{\mathfrak{j}_x} & \to & (A_d)_{\mathfrak{j}_x} & \to & (B_d)_{(\mathfrak{j}_x/\mathfrak{b})} \to 0 \\
 & & & & \uparrow & & \uparrow \\
 & & & & 0 & & 0
\end{array}$$

Or, si L est un anneau local, $\mathfrak{a}$ un idéal de L et Λ l'anneau local quotient $L/\mathfrak{a}$, on a la suite exacte de groupes multiplicatifs

$$1 \to 1 + \mathfrak{a} \to L^* \to \Lambda^* \to 1.$$

Ce résultat, appliqué aux anneaux locaux du diagramme ci-dessus, donne un deuxième diagramme (de groupes multiplicatifs) à lignes et colonnes exactes (l'exactitude des colonnes tient en particulier à la définition de $\mathscr{G}_X$ et $\mathscr{G}_Y$):

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & \\
 & & \uparrow & & \uparrow & & \\
 & & \mathscr{G}_{X,x} & & \mathscr{G}_{Y,x} & & \\
 & & \uparrow & & \uparrow & & \\
1 & \to 1+\mathfrak{b}A_{\mathfrak{J}_x} & \to \mathscr{O}_{X,x} & \to \mathscr{O}_{Y,x} & \to 1 & & \\
 & & \uparrow & & \uparrow & & \\
1 & \to 1+\mathfrak{b}(A_d)_{\mathfrak{j}_x} & \to (\mathscr{O}_d)_{X,x} & \to (\mathscr{O}_d)_{Y,x} & \to 1 & & \\
 & & \uparrow & & \uparrow & & \\
 & & 1 & & 1 & &
\end{array}$$

Il est clair alors qu'il existe une flèche $\mathscr{G}_{X,x} \to \mathscr{G}_{Y,x}$ et une seule laissant le diagramme commutatif, et que cette flèche est un isomorphisme: d'où le théorème.

COROLLAIRE (5.10). *Quel que soit l'entier $q \geqslant 0$,*

$$H^q(X, \mathscr{G}_X) \simeq H^q(Y, \mathscr{G}_Y).$$

COROLLAIRE (5.11). *On a, dans la catégorie des groupes commutatifs le diagramme commutatif suivant, à lignes exactes:*

$$\begin{array}{ccccccccccc}
1 & \to B_d^* & \to B^* & \to H^0(Y, \mathscr{G}_Y) & \xrightarrow{\delta_Y} & \mathrm{Pic}(B_d) & \to \mathrm{Pic}(B) & \to H^1(Y, \mathscr{G}_Y) \\
 & \uparrow & \uparrow & \| & & \uparrow & \uparrow & \| \\
1 & \to A_d^* & \to A^* & \to H^0(X, \mathscr{G}_X) & \xrightarrow{\delta_X} & \mathrm{Pic}(A_d) & \xrightarrow{\bar{u}} \mathrm{Pic}(A) & \to H^1(X, \mathscr{G}_X)
\end{array}$$

Démonstration. Il suffit d'écrire le diagramme à lignes exactes

$$\begin{array}{ccccccc}
1 & \to (\mathscr{O}_d)_Y^* & \to \mathscr{O}_Y^* & \to \mathscr{G}_Y & \to 1 \\
 & \uparrow & \uparrow & \uparrow & \\
1 & \to (\mathscr{O}_d)_X^* & \to \mathscr{O}_X^* & \to \mathscr{G}_X & \to 1,
\end{array}$$

de passer aux suites exactes de cohomologie (limitées au degré 1), et d'appliquer le corollaire (5.10) et les identifications telles que

$$H^0(X, \mathscr{O}_X) \simeq A^*,$$
$$H^1(X, \mathscr{O}_X) \simeq \mathrm{Pic}(A).$$

Nous allons indiquer deux applications des résultats précédents.

Première application.

PROPOSITION (5.12). *Soit A un anneau intègre, intégralement clos et infini. Conservons les conventions* (5.8).

Si $B^* = B_d^*$, et si $\mathrm{Pic}(A) = \mathrm{Pic}(B) = 0$, on a l'isomorphisme suivant:

$$\mathrm{Pic}(B_d) \simeq \mathrm{Pic}(A_d) \otimes (A^*/A_d^*).$$

Démonstration. Le corollaire (5.11) permet d'écrire le diagramme commutatif à lignes exactes

$$\begin{array}{ccccccc} & & 0 & \to H^0(Y,\mathscr{O}_Y) & \to \mathrm{Pic}(B_d) & \to 0 \\ & & & \| & \uparrow & \\ 1 & \to A_d^* & \to A^* & \to H^0(X,\mathscr{O}_X) & \to \mathrm{Pic}(A_d) & \to 0 \end{array}$$

ce qui donne immédiatement l'isomorphisme annoncé.

Exemple. Prenons $A = \boldsymbol{Z}[X]$ et $d = 2$. L'inclusion $d!\,A \subset A_d$ donne $2A \subset A_2$, donc $2A \subset \mathfrak{f}$: nous pouvons prendre $\mathfrak{b} = 2A$. Dès lors, $B = \boldsymbol{F}_2[X]$ et $A_2 = \boldsymbol{Z}[X^2, 2X]$, $B_2 = \boldsymbol{F}_2[X^2]$. A, B et B_2 sont factoriels. De plus, $B^* = B_2^* = \{1\}$ et $A^* = A_2^* = \{-1, 1\}$.

La proposition (5.12) donne tout simplement $\mathrm{Pic}(A_2) = 0$. Ainsi: l'anneau intègre $\boldsymbol{Z}[X^2, 2X]$, qui n'est plus factoriel (il n'est pas intégralement clos), a cependant un groupe des classes d'idéaux inversibles nul.

Deuxième application.

Proposition (5.13). *Soit $m \geqslant 1$ un entier sans facteur carré, et désignons par A l'anneau des entiers du corps quadratique imaginaire $\boldsymbol{Q}(\sqrt{-m})$. Alors*

(i) *Si $m = 1$, on a $A_2 = \boldsymbol{Z}[2i] \neq A$, et $\mathrm{Pic}(A_2) = 0 = \mathrm{Pic}(A)$.*

(ii) *Si $m > 1$, et si $-m \equiv 1 \pmod 4$, on a $A_2 = A$, donc $\mathrm{Pic}(A_2) = \mathrm{Pic}(A)$.*

(iii) *Si $m > 1$, et si $-m \equiv 2$ ou $3 \pmod 4$, on a $A_2 \neq A$, et le groupe $\mathrm{Pic}(A_2)$ est extension du groupe $\mathrm{Pic}(A)$ par un groupe cyclique d'ordre 2.*

Démonstration. (i) L'égalité $A_2 = \boldsymbol{Z}[2i]$ est évidente ainsi que l'égalité $\mathrm{Pic}(A) = 0$ (A est factoriel). Reste à prouver que $\mathrm{Pic}(A_2) = 0$. Comme $2A \subset A_2$, nous pouvons prendre (voir (5.9)) $\mathfrak{b} = 2A$. L'anneau $B = A/\mathfrak{b}$ est alors formé de quatre éléments, les classes modulo 2 de 0, 1, i et $1+i$, soit

$$B = \{\bar{0}, \bar{1}, \bar{i}, \overline{1+i}\};$$

quant à B_2, il est égal au corps premier à deux éléments. Enfin, le sous-espace fermé Y de X est réduit à un point: l'idéal $(1+i)A$, seul idéal premier de A à contenir $\mathfrak{b} = 2A$; ceci permet d'écrire $H^1(Y, \mathscr{O}_Y) = 0$, et le diagramme du corollaire (5.11) devient ici

$$\begin{array}{ccccccccc} 1 & \longrightarrow & 1 & \longrightarrow & \{\bar{1}, \overline{1+i}\} & \longrightarrow H^0 & \to \mathrm{Pic}(B_2) & \to \mathrm{Pic}(B) & \to 0 \\ & & \uparrow & & \uparrow & \| & \uparrow & \uparrow & \\ 1 & \to \{-1,1\} & \to \{\pm 1, \pm i\} & \to H^0 & \to \mathrm{Pic}(A_2) & \to \mathrm{Pic}(A) & \to 0 & & \end{array}$$

Mais, A étant factoriel, B étant local, et B_2 étant un corps, on a $\mathrm{Pic}(A) = \mathrm{Pic}(B) = \mathrm{Pic}(B_2) = 0$. La suite exacte supérieure prouve alors que H^0 est un groupe d'ordre 2. Et la suite exacte inférieure, devenue

$$1 \to \{-1, 1\} \to \{\pm 1, \pm i\} \to H^0 \to \mathrm{Pic}(A_2) \to 0,$$

donne l'égalité

$$\mathrm{Card}\,\mathrm{Pic}(A_2) = \frac{\mathrm{Card}\{\pm 1, \pm i\}}{\mathrm{Card}\{-1, 1\} \cdot \mathrm{Card}\, H^0} = \frac{4}{2 \cdot 2} = 1,$$

soit effectivement $\mathrm{Pic}(A_2) = 0$.

(ii) et (iii). Supposons maintenant $m > 1$. D'après le théorème (4.11), les deux assertions suivantes sont équivalentes:

(a) $A_2 = A$;

(b) L'idéal (2) de $\boldsymbol{Z}$ est non-ramifié dans A.

Or (voir par exemple [28], tome 1, p. 312), l'assertion (b) équivaut à celle-ci:

(c) $-m \equiv 1 \pmod 4$.

L'équivalence de (a) et de (c) démontre (ii) et la première moitié de (iii). Reste à établir ceci:

si $m > 1$ et si $-m \equiv 2$ ou $3 \pmod 4$, le groupe $\mathrm{Pic}(A_2)$ est extension du groupe $\mathrm{Pic}(A)$ par un groupe cyclique d'ordre 2.

Nous allons utiliser à nouveau le corollaire (5.11) en prenant pour $\mathfrak{b}$ l'idéal $2A$. Encore que cela ne soit pas nécessaire, nous allons d'ailleurs prouver ceci:

Lemme (5.14). *Avec les hypothèses précédentes, le conducteur $\mathfrak{f}$ de A_2 dans A est égal à $2A$.*

Démonstration. Puisque $A_2 \neq A$, on a $\mathfrak{f} \neq A$. (2) étant ramifié, soit $\mathfrak{P}$ l'idéal premier de A tel que $\mathfrak{P}^2 = 2A$. On a évidemment

$$(*) \qquad 2A = \mathfrak{P}^2 \subset \mathfrak{f} \subset \mathfrak{P} \subset A,$$

d'où nécessairement (par exemple, parce que A est de Dedekind) $\mathfrak{f} = \mathfrak{P}$ ou $\mathfrak{f} = \mathfrak{P}^2 = 2A$. Mais $2A$ est un idéal maximal de A_2: en effet, l'anneau $A/2A = A/\mathfrak{P}^2$ est local artinien de longueur 2, de corps résiduel $\boldsymbol{F}_2$ (puisque (2) est ramifié). D'où sa structure:

$$A/2A = \{0, 1, \pi, 1+\pi\},$$

avec les relations $2\pi = \pi^2 = 0$. De là

$$(A/2A)_2 = A_2/2A = \{0, 1\} = \boldsymbol{F}_2;$$

ce quotient est un corps, et $2A$ est effectivement maximal dans A_2.

Supposons alors $\mathfrak{f} = \mathfrak{P}$; on aurait

$$\mathfrak{P} = \mathfrak{P} \cap A_2 = \mathfrak{P}^2 \cap A_2 = \mathfrak{P}^2,$$

(la première égalité parce que $\mathfrak{f} \subset A_2$, la troisième parce que $\mathfrak{P}^2 \subset A_2$ et la deuxième égalité parce que $\mathfrak{M} \mapsto \mathfrak{M} \cap A_2$ est une bijection du spectre maximal de A sur celui de A_2). L'égalité $\mathfrak{f} = \mathfrak{P}$ impliquerait ainsi $\mathfrak{P} = \mathfrak{P}^2$: absurde, puisque A est de Dedekind; on a donc forcément $\mathfrak{f} = \mathfrak{P}^2 = 2A$, C.Q.F.D.

La démonstration de ce lemme a prouvé que

$$B = A/2A = \{0, 1, \pi, 1+\pi\},$$
$$B_2 = A_2/2A = \{0, 1\} = \boldsymbol{F}_2.$$

Ces deux anneaux sont *locaux*, d'où

$$\mathrm{Pic}(B_2) = \mathrm{Pic}(B) = 1.$$

L'espace Y est réduit à un point, l'idéal premier $\mathfrak{P}$, d'où également

$$H^1(X, \mathscr{G}_X) = H^1(Y, \mathscr{G}_Y) = 0.$$

Enfin, $B_2^* = \{1\}$, et $B^* = \{1, 1+\pi\}$. Donc, toujours grâce au corollaire (5.11), $H^0(X, \mathscr{G}_X) = H^0(Y, \mathscr{G}_Y) =$ un groupe cyclique d'ordre 2. Maintenant, puisque les valeurs $-m = -1$ et $-m = -3$ sont exclues, on a $A_2^* = A^* = \{-1, 1\}$. On arrive finalement à une suite exacte:

$$1 \to H^0 \to \mathrm{Pic}(A_2) \to \mathrm{Pic}(A) \to 0,$$

où H^0 est cyclique d'ordre 2: ceci achève de prouver la proposition (5.13).

5. Cas d'un anneau de Dedekind. Dans tout ce paragraphe, nous conservons les hypothèses et conventions du paragraphe 3, en les particularisant ainsi: A est désormais supposé être un *anneau de Dedekind*, soumis en outre à la condition suivante:

(F) Le conducteur $\mathfrak{f}$ de A_d dans A n'est pas nul.

Nous poserons $\mathfrak{b} = \mathfrak{f}$. Notons ceci:

Proposition (5.15). *La condition* (F) *est vérifiée dans chacun des deux cas suivants (entre autres):*

(i) *A est sans torsion (autrement dit, K est de caractéristique 0).*

(ii) *A est un A_d-module de type fini.*

Démonstration. (i) entraîne (F) d'après la relation $d!\,A \subset A_d$. Prouvons que (ii) entraîne (F): puisque A_d et A ont même corps des fractions (convention faite au début du paragraphe 4), il existe un système générateur de A sur A_d de la forme $(a_1/b, a_2/b, \ldots, a_m/b)$, avec les $a_j \in A_d$, $b \in A_d$, et $b \neq 0$; mais alors

$$bA = \sum a_j A_d \subset A_d,$$

d'où $bA \subset \mathfrak{f}$, et $\mathfrak{f} \neq 0$.

On peut remarquer que la propriété (i) est satisfaite si A est un anneau d'entiers algébriques. Il est facile de vérifier par ailleurs que (ii) est satisfaite si A est une algèbre affine sur un corps parfait k (algèbre qu'on devra naturellement supposer intègre, intégralement close et de dimension 1 si l'on veut que ce soit un anneau de Dedekind).

Cela étant:

Proposition (5.16). *Si A est un anneau de Dedekind satisfaisant à* (F), *Y est un ensemble fini de points fermés de X.*

Démonstration. En effet, le conducteur $\mathfrak{f}$, n'étant pas nul, se décompose dans l'anneau de Dedekind A en facteurs premiers:

$$\mathfrak{f} = \mathfrak{P}_1^{n_1} \mathfrak{P}_2^{n_2} \ldots \mathfrak{P}_s^{n_s};$$

et le sous-espace Y (sur lequel $\mathscr{G}_X$ se trouve concentré; voir le théorème (5.9)) se compose des s points fermés $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_s$.

Corollaire (5.17). *La cohomologie du faisceau $\mathscr{G}_X$ est donnée par les formules suivantes:*

$$H^0(X, \mathscr{G}_X) = \prod_{x \in Y} A^*_{\mathfrak{I}_x}/(A_{\mathfrak{I}_x})^*_d;$$

$$H^q(X, \mathscr{G}_X) = 0 \quad \textit{pour tout } q \geqslant 1.$$

Démonstration. Il suffit d'appliquer le corollaire (5.11).

Notation (5.18). Pour alléger l'écriture, nous noterons Q le groupe produit

$$\prod_{x \in Y} A^*_{\mathfrak{I}_x}/(A_{\mathfrak{I}_x})^*_d = \prod_{x \in Y} A^*_{\mathfrak{I}_x}/(A_d)^*_{\mathfrak{i}_x}.$$

Corollaire (5.19). *On a la suite exacte de groupes*

$$1 \to A_d^* \xrightarrow{u^*} A^* \xrightarrow{\delta} Q \xrightarrow{\delta} \mathrm{Pic}(A_d) \xrightarrow{\bar{u}} \mathrm{Pic}(A) \to 0.$$

Démonstration. Ce corollaire est un cas particulier de (5.11), compte tenu de (5.17) et (5.18).

L'énoncé (5.19) amène plusieurs conséquences intéressantes.

Théorème (5.20). *A étant un anneau de Dedekind soumis à la condition* (F), *l'homomorphisme canonique*

$$\bar{u} : \mathrm{Pic}(A_d) \to \mathrm{Pic}(A)$$

est surjectif.

Démonstration. Regarder les trois termes de droite dans la suite exacte du corollaire (5.19). Remarquons qu'ici, puisque A est de Dedekind, $\mathrm{Pic}(A)$ est le *groupe des classes d'idéaux* de A. En revanche, A_d n'est pas un anneau de Dedekind en général, car si $A \neq A_d$, A_d n'est

pas intégralement clos. Le théorème (5.20) nous dit toutefois ceci: tout idéal fractionnaire de A est de la forme $A\cdot\mathfrak{i}$, où $\mathfrak{i}$ est un idéal inversible de A_d.

Deuxième conséquence de (5.19):

PROPOSITION (5.21). *L'homomorphisme* $\overline{u}$: $\mathrm{Pic}(A_d) \to \mathrm{Pic}(A)$ *n'est pas injectif en général.*

La démonstration résulte du contre-exemple ci-dessous:

CONTRE-EXEMPLE (5.22). Posons

$$K = \boldsymbol{Q}(\sqrt{-6}), \quad \text{corps quadratique imaginaire,}$$

$$A = \boldsymbol{Z}(\sqrt{-6}), \quad \text{anneau des entiers de } K,$$

et prenons pour exposant $d = 3$. Il est clair tout d'abord que $A_3 \neq A$: en effet, A_3 est engendré par les éléments de la forme

$$(a+b\sqrt{-6})^3 = (a^3-18ab^2)+(a^2b-2b^3)3\sqrt{-6},$$

ce qui implique $A_3 \subset \boldsymbol{Z}[3\sqrt{-6}] \neq A$. Maintenant, l'inégalité $A_3 \neq A$ implique $\mathfrak{f} \neq A$ (on a par ailleurs $\mathfrak{f} \neq 0$, puisque A est sans torsion: voir (5.15)). Il existe donc au moins un $x \in X = \mathrm{Spec}(A)$ tel que

$$A_{\mathfrak{J}_x} \neq (A_3)_{\mathfrak{i}_x} = (A_{\mathfrak{J}_x})_3.$$

Comme il s'agit d'anneaux locaux emboités, ceci implique

$$A^*_{\mathfrak{J}_x} \neq (A_{\mathfrak{J}_x})^*_3,$$

et par conséquent $Q \neq 1$. Considérons alors la suite exacte du corollaire (5.19); comme

$$A^*_3 = A^* = \{-1, 1\},$$

l'homomorphisme u^* est un isomorphisme; cette suite donne lieu à une nouvelle suite exacte:

$$1 \to Q \to \mathrm{Pic}(A_3) \xrightarrow{\overline{u}} \mathrm{Pic}(A) \to 0,$$

et le fait que $Q \neq 1$ montre bien que $\overline{u}$ n'est pas injectif.

Avant de donner une troisième conséquence du corollaire (5.19), introduisons un lemme:

LEMME (5.23). *Considérons la suite exacte de* (5.19):

(i) *Le noyau de* $\overline{u}$: $\mathrm{Pic}(A_d) \to \mathrm{Pic}(A)$ *est isomorphe au conoyau de* θ: $A^* \to Q$.

(ii) *D'autre part, le groupe* Q *est isomorphe à un quotient du groupe*

$$R = \prod_{x \in Y} (A_{\mathfrak{J}_x}/\mathfrak{f}A_{\mathfrak{J}_x})^*.$$

(iii) *A fortiori, le noyau de* $\overline{u}$ *est isomorphe à un quotient de* R.

Démonstration. L'isomorphisme $\ker(\overline{u}) \simeq \mathrm{coker}(\theta)$ est évident. Prouvons (ii): il suffit de montrer que, pour tout $x \in Y$, le groupe $(A_{\mathfrak{J}_x}/\mathfrak{f}A_{\mathfrak{J}_x})^*$ est un quotient de $A^*_{\mathfrak{J}_x}/(A_d)^*_{\mathfrak{i}_x}$. Or, on a $\mathfrak{f}A_{\mathfrak{J}_x} \subset \mathfrak{J}_x A_{\mathfrak{J}_x}$ d'une part; et d'autre part, puisque $\mathfrak{f}A \subset A_d$, $\mathfrak{f}A_{\mathfrak{J}_x} \subset (A_d)_{\mathfrak{i}_x}$. (Naturellement, $\mathfrak{f}A_{\mathfrak{J}_x} \neq 0$, par l'hypothèse (F).) Les deux inclusions ci-dessus donnent alors

$$1+\mathfrak{f}A_{\mathfrak{J}_x} \subset (1+\mathfrak{J}_x A_{\mathfrak{J}_x}) \cap (A_d)_{\mathfrak{i}_x} \subset A^*_{\mathfrak{J}_x} \cap (A_d)_{\mathfrak{i}_x},$$

ou finalement

$$1+\mathfrak{f}A_{\mathfrak{J}_x} \subset (A_d)^*_{\mathfrak{i}_x}.$$

Le groupe $A^*_{\mathfrak{J}_x}/(A_d)^*_{\mathfrak{i}_x}$ est donc un quotient du groupe $A^*_{\mathfrak{J}_x}/(1+\mathfrak{f}A_{\mathfrak{J}_x})$, lequel est précisément égal à $(A_{\mathfrak{J}_x}/\mathfrak{f}A_{\mathfrak{J}_x})^*$.

Démontrons (iii) : $\ker(\overline{u})$ est, d'après (i), isomorphe à $\mathrm{coker}(\theta)$ donc à un quotient de Q: mais Q est, par (ii), isomorphe à un quotient de R, donc $\ker(\overline{u})$ est isomorphe à un quotient de R, C.Q.F.D.

Cela étant, une troisième conséquence du corollaire (5.19) est celle-ci:

PROPOSITION (5.24). *Si* A *est un anneau d'entiers algébriques, le groupe* $\mathrm{Pic}(A_d)$ *des classes d'idéaux fractionnaires inversibles de l'anneau* A_d *est un groupe d'ordre fini.*

Démonstration. D'après le corollaire (5.19) et le lemme (5.23), on a une suite exacte

$$R \to \mathrm{Pic}(A_d) \xrightarrow{\overline{u}} \mathrm{Pic}(A) \to 1.$$

Maintenant, l'hypothèse faite sur A implique que $\mathrm{Pic}(A)$ est d'ordre fini; il suffit donc de prouver que R est lui-même d'ordre fini, ou encore, que chacun des anneaux quotients $A_{\mathfrak{J}_x}/\mathfrak{f}A_{\mathfrak{J}_x}$ est fini: mais c'est évident, car chaque $A_{\mathfrak{J}_x}$ est un anneau de valuation discrète à corps résiduel fini, et par ailleurs $\mathfrak{f}A_{\mathfrak{J}_x} \neq 0$ pour tout $x \in Y$, puisque $\mathfrak{f} \neq 0$.

Naturellement, la finitude du groupe $\mathrm{Pic}(A_d)$ n'est qu'un cas particulier de la finitude du groupe $\mathrm{Pic}(B)$ pour un ordre d'entiers algébriques quelconque B.

DEUXIÈME PARTIE

Chapitre 6

REPRÉSENTATION DE -1 COMME SOMME DE PUISSANCES d-IÈMES

1. Généralités sur $u(d; A)$. Rappelons que, A étant un anneau et d un entier $\geqslant 1$, la notation $u(d; A)$ désigne

le symbole ∞, si $-1 \notin A_d^+$;

le plus petit entier m tel que -1 puisse s'écrire comme somme de m puissances d-ièmes, dans le cas contraire.

La question de savoir si $u(d;A)$ est fini ou non ne se pose que si d est *pair*: sinon en effet, $-1=(-1)^d$, d'où $u(d;A)=1$. En outre, si A est *intègre*, avec corps des fractions de caractéristique p, cette question ne se pose que si $p=0$: sinon

$$-1=1^d+1^d+\ldots+1^d \quad (p-1 \text{ fois})$$

et $u(d;A)\leqslant p-1$.

Donnons ici deux résultats évidents:

PROPOSITION (6.1). *Soit $h\colon A\to B$ un homomorphisme d'anneaux. Quel que soit $d\geqslant 1$,*

$$u(d;B)\leqslant u(d;A).$$

PROPOSITION (6.2). *Soient K un corps, et $m\geqslant 1$ un entier, d désignant toujours un exposant $\geqslant 1$. Les deux assertions suivantes sont équivalentes:*

(a) $u(d;K)\leqslant m$ $(<\infty)$;

(b) *la forme diagonale à $m+1$ variables*

$$X_0^d+X_1^d+\ldots+X_m^d$$

admet sur K un zéro non trivial (autrement dit, est isotrope).

L'énoncé (6.2) reste vrai pour un anneau de valuation mais est faux pour un anneau quelconque (voir (6.8) et (6.3)).

Soit maintenant A un anneau intègre, de corps des fractions K, et soit d un entier $\geqslant 1$. Il est clair que $u(d;K)\leqslant u(d;A)$; en particulier, si $u(d;A)<\infty$, alors $u(d;K)<\infty$. Mais la réciproque est fausse:

EXEMPLE (6.3). Soit A l'anneau intègre

$$\boldsymbol{R}[X,Y]/(X^2+Y^2)=\boldsymbol{R}[x,y].$$

Son corps des fractions K est $\boldsymbol{R}(x,y)$ avec $x^2+y^2=0$; donc $K=\boldsymbol{C}(x)$. Prenons pour exposant $d=2$. Alors, dans K, $i^2=-1$, donc

$$u(2;K)=1.$$

Mais en revanche

$$u(2;A)=\infty.$$

En effet, si l'on avait $u(2;A)=m<\infty$, il existerait, dans $\boldsymbol{R}[X,Y]$, $m+1$ polynômes $P_1,P_2,\ldots,P_m$ et Q tels que

$$-1=P_1^2+P_2^2+\ldots+P_m^2+(X^2+Y^2)Q;$$

mais on déduirait de là, en faisant $X=Y=0$ et en posant $x_i=P_i(0,0)$, $-1=x_1^2+x_2^2+\ldots+x_m^2$, ce qui est absurde, puisque $u(2;\boldsymbol{R})=\infty$.

Notons que A nous fournit l'exemple d'un *anneau* où la forme $X_0^2+X_1^2$ est isotrope (elle admet le zéro $X_0=x$, $X_1=y$) et où cependant $u(2;A)=\infty$.

Malgré cela, il est possible dans certains cas particuliers, de déduire la finitude de $u(d;A)$ de celle de $u(d;K)$.

PROPOSITION (6.4). *Soient k un corps, et $\boldsymbol{X}=(X_a)$ une famille quelconque d'indéterminées. Posons*

$$A=k[\boldsymbol{X}], \quad K=k(\boldsymbol{X}).$$

Les trois assertions suivantes sont alors équivalentes:

(a) $u(d;K)<\infty$;

(b) $u(d;A)<\infty$;

(c) $u(d;k)<\infty$.

En fait, on a même, plus précisément,

$$u(d;K)=u(d;A)=u(d;k).$$

Démonstration. La double inclusion $k\subset A\subset K$ nous permet d'écrire immédiatement

$$u(d;K)\leqslant u(d;A)\leqslant u(d;k).$$

La seule chose à prouver est donc l'inégalité

$$u(d;k)\leqslant u(d;K),$$

et il suffit naturellement de la faire lorsque $u(d;K)<\infty$. Notons en outre qu'on peut supposer la famille $\boldsymbol{X}$ finie, puis, par récurrence, se ramener au cas où elle est réduite à une seule indéterminée X.

Posons alors $u(d;K)=m$ $(<\infty)$; il existe dans $A=k[X]$ des polynômes $P_1,P_2,\ldots,P_m$ et Q, *non tous divisibles par X*, et tels que

$$(P_1/Q)^d+(P_2/Q)^d+\ldots+(P_m/Q)^d=-1.$$

Cela s'écrit encore

$$Q^d+P_1^d+P_2^d+\ldots+P_m^d=0,$$

et prouve que, sur le corps k, la forme diagonale $X_0^d+X_1^d+\ldots+X_m^d$ admet le zéro non trivial

$$\big(Q(0),P_1(0),\ldots,P_m(0)\big);$$

d'où, d'après (6.2), $u(d;k)\leqslant m=u(d;K)$, C.Q.F.D.

PROPOSITION (6.5). *Soient A un anneau intègre, K son corps des fractions et d un entier $\geqslant 1$. Si le groupe additif K/A est un groupe de torsion, les deux assertions suivantes sont équivalentes:*

(a) $u(d;K)<\infty$;

(b) $u(d;A)<\infty$.

Démonstration. Il s'agit de prouver que (a) implique (b). Par hypothèse, il existe $x_1, x_2, \ldots, x_m \in K$ tels que

$$(*) \qquad -1 = x_1^d + x_2^d + \ldots + x_m^d.$$

Comme K/A est de torsion, il existe également un entier $h > 0$ tel que $hx_i \in A$ pour $i = 1, 2, \ldots, m$. Posons $hx_i = a_i$ et multiplions les deux membres de l'égalité $(*)$ par h^d:

$$-h^d = a_1^d + a_2^d + \ldots + a_m^d,$$

ou encore

$$-1 = a_1^d + a_2^d + \ldots + a_m^d + \underbrace{1^d + 1^d + \ldots + 1^d}_{(h^d - 1 \text{ fois})},$$

d'où $u(d; A) \leqslant m + h^d - 1 < \infty$.

Corollaire (6.6). *Soit A un ordre d'entiers algébriques, de corps des fractions K, et soit d un entier $\geqslant 1$. Si -1 est somme de puissances d-ièmes dans K, -1 est également somme de puissances d-ièmes dans A.*

Démonstration. Compte tenu de (6.5), il s'agit de prouver que K/A est de torsion: mais par hypothèse, A est un $\boldsymbol{Z}$-module libre de rang $n = [K: \boldsymbol{Q}]$; soit (e_i) une base, à la fois de A sur $\boldsymbol{Z}$ et de K sur $\boldsymbol{Q}$; la donnée de (e_i) identifie K (en tant que groupe additif) à $\boldsymbol{Q}^n$, et identifie de même A au sous-groupe $\boldsymbol{Z}^n$ de $\boldsymbol{Q}^n$; K/A s'identifie alors à $(\boldsymbol{Q}/\boldsymbol{Z})^n$, qui est un groupe de torsion.

Remarque (6.7). La proposition (6.5) s'applique également au cas d'un *anneau de valuation discrète d'inégales caractéristiques* 0 *et* $p > 0$: car si $x \in K$ n'est pas dans A, il a une valuation négative $-n$ $(n > 0)$, et si p est de valuation e, on a

$$v(p^n x) = ne - n \geqslant 0,$$

d'où $p^n x \in A$; K/A est un groupe de torsion. Mais en fait, on a un résultat valable pour tous les anneaux de valuation:

Proposition (6.8). *Soient A un anneau de valuation, K son corps des fractions, et d un entier $\geqslant 1$. On a alors l'égalité:*

$$u(d; A) = u(d; K).$$

Démonstration. Il est clair que $u(d; K) \leqslant u(d; A)$, et que si $u(d; K) = \infty$, $u(d; A) = \infty$. Il suffit donc de prouver ceci: si $u(d; K) = m < \infty$, alors $u(d; A) \leqslant m$. Mais l'hypothèse $u(d; K) = m$ implique (voir (6.2)) que la forme diagonale

$$X_0^d + X_1^d + \ldots + X_m^d$$

admet sur K un zéro non trivial, zéro que l'on peut toujours supposer *primitif*: autrement dit, il existe $x_0, x_1, \ldots, x_m \in A$ tels que

$$x_0^d + x_1^d + \ldots + x_m^d = 0$$

et que l'un des x_i (disons x_0) soit *inversible*: mais alors

$$(x_0^{-1}x_1)^d + (x_0^{-1}x_2)^d + \ldots + (x_0^{-1}x_m)^d = -1;$$

et comme les $x_0^{-1}x_i \in A$, on a bien $u(d; A) \leqslant m$.

2. Résultats relatifs au cas d'un corps K et de l'exposant $d = 2$. Ce paragraphe ne fait que rappeler, sans démonstration, quelques résultats connus, pour lesquels on donne des références.

Soient K un corps quelconque et p sa caractéristique. Supposons d'abord $p > 0$; alors, $-1 = 1^2 + 1^2 + \ldots + 1^2$ ($p-1$ fois), donc $u(2; K) \leqslant p - 1$. On a même mieux: car -1 appartient au corps premier $\boldsymbol{F}_p$, et dans ce corps, tout élément est somme de deux carrés: c'est là une propriété bien connue, qui résulte par exemple de la proposition (7.16) que nous démontrerons au chapitre suivant, ou encore du théorème de Chevalley (voir [7]). On peut d'ailleurs l'établir directement de la façon suivante:

posons $k = \boldsymbol{F}_p$, et considérons k^{*2}, sous-groupe de k^*; si $-1 \in k^{*2}$, il n'y a rien à démontrer; supposons donc $-1 \notin k^{*2}$. On a alors $k^{*2} \neq k^*$, et k^{*2} est d'indice 2 dans k^*, car k^* est cyclique, et le quotient k^*/k^{*2} est un groupe cyclique non trivial d'exposant 2. Considérons maintenant l'ensemble G des éléments de k^* de la forme $x^2 + y^2$ $(x, y \in k)$. C'est un sous-groupe de k^* (utiliser l'identité de Lagrange), et, du fait que

$$k^{*2} \subset G \subset k^*$$

et que $(k^*: k^{*2}) = 2$, on a, soit $G = k^*$, soit $G = k^{*2}$. Mais la deuxième égalité est impossible, car elle entraînerait par récurrence que tout élément de k^*, et en particulier -1, est un carré, ce qui est exclu par hypothèse. Donc, $G = k^*$, et $-1 \in G$, ce qui signifie précisément que -1 est somme de deux carrés.

Finalement, si $p > 0$, $u(2; K) \leqslant 2$.

Supposons maintenant la caractéristique p quelconque (nulle ou non). D'après la théorie d'Artin, les deux assertions suivantes sont équivalentes;

(a) $u(2; K) = \infty$;

(b) le corps K est *ordonnable*.

Si K n'est pas ordonnable (donc si $u(2; K) < \infty$), les valeurs possibles de $u(2; K)$ ne sont pas quelconques. En effet:

THÉORÈME (6.9) (Cassels–Pfister; voir par exemple [6]). *Si K est un corps non-ordonnable, le nombre $u(2;K)$ est une puissance de 2. Et toute puissance de 2 est un $u(2;K)$ pour K convenablement choisi.*

Le fait que $u(2;K)$ est une puissance de 2 est prouvé dans [6] à partir du résultat suivant:

LEMME (6.10) (Pfister). *Soient K un corps et 2^m $(m \geqslant 0)$ une puissance de 2. Alors, l'ensemble $G(2^m)$ des éléments non nuls de K qui sont sommes de 2^m carrés (au plus) est un groupe multiplicatif.*

(Ce lemme généralise ce que l'on savait depuis longtemps pour $m = 1, 2, 3$: les identités de Lagrange, Hamilton et Cayley prouvent en effet respectivement que $G(2), G(4)$ et $G(8)$ sont des groupes; voir d'ailleurs la démonstration donnée à l'instant du fait que $u(2;F_p) \leqslant 2$.)

Rappelons comment on déduit de (6.10) la première assertion de (6.9): supposons que $u(2;K)$ ne soit pas une puissance de 2; il existerait alors un exposant m tel que

$$2^m < u(2;K) < 2^{m+1},$$

d'où $u(2;K) = 2^m+q$ $(1 \leqslant q \leqslant 2^m-1)$. On pourrait écrire $-1 = a+b$, avec a, somme de 2^m carrés (et pas moins), b, somme de q carrés (et pas moins), et on aurait, puisque visiblement $a \neq 0$, $-1 = (b+1)/a$. Mais comme $a \in G(2^m)$, et $b+1 \in G(2^m)$ (puisque $q+1 \leqslant 2^m$), on aurait, compte tenu de (6.10), $-1 \in G(2^m)$, donc $u(2;K) \leqslant 2^m$, ce qui contredit $2^m < u(2;K)$.

Le fait que toute puissance de 2 est un $u(2;K)$ tient par exemple au résultat suivant (Cassels, [6]):

LEMME (6.11). *Soient $m \geqslant 0$ un entier, $n = 2^m$, A l'anneau intègre*

$$\boldsymbol{R}[X_1, X_2, \ldots, X_n, Y]/(X_1^2+X_2^2+\ldots+X_n^2+Y^2)$$

et K le corps des fractions de A. On a alors l'égalité

$$u(2;K) = n = 2^m.$$

Naturellement, d'après ce qu'on a dit plus haut, les valeurs $u(2;K) = 4, 8, 16, \ldots$ ne peuvent se produire de toute façon qu'en caractéristique 0. Par exemple, si K est le corps des rationnels 2-adiques, $u(2;K) = 4$.

REMARQUE (6.12). Le lemme (6.10) peut être précisé par l'énoncé suivant: soit K un corps *non-ordonnable*, et posons $u(2;K) = 2^m$.

Alors

(i) La suite:

$$G(1) \subset G(2) \subset \ldots \subset G(2^{m-1}) \subset G(2^m)$$

est strictement croissante.

(ii) En revanche, on a

$$G(2^{m+1}) = G(2^{m+2}) = \ldots = G(2^{m+k}) = \ldots = K_2^+ \setminus \{0\}.$$

(iii) Enfin les deux circonstances

$$G(2^m) = G(2^{m+1}) \quad \text{et} \quad G(2^m) \neq G(2^{m+1})$$

sont possibles.

Prouvons (i). Ecrivons $-1 = u_1^2+u_2^2+\ldots+u_{2^m}^2$. Si la suite $G(2^j)$ $(0 \leqslant j \leqslant m)$ n'était pas strictement croissante, il existerait un indice i $(0 \leqslant i \leqslant m-1)$ tel que

$$(*) \qquad G(2^i) = G(2^{i+1}).$$

Or, $u_1^2+u_2^2+\ldots+u_{2^{i+1}}^2 \in G(2^{i+1})$; car le premier membre est somme de 2^{i+1} puissances d-ièmes, et n'est pas nul (s'il l'était, on aurait $-1 = u_{2^{i+1}+1}^2+\ldots+u_{2^m}^2$, donc $u(2;K) < 2^m$: contradiction). Mais l'égalité $(*)$ impliquerait alors l'existence de $v_1, v_2, \ldots, v_{2^i}$ tels que

$$u_1^2+u_2^2+\ldots+u_{2^{i+1}}^2 = v_1^2+v_2^2+\ldots+v_{2^i}^2,$$

et par conséquent

$$-1 = v_1^2+\ldots+v_{2^i}^2+u_{2^{i+1}+1}^2+\ldots+u_{2^m}^2;$$

d'où $u(2;K) \leqslant 2^m-2^i < 2^m$: contradiction; l'égalité $(*)$ est impossible, et (i) est démontré.

Démontrons (ii). Il s'agit en fait de prouver que $w(2;K) \leqslant 2^{m+1}$ (pour la définition de $w(2;K)$, voir l'introduction). Mais si K est de caractéristique 2, on a évidemment $u(2;K) = 1$, $m = 0$, et $w(2;K) = 1 < 2 = 2^{m+1}$. Si au contraire K est de caractéristique $\neq 2$, on a pour tout $x \in K$,

$$x = \left(\frac{x+1}{2}\right)^2 + (-1)\left(\frac{x-1}{2}\right)^2,$$

donc $w(2;K) \leqslant 1+u(2;K) = 1+2^m \leqslant 2^{m+1}$.

Prouvons (iii). L'égalité $G(2^m) = G(2^{m+1})$ est réalisée lorsque K est algébriquement clos, ou encore lorsque K est de caractéristique 2. L'inégalité $G(2^m) \neq G(2^{m+1})$ est réalisée par exemple pour $K = \boldsymbol{Q}(i)$: dans ce cas en effet, $u(2;K) = 1$ puisque $i^2 = -1$; mais $G(1) \neq G(2)$, car il existe des éléments de K qui ne sont pas des carrés.

3. Etude de $u(d;K)$ pour un corps de nombres algébriques K.

THÉORÈME (6.13). *Soient A un ordre d'entiers algébriques et K le corps des fractions de A. Les cinq assertions suivantes sont équivalentes:*

(a) *-1 est somme de carrés dans K;*

(a′) *-1 est somme de carrés dans A;*

(b) *quel que soit* $d \geqslant 1$, -1 *est somme de puissances* d*-ièmes dans* K;

(b') *quel que soit* $d \geqslant 1$, -1 *est somme de puissances* d*-ièmes dans* A;

(c) *le corps* K *est totalement imaginaire.*

Démonstration. L'équivalence entre (a) et (a'), ainsi que celle entre (b) et (b'), résultent du corollaire (6.6). Il est clair en outre que (b) implique (a) et que (a) implique (c). Reste à prouver que (c) implique (b); les données sont les suivantes: un corps K totalement imaginaire; un entier naturel $d \geqslant 1$.

Soit $2n = [K: \boldsymbol{Q}]$ le degré de K sur le corps $\boldsymbol{Q}$ des nombres rationnels, et soient $s_1, s_2, \ldots, s_{2n}$ les $2n$ $\boldsymbol{Q}$-isomorphismes de K dans sa clôture algébrique, l'indexation étant choisie telle que s_1 soit l'application identique, et que de plus

$$s_{n+h}x = \overline{s_h x} \quad \text{(complexe conjugué de } s_h x) \tag{1}$$

pour tout $x \in K$ et tout entier h entre 1 et n. Nous aurons besoin du résultat auxiliaire suivant:

Lemme (6.14). *Il existe* $z \in K$ *tel que les* $2n$ *éléments*

$$(s_j z)^d = s_j(z^d) \qquad (1 \leqslant j \leqslant 2n)$$

aient tous une partie réelle strictement négative.

Démonstration du lemme. Notons v la valeur absolue usuelle: $v(x) = |x|$; les n applications $v_j = v \circ s_j$ $(1 \leqslant j \leqslant n)$ sont alors n valeurs absolues independantes sur le corps K. Soit d'autre part $\varepsilon > 0$ un nombre réel. Puisque K est totalement imaginaire, chacun des corps $s_j K$ est dense dans le corps des nombres complexes, et nous pouvons, pour tout j entre 1 et n, trouver $a_j \in s_j K$ tel que

$$v(a_j - e^{i\pi/d}) < \varepsilon. \tag{2}$$

Maintenant, par le *Théorème d'Approximation*, nous pouvons également trouver $z \in K$ tel que, pour tout j entre 1 et n, $v_j(z - s_j^{-1} a_j) < \varepsilon$, c'est-à-dire, par définition même de v_j,

$$v(s_j z - a_j) < \varepsilon. \tag{3}$$

En rapprochant (2) et (3), nous obtenons donc

$$v(s_j z - e^{i\pi/d}) < 2\varepsilon,$$

c'est-à-dire

$$|s_j z - e^{i\pi/d}| < 2\varepsilon, \tag{4}$$

pour tout j entre 1 et n, et aussi, compte tenu de (1),

$$|s_j z - e^{-i\pi/d}| < 2\varepsilon, \tag{5}$$

pour tout j entre $n+1$ et $2n$. Comme $(e^{i\pi/d})^d = (e^{-i\pi/d})^d = -1$, il résulte de (4) et (5) qu'en choisissant ε assez petit, nous aurons

$$|(s_j z)^d + 1| < 1$$

pour tout j; en particulier, les $2n$ éléments $(s_j z)^d$ auront bien leur partie réelle strictement négative.

Ce lemme étant prouvé, achevons la démonstration du théorème; z gardant la même signification que ci-dessus, considérons le polynôme

$$F(X) = \prod_{1 \leqslant j \leqslant 2n} \left(X - (s_j z)^d\right),$$

et soit

$$F(X) = X^{2n} + c_1 X^{2n-1} + \ldots + c_{2n-1} X + c_{2n}$$

sa forme réduite. Ses coefficients c_j sont évidemment tous *rationnels*; de plus, ils sont tous *positifs ou nuls*: en effet, nous pouvons écrire

$$F(X) = \prod_{1 \leqslant h \leqslant n} F_h(X), \tag{6}$$

en posant $F_h(X) = \left((X - s_h z)^d\right)\left(X - (s_{n+h} z)^d\right)$, ou encore, compte tenu de (3),

$$F_h(X) = \left((X - s_h z)^d\right)\left(X - (\overline{s_h z})^d\right).$$

Mais $F_h(X)$ est un trinôme unitaire dont les deux racines sont complexes conjuguées de partie réelle *négative*: ses coefficients sont donc réels *positifs*, et il en est de même de ceux de $F(X)$, d'après (6). Notons enfin que le terme constant c_{2n} est *non nul*, car les racines de $F(X)$ sont toutes distinctes de 0. En résumé:

pour tout j entre 1 et $2n$, $c_j \in \boldsymbol{Q}$, $c_j \geqslant 0$; de plus, $c_{2n} \neq 0$.

Soit alors $b > 0$ un entier naturel tel que, pour tout j entre 1 et $2n$, $bc_j = m_j$ soit lui-même un entier $(\geqslant 0)$. Ecrivons que $z^d = (s_1 z)^d$ annule $F(X)$ et multiplions par b les deux membres de l'égalité ainsi obtenue:

$$b(z^d)^{2n} + m_1 (z^d)^{2n-1} + \ldots + m_{2n-1} z^d + m_{2n} = 0; \tag{7}$$

comme $m_{2n} > 0$, $m_{2n} - 1 \geqslant 0$; (7) peut alors s'écrire

$$-1 = b(z^{2n})^d + m_1 (z^{2n-1})^d + \ldots + (m_{2n} - 1)$$

et ceci prouve bien que -1 est somme de puissances d-ièmes dans K (en fait, somme d'au plus $b + m_1 + \ldots + m_{2n} - 1$ puissances d-ièmes).

4. Etude de $u(d; K)$ **pour un corps** K **quelconque de caractéristique** 0.

L'objet de ce paragraphe est de généraliser à un corps K quelconque de caractéristique 0 l'équivalence (a) $\Leftrightarrow$ (b) du théorème (6.13).

THÉORÈME (6.15). *Soit K un corps de caractéristique 0. Les deux assertions suivantes sont équivalentes:*

(a) *-1 est somme de carrés dans K (autrement dit, K est non-ordonnable);*

(b) *quel que soit $d \geqslant 1$, -1 est somme de puissances d-ièmes dans K.*

Démonstration. Il s'agit en fait de prouver (a) $\Rightarrow$ (b). Supposons donc $u(2;K) < \infty$; comme la caractéristique est 0, on peut écrire, pour tout $x \in K$,

$$x = \left(\frac{x+1}{2}\right)^2 + (-1)\left(\frac{x-1}{2}\right)^2.$$

D'où

$$(*) \qquad K = K_2 \quad \text{et} \quad w(2;K) \leqslant 1 + u(2;K) < \infty.$$

Démontrons alors (b) par récurrence sur le degré. En degré 2, rien à démontrer. Supposons la propriété établie jusqu'à un certain degré $D-1 \geqslant 2$, et prouvons-la pour le degré D. Distinguons deux cas:

1° *D impair*: alors, $-1 = (-1)^D$ et $u(D;K) = 1$.

2° *D pair*: on peut alors écrire $D = 2d$ avec $d < D-1$.

Par hypothèse de récurrence,

$$q = u(d;K) < \infty,$$

d'où une décomposition

$$-1 = y_1^d + y_2^d + \ldots + y_q^d \quad (\text{les } y_j \in K).$$

Posons $m = 1 + u(2;K)$. D'après (*), on peut, pour tout j de 1 à q, écrire une décomposition

$$y_j = x_{j,1}^2 + x_{j,2}^2 + \ldots + x_{j,m}^2.$$

Pour chaque j, faisons (dans l'identité du théorème (8.1): voir l'appendice) $X_1 = x_{j,1}, \ldots, X_m = x_{j,m}$, puis additionnons les q égalités ainsi obtenues:

$$q\left(\sum_j y_j^d\right) = \sum_j \sum_h q_h (c_{1,h}x_{j,1} + \ldots + c_{m,h}x_{j,m})^D,$$

ou encore

$$-1 = \sum_j \sum_h q_h (c_{1,h}x_{j,1} + \ldots + c_{m,h}x_{j,m})^D + q - 1;$$

comme $q-1$ et les q_h sont des entiers $\geqslant 0$, ils peuvent s'écrire $1^D + 1^D + \ldots + 1^D$; et l'égalité ci-dessus prouve que $-1 \in K_D^{\dagger}$, c'est-à-dire que $u(D;K) < \infty$, C.Q.F.D.

On peut d'ailleurs ajouter une précision au théorème (6.15):

THÉORÈME (6.16). *Soient u et d deux variables entières $\geqslant 1$. Il existe une fonction $U(u,d)$, à valeurs entières $\geqslant 1$ et possédant la propriété suivante:*

quel que soit K, corps de caractéristique 0 non-ordonnable, on a

$$u(d;K) \leqslant U\big(u(2;K), d\big)$$

pour toute valeur de l'exposant d.

Démonstration. Toujours par récurrence sur le degré. Notons d'abord que l'on peut poser

$$U(u,d) = 1 \quad \text{pour } d \text{ impair};$$

$$U(u,d) = u \quad \text{pour } d = 2.$$

Supposons l'existence de $U(u,d)$ établie pour tout degré $\leqslant D-1$ ($D-1 \geqslant 2$), et prouvons-la pour le degré D. D'après ce qu'on vient de dire, on peut supposer D pair, $D = 2d$ (et alors $d < D-1$). Comme dans (6.15), posons

$$m = u(2;K) + 1;$$

alors d et m ne dépendent que de D et $u(2;K)$. Maintenant, parmi les identités du type (8.1) avec d et m ainsi fixés, écrivons-en une donnant au nombre

$$m(q_1 + q_2 + \ldots + q_{2d+1}) + q - 1$$

la plus petite valeur possible. Cette valeur minima ne dépend que de d et m, donc, en fait, de D et $u(2;K)$: notons-la $U\big(u(2;K), D\big)$. Avec les calculs faits pour prouver (6.15), nous obtenons alors une égalité du type

$$-1 = \sum_{j=1}^{m} \sum_{h=1}^{2d+1} q_h [L_h(x_j)]^D + q - 1$$

qui implique

$$u(D;K) \leqslant m(q_1 + q_2 + \ldots + q_{2d+1}) + q - 1,$$

soit, finalement,

$$u(D;K) \leqslant U\big(u(2;K), D\big).$$

(Notons qu'en fait, pour D pair, nous n'avons défini $U(u,D)$ que lorsque la variable u est un nombre de la forme $u(2;K)$, c'est-à-dire une puissance de 2 (voir (6.9).) Naturellement, si u n'est pas une puissance de 2, on peut poser, par exemple, $U(u,D) = 1$).

REMARQUE (6.17). Dans la majoration

$$u(d;K) \leqslant U\big(u(2;K), d\big),$$

on ne peut supprimer, dans le second membre, ni la dépendance par rapport à d, ni la dépendance par rapport à $u(2;K)$; en effet, si $K=\boldsymbol{Q}_2$, corps des rationnels 2-adiques, et si $d=2^m$ $(m\geqslant 2)$, on a $u(2;K)=4$, et $u(d;K)\geqslant 4d-1$; l'indépendance de U par rapport à d donnerait alors, pour tout $m\geqslant 2$, $4\cdot 2^m\leqslant U(4)+1$; absurde. D'autre part, nous avons vu (théorème (6.9)) qu'il existe pour tout $m\geqslant 0$ un corps $K_{(m)}$ de caractéristique 0 tel que $u(2;K_{(m)})=2^m$; l'indépendance de U par rapport à u donnerait alors, pour tout $m\geqslant 0$, $2^m\leqslant U(2)$; absurde.

Remarque (6.18). Pour tout corps K de caractéristique $p>0$, on a évidemment $u(d;K)<\infty$ quel que soit d; on a même, puisque $\boldsymbol{F}_p\subset K$, $u(d;K)\leqslant d$: on verra en effet au chapitre 7 (proposition (7.16)) que si k est un corps fini, $u(d;k)\leqslant d$.

Ainsi, les théorèmes (6.15) et (6.16) sont en réalité valables sans hypothèse sur la caractéristique (et donc avec la seule hypothèse: *K non-ordonnable*).

5. Etude de $u(d;A)$ pour un anneau local hensélien A.

Théorème (6.19). *Soient A un anneau local hensélien, k le corps résiduel de A et d un entier $\geqslant 1$. Les deux conditions suivantes sont équivalentes:*

(a) *-1 est somme de puissances d-ièmes dans k;*

(b) *-1 est somme de puissances d-ièmes dans A.*

Démonstration. Le fait que (b) implique (a) est un cas particulier de la proposition (6.1). Montrons la réciproque; distinguons trois cas:

1er cas: l'anneau A est de torsion. Il existe alors un nombre premier p et un exposant s tels que l'on ait $p^s\cdot 1=0$ dans A, et $p\cdot 1=0$ dans k. Mais ceci peut s'écrire

$$-1=1^d+1^d+\ldots+1^d \quad (p^s-1 \text{ fois})$$

dans l'anneau A, et

$$-1=1^d+1^d+\ldots+1^d \quad (p-1 \text{ fois})$$

dans le corps k: il n'y a donc en fait rien à démontrer dans ce cas.

2e cas: k est de caractéristique 0. Dans ce cas, d n'est pas divisible par la caractéristique $p=0$ de k, et l'implication à prouver résulte de l'égalité $u(d;A)=u(d;k)$ démontrée au chapitre 2 (remarque (2.16) suivant le lemme (2.14)).

3e cas: l'anneau A est sans torsion, mais le corps k est de caractéristique $p>0$. Si p ne divise pas d, le raisonnement du cas précédent s'applique encore. Sinon, voici comment on peut procéder:

dans le corps k, -1 est toujours somme de puissances d-ièmes, par la sempiternelle égalité

$$-1=1^d+1^d+\ldots+1^d \quad (p-1 \text{ fois}).$$

Il s'agit donc de prouver que, dans A aussi, -1 est toujours somme de puissances d-ièmes. Mais soit $\boldsymbol{Z}_{(p)}$ le localisé en (p) de l'anneau $\boldsymbol{Z}$ des entiers rationnels, et soit B le hensélisé de l'anneau local $\boldsymbol{Z}_{(p)}$; l'homomorphisme canonique $\boldsymbol{Z}\to A$ se prolonge en un homomorphisme $B\to A$, et la proposition (6.1) nous permet d'écrire $u(d;A)\leqslant u(d;B)$. Il suffit donc de montrer que $u(d;B)<\infty$, ou, plus généralement, que $u(d;A)<\infty$ lorsque A est un anneau local hensélien *intègre, sans torsion*, et à corps résiduel k de caractéristique $p>0$. L'idée est alors d'utiliser le théorème (6.13) en faisant intervenir une sorte de polynôme d'Artin–Schreier.

De façon précise, soient $\mathfrak{m}$ l'idéal maximal de A, K le corps des fractions de A (supposé intègre, rappelons-le), et désignons par $P(X)$ le polynôme X^p-X+p (considéré comme élément de $A[X]$). Modulo $\mathfrak{m}$, il se réduit à $P(X)=X^p-X$, qui admet (dans k) p racines distinctes: les éléments du corps premier. Comme A est hensélien, $P(X)$ admet donc (dans A) p racines distinctes $a_1, a_2, \ldots, a_p$; et comme $P(X)$ est unitaire, $a_1, a_2, \ldots, a_p$ sont entiers sur $\boldsymbol{Z}$. Ainsi, A contient $\boldsymbol{Z}[a_1, a_2, \ldots, a_p]$, ordre d'entiers algébriques, $a_1, a_2, \ldots, a_p$ étant les racines dans K, corps de caractéristique 0, du polynôme unitaire $P(X)$. Je dis que -1 est somme de puissances d-ièmes dans $\boldsymbol{Z}[a_1, a_2, \ldots, a_p]$ (donc a fortiori dans A, ce qu'il faut démontrer): en effet, le corps des fractions de cet ordre d'entiers n'est autre que $L=\boldsymbol{Q}(a_1, a_2, \ldots, a_p)$; c'est le corps de toutes les racines de $P(X)$; pour prouver notre assertion, il suffit de montrer que L est totalement imaginaire (voir (6.13)) et même, l'extension $L/\boldsymbol{Q}$ étant galoisienne, que $P(X)$ admet toujours une racine non-réelle. Or, pour $p=2$ et 3, c'est immédiat; et pour $p\geqslant 5$, cela tient à ce que $P(X)$ a au maximum trois racines réelles, comme on le voit en étudiant les variations de la fonction $P(x)$ à l'aide de la dérivée $P'(x)=px^{p-1}-1$ qui ne s'annule que deux fois.

Chapitre 7

PROBLÈME DE WARING GÉNÉRALISÉ

1. Généralités relatives à $v(d;A)$ et $w(d;A)$. Pour la définition des notations $v(d;A)$ et $w(d;A)$, nous renvoyons à l'introduction. Nous allons commencer par indiquer, le plus souvent sans démonstration, quelques propriétés et remarques très simples qui serviront de lemmes pour des théorèmes ultérieurs.

Proposition (7.1). *Soient A un anneau, d un entier $\geqslant 1$. Si $u(d;A)<\infty$, on a les trois inégalités*

$$u(d;A)\leqslant w(d;A);$$
$$v(d;A)\leqslant w(d;A);$$
$$w(d;A)\leqslant u(d;A)\cdot v(d;A).$$

En particulier, si d est impair:

$$v(d; A) = w(d; A).$$

En revanche, si $u(d; A) = \infty$, il semble difficile de comparer $v(d; A)$ et $w(d; A)$. En effet, pour tout x dans A_d (resp. $A_d^\dagger$), soit $\lambda(x)$ (resp. $\lambda_+(x)$) le plus petit entier m tel que x s'exprime à l'aide (resp. soit somme) de m puissances d-ièmes. On a évidemment de façon générale

$$v(d; A) = \sup_{x \in A_d} \lambda(x); \qquad w(d; A) = \sup_{x \in A_d^\dagger} \lambda_+(x);$$

et, si $x \in A_d^\dagger$, $\lambda(x) \leqslant \lambda_+(x)$; d'où l'inégalité $v(d; A) \leqslant w(d; A)$ si $u(d; A) < \infty$ (ce qui équivaut à $A_d = A_d^\dagger$). Au contraire, si $u(d; A) = \infty$, on a $A_d^\dagger \subset A_d$, mais $A_d^\dagger \neq A_d$: la fonction $\lambda(x)$, qui est numériquement plus petite que $\lambda_+(x)$, est donc définie sur un ensemble strictement plus grand, ce qui interdit a priori toute comparaison des bornes supérieures $v(d; A)$ et $w(d; A)$.

PROPOSITION (7.2). *Soit $h : A \to B$ un homomorphisme d'anneaux, que nous supposerons surjectif. Soit $\mathfrak{a}$ le noyau de h, et soit par ailleurs d un entier $\geqslant 1$. Alors*

(i) $h(A_d) = B_d$, $h(A_d^\dagger) = B_d^\dagger$ (voir (1.1));

(ii) $v(d; B) \leqslant v(d; A)$ *et* $w(d; B) \leqslant w(d; A)$;

(iii) *en outre, si tout élément de l'idéal $\mathfrak{a}$ s'exprime à l'aide de s puissances d-ièmes d'éléments de A, on a aussi*

$$v(d; A) \leqslant w(d; B) + s;$$

de même, si tout élément de l'idéal $\mathfrak{a}$ est somme de s puissances d-ièmes d'éléments de A, on a

$$w(d; A) \leqslant w(d; B) + s.$$

COROLLAIRE (7.3). *Soient A un anneau, d un entier $\geqslant 1$ et B l'anneau quotient $A/d!A$. On a alors l'inégalité*:

$$v(d; A) \leqslant v(d; B) + 2^d; \tag{7.3.1}$$

si d est impair, ou si 2 est inversible dans A, on a même, plus précisément:

$$v(d; A) \leqslant v(d; B) + 2^{d-1}. \tag{7.3.2}$$

Démonstration. L'identité (8.2.2) (appendice) montre en effet que tout élément de l'idéal $d!A$ s'exprime à l'aide de

$$2\sum_h \binom{d-1}{h} = 2 \cdot 2^{d-1} = 2^d$$

puissances d-ièmes: (7.3.1) résulte alors de (7.2), (iii). Même méthode pour prouver (7.3.2), en utilisant maintenant l'identité (8.2.1).

PROPOSITION (7.4). *Soient $A_1, A_2, \ldots, A_n$ des anneaux en nombre fini, B l'anneau produit $\prod A_i$, et d un entier $\geqslant 1$. Alors*

$$w(d; B) = \sup_i w(d; A_i); \tag{7.4.1}$$

$$\sup_i v(d; A_i) \leqslant v(d; B) \leqslant 2 \sup_i v(d; A_i). \tag{7.4.2}$$

REMARQUE (7.5). On peut avoir effectivement

$$v(d; B) > \sup_i v(d; A_i).$$

EXEMPLE. $B = \boldsymbol{R} \times \boldsymbol{R}$ et $d = 2$. On a $v(2; \boldsymbol{R}) = 1$, car tout nombre réel s'écrit $\pm x^2$. Ici donc

$$\sup_i v(d; A_i) = 1.$$

Mais dans $\boldsymbol{R} \times \boldsymbol{R}$, considérons un élément de la forme (a, b), avec $ab < 0$: ce n'est ni un carré, ni l'opposé d'un carré, car on aurait alors $ab \geqslant 0$; donc $v(2; B) > 1$, et en fait $v(2; B) = 2 = 2 \sup_i v(d; A_i)$.

PROPOSITION (7.6). *Soient A un anneau, S une partie multiplicative de A et d un entier $\geqslant 1$. On a les inégalités*

$$v(d; S^{-1}A) \leqslant v(d; A);$$

$$w(d; S^{-1}A) \leqslant w(d; A).$$

En particulier, la localisation ne peut que diminuer v et w.

2. Le problème de Waring généralisé. Nous appelons problème de Waring généralisé le type de problème suivant:

> un entier $d \geqslant 1$ et une classe d'anneaux $\mathscr{A}$ étant donnés, le nombre $v(d; A)$ reste-t-il borné quand A décrit $\mathscr{A}$ (et dans l'affirmative, quelle majoration de $v(d; A)$, indépendante de $A \in \mathscr{A}$, peut-on trouver) ? ou bien, existe-t-il un $A \in \mathscr{A}$ tel que $v(d; A) = \infty$? mêmes questions pour $w(d; A)$.

Voici quelques exemples de résultats liés à ce type de problème:

EXEMPLE (7.7). Si K est un corps de nombres algébriques, il est bien connu que les sommes de carrés, dans K, sont les éléments totalement positifs de K, et que tout élément totalement positif de K est somme de 4 carrés; donc

$$w(2; K) \leqslant 4$$

lorsque K décrit la classe de tous les corps de nombres algébriques.

EXEMPLE (7.8). Ramanujam a démontré le résultat suivant (voir [23]): quel que soit l'anneau $\mathfrak{P}$-adique A, on a

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

Birch avait d'ailleurs prouvé par une autre méthode (voir [3]) l'inégalité $w(d; A) \leqslant d^{16d^2}$. Ici, la classe $\mathscr{A}$ est celle de tous les anneaux $\mathfrak{P}$-adiques.

Ajoutons comme troisième exemple un résultat fort simple, qui règle complètement le cas $d = 2$:

THÉORÈME (7.9). *Quel que soit l'anneau A,*

$$v(2; A) \leqslant 3.$$

De façon plus précise: quel que soit A, et quel que soit $a \in A_2$, il existe x et $y \in A$ tels que

$$a = x^2 + (y+1)^2 - y^2.$$

Démonstration. Puisque $a \in A_2$, il existe $m \geqslant 1$, $x_1, x_2, \ldots, x_m \in A$ et $e_1, e_2, \ldots, e_m = \pm 1$ tels que

$$a = e_1 x_1^2 + e_2 x_2^2 + \ldots + e_m x_m^2.$$

Posons $x = x_1 + x_2 + \ldots + x_m + 1$. Alors

$$a - x^2 = \sum_i (e_i - 1) x_i^2 - 2 \sum_{i<j} x_i x_j - 2 \sum_i x_i - 1.$$

Mais puisque $e_i = \pm 1$ pour tout i, on a $e_i - 1 = 0$ ou -2, de toute façon un coefficient *pair*; par ailleurs, $-1 = -2+1$. Grâce à ces remarques profondes, l'égalité ci-dessus devient, par mise en facteur du coefficient 2,

$$a - x^2 = 2y + 1 \qquad (y \in A).$$

Or, $2y+1 = (y+1)^2 - y^2$; le théorème est démontré.

Notons que la borne 3 est la meilleure possible; ainsi, dans l'anneau $\mathbf{Z}$, le nombre 6 ne peut s'exprimer à l'aide de deux carrés: car il n'est pas somme de deux carrés; et d'autre part, toute différence de deux carrés est, soit impaire, soit multiple de 4.

Dans (7.9), $\mathscr{A}$ est la classe de tous les anneaux. Si on se restreint à la classe de tous les corps, on a le résultat suivant, qui sera notre quatrième exemple:

EXEMPLE (7.10). Quel que soit le corps K,

$$v(2; K) \leqslant 2.$$

En effet, en caractéristique 2, $-1 = 1$, et toute somme de carrés est un carré; d'où, dans ce cas, $v(2; K) = 1$; et, en caractéristique $\neq 2$, on peut écrire, pour tout $x \in K$,

$$x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2$$

qui implique bien $v(2; K) \leqslant 2$.

Le résultat suivant, qui sera notre dernier exemple, concerne $w(d; A)$. Remarquons que, puisque, pour d impair, $w(d; A) = v(d; A)$, la constante w proprement dite n'existe que pour d pair. En ce sens, le résultat ci-dessous résout alors complètement le problème de Waring pour $w(d; A)$, lorsque A parcourt la classe de tous les anneaux:

THÉORÈME (7.11). *Soit d un entier pair $\geqslant 2$.*

(i) *Quel que soit N, il existe un anneau A tel que $N \leqslant w(d; A)$ (autrement dit, $w(d; A)$ n'est pas borné).*

(ii) *Il existe un anneau A tel que $w(d; A) = \infty$.*

Démonstration. (i) Pour tout $m \geqslant 0$, désignons par $K_{(m)}$ un corps tel que $u(2; K_{(m)}) = 2^m$ (voir (6.9)). D'après le théorème (6.15), on a $u(d; K_{(m)}) < \infty$, et plus précisément, puisque d est pair et que toute somme de puissances d-ièmes est donc une somme de carrés,

$$2^m = u(2; K_{(m)}) \leqslant u(d; K_{(m)}) < \infty.$$

Comme $w(d; K_{(m)}) \geqslant u(d; K_{(m)})$, et que 2^m peut être pris arbitrairement grand, (i) se trouve démontré.

(ii) Soit A l'anneau produit $\prod K_{(m)}$; je dis que $w(d; A) = \infty$. Supposons en effet le contraire: $w(d; A) = n < \infty$, et soit m_0 un entier tel que $2^{m_0} > n$. La proposition (7.2), appliquée à l'homomorphisme m_0-ième projection $A \to K_{(m_0)}$, conduirait à l'inégalité

$$w(d; K_{(m_0)}) \leqslant w(d; A) = n.$$

En particulier, on aurait

$$2^{m_0} = u(d; K_{(m_0)}) \leqslant w(d; K_{(m_0)}) \leqslant n,$$

ce qui contredirait le choix de m_0.

Nous verrons au paragraphe 4 que le théorème (7.11) reste vrai si on se restreint à la classe des corps: en fait, il existe un corps K tel que, quel que soit d pair, $w(d; K) = \infty$.

Dans la suite de ce chapitre, nous allons étudier $v(d; A)$ et $w(d; A)$ lorsque A est un corps, ou bien lorsque A est une algèbre sur un corps infini (paragraphe 4): nous obtiendrons des résultats assez complets. Nous étudierons également $w(d; A)$ lorsque A est un anneau local hensélien et que d est premier (paragraphe 5). Quant au paragraphe 3, il contient des résultats relatifs à $v(d; K)$ et $w(d; K)$ lorsque K est un corps tel que l'indice $(K^* : K^{*d})$ soit fini.

Le principal problème, qui restera sans réponse, est le suivant:

$d \geqslant 3$ étant fixé, et A parcourant la classe de tous les anneaux, $v(d; A)$ reste-t-il borné?

Notons que si $v(d;A)$ n'est pas borné, il existe un anneau A tel que $v(d;A)=\infty$ (raisonner comme dans le théorème (7.11)). Et inversement, bien entendu.

Voici quelques résultats liés à ce problème, mais qui ne semblent pas devoir le faire avancer beaucoup.

PROPOSITION (7.12). *Soit d un entier $\geqslant 1$. Les assertions suivantes sont équivalentes*:

(a) *Il existe un entier $M_1(d)$ tel que, quel que soit l'anneau A,*

$$v(d;A)\leqslant M_1(d);$$

(b) *Il existe un entier $M_2(d)$ tel que, quel que soit l'entier $n\geqslant 0$, on ait*

$$v(d;\mathbf{Z}[n])\leqslant M_2(d),$$

(en posant pour abréger $\mathbf{Z}[n]=\mathbf{Z}[T_1,T_2,\ldots,T_n]$);

(c) *Quel que soit $n\geqslant 0$, on a*

$$v(d;\mathbf{Z}[n])<\infty,$$

et de plus, il existe un entier $N_3(d)$ tel que, pour tout $n>N_3(d)$, on ait

$$v(d;\mathbf{Z}[n])<n.$$

Démonstration. (b) implique (a): soit A un anneau quelconque et soit $x\in A_d$; il existe un entier n, des e_j et des x_j $(1\leqslant j\leqslant n)$ tels que

$$x=e_1x_1^d+\ldots+e_nx_n^d.$$

Considérons l'anneau $\mathbf{Z}[n]=\mathbf{Z}[T_1,T_2,\ldots,T_n]$, l'homomorphisme $h:\mathbf{Z}[n]\to A$ tel que $h(T_j)=x_j$ pour $j=1,2,\ldots,n$, et posons $t=e_1T_1^d+e_2T_2^d+\ldots+e_nT_n^d$; alors $h(t)=x$ et $t\in(\mathbf{Z}[n])_d$. Appliquons l'hypothèse (b) avec $m=M_2(d)$: il existe $u_1,u_2,\ldots,u_m\in\mathbf{Z}[n]$ et $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_m$, égaux à ±1, tels que

$$t=\varepsilon_1u_1^d+\varepsilon_2u_2^d+\ldots+\varepsilon_mu_m^d;$$

si $h(u_i)=y_i$, ceci donne, dans l'anneau A,

$$x=\varepsilon_1y_1^d+\varepsilon_2y_2^d+\ldots+\varepsilon_my_m^d,$$

donc $v(d;A)\leqslant m=M_2(d)$, ce qui prouve (a). En fait, on peut prendre $M_1(d)=M_2(d)$.

(c) implique (b): posons $N_3=N_3(d)$ et $M_3(d)=v(d;\mathbf{Z}[N_3])$. Il est clair que si $n\leqslant N_3$, on a $v(d;\mathbf{Z}[n])\leqslant M_3(d)$, car il existe un homomorphisme surjectif de $\mathbf{Z}[N_3]$ sur $\mathbf{Z}[n]$ obtenu en annulant les N_3-n dernières variables T_j. Nous allons prouver par récurrence sur n la chose suivante:

pour tout $n\geqslant N_3$, on a également $v(d;\mathbf{Z}[n])\leqslant M_3(d)$.

Pour $n=N_3$, rien à démontrer; supposons donc $n>N_3$, et l'assertion prouvée pour l'anneau $\mathbf{Z}[n-1]$. Soit x un élément de $(\mathbf{Z}[n])_d$; puisque, par l'hypothèse (c), $v(d;\mathbf{Z}[n])<n$, il existe des e_j et des x_j $(1\leqslant j\leqslant n-1)$ tels que

$$x=e_1x_1^d+e_2x_2^d+\ldots+e_{n-1}x_{n-1}^d.$$

Considérons l'homomorphisme $\varphi:\mathbf{Z}[n-1]\to\mathbf{Z}[n]$, tel que $\varphi(T_j)=x_j$ pour $j=1,2,\ldots,n-1$, et posons

$$t=e_1T_1^d+e_2T_2^d+\ldots+e_{n-1}T_{n-1}^d;$$

alors $h(t)=x$, et $t\in(\mathbf{Z}[n-1])_d$. Si $\mu=M_3(d)$, l'hypothèse de récurrence nous garantit l'existence de $u_1,u_2,\ldots,u_\mu\in\mathbf{Z}[n-1]$ et de $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_\mu$, égaux à ±1, tels que

$$t=\varepsilon_1u_1^d+\varepsilon_2u_2^d+\ldots+\varepsilon_\mu u_\mu^d;$$

si $h(u_i)=y_i$, ceci donne, dans l'anneau $\mathbf{Z}[n]$,

$$x=\varepsilon_1y_1^d+\varepsilon_2y_2^d+\ldots+\varepsilon_\mu y_\mu^d,$$

donc $v(d;\mathbf{Z}[n])\leqslant\mu=M_3(d)$, ce qui prouve (b). En fait, on peut prendre $M_3(d)=M_2(d)$.

Comme par ailleurs le fait que (a) implique (c) est évident, la proposition est démontrée.

On peut compléter (7.12) par cette autre proposition:

PROPOSITION (7.13). *Soit d un entier $\geqslant 1$. Les assertions suivantes sont équivalentes*:

(b) (*voir proposition* (7.12));

(e) *Il existe un entier $M_4(d)$ tel que, quels que soient les entiers n et r et le nombre premier p, on ait*

$$v\big(d;(\mathbf{Z}/p^r\mathbf{Z})[T_1,T_2,\ldots,T_n]\big)\leqslant M_4(d);$$

(f) *Il existe un entier $M_5(d)$ tel que, quels que soient les entiers m et n, on ait*

$$v\big(d;(\mathbf{Z}/m\mathbf{Z})[T_1,T_2,\ldots,T_n]\big)\leqslant M_5(d);$$

(g) *Il existe un entier $M_6(d)$ tel que, quels que soient l'entier n et le nombre premier p, on ait*

$$v(d;\mathbf{Z}_p[T_1,T_2,\ldots,T_n])\leqslant M_6(d).$$

Démonstration. Laissée au lecteur.

3. Etude de $v(d;K)$ et $w(d;K)$ pour un corps K tel que $(K^*:K^{*d})<\infty$.

THÉORÈME (7.14). *Soient K un corps et d un entier $\geqslant 1$ tels que le groupe quotient K^*/K^{*d} soit d'ordre fini. Posons $(K^*:K^{*d})=g$. Alors*

(i) *Si* -1 *est somme de puissances* d*-ièmes dans* K*, on a l'inégalité*

$$w(d; K) \leqslant g,$$

et en particulier

$$u(d; K) \leqslant g.$$

(ii) *Si* -1 *n'est pas puissance* d*-ième dans* K *(et en particulier, si* -1 *n'est pas somme de puissances* d*-ièmes dans* K*),* g *est nécessairement pair, soit* $g = 2h$*; et on a l'inégalité*

$$v(d; K) \leqslant h.$$

(iii) *D'autre part, si* K *est infini, on a l'égalité* $K_d = K$.

L'énoncé (7.14), (i) ressemble beaucoup au théorème de Demyanov (voir [9]); il ne semble pas cependant possible de déduire l'un de ces deux théorèmes de l'autre.

Démonstration. Envisageons d'abord le cas (i); K_d est alors égal à K_d^+, ensemble des sommes de puissances d-ièmes. Pour tout $n \geqslant 1$, désignons par S_n l'ensemble des éléments de K^* qui sont sommes de n puissances d-ièmes au plus; il est clair que

$$K^{*d} = S_1 \subset S_2 \subset \ldots \subset S_n \subset S_{n+1} \subset \ldots$$

et que, dans le groupe K^*, chaque sous-ensemble S_n est saturé modulo le sous-groupe K^{*d}: la suite des S_n ne peut donc présenter que $g-1$ inclusions strictes au plus. Or, un raisonnement par récurrence immédiat montre que si, pour une valeur $n = i$, $S_i = S_{i+1}$, alors, quel que soit $j \geqslant i$, $S_{i+j} = S_i$. Il résulte de ces deux remarques que

$$S_g = S_{g+1} = \ldots = S_{g+j} = \ldots$$

et par conséquent que

$$K_d^* = K_d^+ - \{0\} = \bigcup_{n \geqslant 1} S_n = S_g.$$

Autrement dit, tout élément de K_d^* (donc aussi de $K_d = K_d^* \cup \{0\}$) est somme d'au plus g puissances d-ièmes, C.Q.F.D.

Passons maintenant au cas (ii), où -1 n'est pas puissance d-ième dans K. Désignons par D le sous-groupe $\{-1, 1\}$ de K^*: par hypothèse, $-1 \neq 1 = 1^d$, donc D est d'ordre 2, et $D \cap K^{*d} = \{1\}$. Il en résulte que K^*/K^{*d} admet un sous-groupe d'ordre 2, $DK^{*d}/K^{*d} \simeq D/(D \cap K^{*d}) \simeq D$; $g = (K^*: K^{*d})$ est donc pair, $g = 2h$, et h est l'ordre du groupe quotient K^*/DK^{*d}. Cela étant, pour tout $n \geqslant 1$, désignons par T_n l'ensemble des éléments de K^* qui s'expriment à l'aide de n puissances d-ièmes au plus. Il est clair que

$$DK^{*d} = T_1 \subset T_2 \subset \ldots \subset T_n \subset T_{n+1} \subset \ldots$$

et que, dans le groupe K^*, chaque sous-ensemble T_n est saturé modulo DK^{*d}. On conclut comme précédemment que $K_d = T_h$, et donc que tout élément de K_d s'exprime à l'aide de h puissances d-ièmes, C.Q.F.D.

Prouvons maintenant la partie (iii) du théorème. Posons $L = K_d$; comme K est infini, L est infini; et comme l'indice $(K^*: K^{*d})$ est fini, l'indice $(K^*: L^*)$ est fini. Posons $(K^*: L^*) = q$, et soient $x_1, x_2, \ldots, x_q$ des représentants des q classes de K^* modulo L^*. On a

$$K^* = (L^* x_1) \cup (L^* x_2) \cup \ldots \cup (L^* x_q)$$

et a fortiori

$$K = (Lx_1) \cup (Lx_2) \cup \ldots \cup (Lx_q).$$

Ceci signifie que K, considéré comme espace vectoriel sur L, est réunion de q droites. Comme L est infini, ce n'est possible que si $[K: L] = 1$. D'où $L = K$, c'est à dire $K_d = K$, C.Q.F.D.

Remarque (7.15). La partie (i) de (7.14) est bien connue, du moins lorsque K est un corps fini (voir Tornheim [26]). Notons que la conclusion de (i) implique que la forme diagonale $X_1^d + X_2^d + \ldots + X_g^d$ représente tout élément de K_d. De même, la conclusion de (ii) implique que la forme diagonale $X_1^d + \ldots + X_h^d - X_{h+1}^d - \ldots - X_g^d$ représente tout élément de K_d. Ainsi, dans tous les cas, il existe g $(= (K^*: K^{*d}))$ coefficients $e_1, e_2, \ldots, e_g$, égaux à ± 1, tels que la forme diagonale à g variables

$$e_1 X_1^d + e_2 X_2^d + \ldots + e_g X_g^d$$

représente tout élément de K_d. Notons que lorsque K est infini, la forme en question est universelle pour K, c'est-à-dire représente tout élément de K (conséquence de (iii)), mais que la conclusion $K_d = K$ de (iii) peut devenir fausse si on abandonne l'hypothèse K infini. En effet, si K est fini, on a évidemment $(K^*: K^{*d}) < \infty$, mais il peut arriver que $K_d \neq K$ (voir l'exemple (2.6)).

Le théorème (7.14) amène la question suivante: *quels sont les corps usuels satisfaisant à la condition* $(K^*: K^{*d}) = g < \infty$*, et quelle est alors la valeur de* g ? On peut citer les trois principaux types suivants:

(I) *Corps finis.* Soit $k = \boldsymbol{F}_q$, $q = p^f$, un corps fini. On a vu (lemme (2.2)) que $(k^*: k^{*d}) = (q-1, d)$.

D'autre part, $u(d; k) < \infty$, puisqu'on est en caractéristique $p > 0$. Le théorème (7.14) donne alors l'énoncé suivant:

Proposition (7.16). *Si* k *est un corps fini à* q *éléments, on a*

$$u(d; k) \leqslant w(d; k) \leqslant (q-1, d) \leqslant d.$$

(II) *Corps de Brauer.* Rappelons (voir [14], [27]) qu'on appelle *corps de Brauer* tout corps *parfait* K possédant l'une des deux propriétés équivalentes (a) et (b) ci-après ($\overline{K}$ désigne la clôture algébrique de K):

(a) quel que soit l'entier $n \geqslant 1$, K possède dans $\bar{K}$ au plus une extension de degré n;

(b) le groupe de Galois $G_K = G(\bar{K}/K)$ est procyclique.

Soient K un corps de Brauer et D_K l'ordre de G_K: c'est un nombre surnaturel $\prod_p p^{n(p)}$ dont la donnée détermine d'ailleurs G_K à un isomorphisme près (voir [13]). Deux cas sont possibles:

ou bien $D_K = 2$; K est alors un corps ordonné maximal. Ou bien la partie finie de D_K est égale à 1, ce qui équivaut à dire que, quel que soit p, $n(p) = 0$ ou ∞. On dit alors que K est un corps de Brauer strict.

Soit K un corps de Brauer strict, et soit d un entier $\geqslant 1$. On peut démontrer deux choses (voir [14], [27]):

(i) K est non-ordonnable; compte tenu de (6.15), on a donc

$$u(d; K) < \infty.$$

(ii) Si E_K désigne l'ordre du groupe de toutes les racines de l'unité dans K (c'est, comme D_K, un nombre surnaturel), on a

$$(K^*: K^{*d}) = \gcd(d, D_K, E_K) < \infty.$$

Le théorème (7.14) donne alors l'énoncé suivant:

PROPOSITION (7.17). *Soient K un corps de Brauer strict, d un entier $\geqslant 1$, et désignons par D_K et E_K l'ordre du groupe de Galois $G_K = G(\bar{K}/K)$ et l'ordre du groupe de toutes les racines de l'unité dans K. On a alors*

$$u(d; K) \leqslant w(d; K) \leqslant \gcd(d, D_K, E_K) \leqslant d.$$

Cet énoncé généralise (7.16); si K est un corps fini à q éléments, c'est en effet un corps de Brauer strict, et $D_K = \prod_p p^\infty$, $E_K = q-1$: d'où

$$(K^*: K^{*d}) = \gcd(d, D_K, E_K) = (q-1, d).$$

Parmi les corps de Brauer infinis, signalons

les corps absolument algébriques de caractéristique > 0 et de degré infini sur le corps premier;

les corps de séries formelles $k((T))$, avec k corps algébriquement clos de caractéristique 0; et les extensions algébriques quelconques de tels corps.

(III) *Corps $\mathfrak{P}$-adiques.* Soit K un corps $\mathfrak{P}$-adique, avec $\mathfrak{P}|p$. On sait que le groupe K^*/K^{*d} est d'ordre fini (voir [19]): si μ_d désigne le groupe des racines d-ièmes de l'unité dans K, on a d'ailleurs $(K^*: K^{*d}) = d \cdot p^{e v_p(d)} \cdot (\mu_d: 1)$, e étant l'indice de ramification de $K/\mathbf{Q}_p$.

Notons que lorsque $K = \mathbf{Q}_p$, le second membre de cette égalité est majoré par d^2, sauf pour $p = 2$ et $d =$ une puissance de 2, auquel cas il est égal à $2d^2$. Comme par ailleurs $u(d; \mathbf{Z}_p) < \infty$ (voir (6.19)), le théorème (7.14) nous permet d'énoncer:

PROPOSITION (7.18). *Pour le corps $\mathbf{Q}_p$ des rationnels p-adiques, on a les inégalités*

$$u(d; \mathbf{Q}_p) \leqslant w(d; \mathbf{Q}_p) \leqslant d^2,$$

(sauf peut-être si $p = 2$ et $d =$ une puissance de 2, auquel cas on peut quand même écrire

$$u(d; \mathbf{Q}_p) \leqslant w(d; \mathbf{Q}_p) \leqslant 2d^2).$$

En fait, l'inégalité $w(d; \mathbf{Q}_p) \leqslant d^2$ est vraie même lorsque $p = 2$ et $d = 2^m$; voir par exemple [8].

4. Etude de $v(d; A)$ et $w(d; A)$ pour une algèbre A sur un corps infini. Nous allons d'abord étudier $v(d; A)$.

LEMME (7.20). *Soient A une algèbre sur un corps de caractéristique 0, et d un entier $\geqslant 1$. Alors*

$$v(d; A) \leqslant 2^{d-1}.$$

Démonstration. Puisque le corps de base K est de caractéristique 0, $d!$ est inversible dans K, donc dans A, et l'application

$$x \mapsto d!\, x + \frac{(d-1)\,d!}{2}$$

est une bijection de A sur elle-même. L'identité (8.2.2) (appendice) montre alors que tout élément de A peut s'écrire

$$\sum_{h=0}^{d-1} (-1)^{d-1-h} \binom{d-1}{h} (y+h)^d;$$

d'où $A = A_d$, ce qu'on savait déjà, et surtout

$$v(d; A) \leqslant \sum_{h=0}^{d-1} \binom{d-1}{h} = 2^{d-1}.$$

LEMME (7.21). *Soient A une algèbre sur un corps (fini ou non) de caractéristique $p > 0$, et d un entier $\geqslant 1$. Supposons $d \leqslant p$; alors*

$$v(d; A) \leqslant d^2.$$

Démonstration. Si $d = p$, $v(d; A) = 1$, car alors $A_d = A^p$, image de A par l'endomorphisme (d'anneau) $x \mapsto x^p$. Supposons donc $d < p$. Dans ce cas $d!$ n'est pas divisible par p, il est donc inversible dans A; l'application

$$x \mapsto d!\, x + \frac{(d-1)\,d!}{2}$$

est ici encore une bijection de A sur elle-même, et tout élément de A peut s'écrire

$$\sum_{h=0}^{d-1} (-1)^{d-1-h} \binom{d-1}{h} (y+h)^d.$$

Maintenant, chaque coefficient $(-1)^{d-1-h}\binom{d-1}{h}$ appartient au corps premier $\boldsymbol{F}_p$, et par conséquent s'écrit comme somme d'au plus d puissances d-ièmes; tout élément de A peut donc s'écrire comme somme d'au plus d^2 puissances d-ièmes: $w(d; A) \leqslant d^2$, et a fortiori $v(d; A) \leqslant d^2$, C.Q.F.D.

Lemme (7.22). *Soient p un nombre premier et d un entier $> p$. Ecrivons $d = p^r \cdot e$, avec $(p, e) = 1$, et posons*

$$m = p^{\varphi(e)} - 1,$$

φ étant la fonction indicatrice d'Euler (m ne dépend donc que de p et d). Il existe alors un nombre $H(p, d)$ ne dépendant lui-même que de p et d et ayant la propriété suivante:

pour tout corps K de caractéristique p, tel que $(K^{*m}: 1) \geqslant m-1$, et pour toute K-algèbre A, l'inégalité suivante est vérifiée:

$$v(d; A) \leqslant H(p, d).$$

Démonstration. Remarquons d'abord qu'avec nos notations habituelles

$$\left(\sum e_i a_i^e\right)^{p^r} = \sum e_i a_i^{p^r \cdot e} = \sum e_i a_i^d;$$

d'après le lemme (2.7), $A_e = A$; le calcul ci-dessus prouve donc que $A_d = A^{p^r}$, et surtout que $v(d; A) = v(e; A)$. Mais $(p, e) = 1$; donc (comme dans le lemme (2.7)), e divise m, et par conséquent

$$v(d; A) \leqslant v(m; A).$$

Il suffit dans ces conditions d'établir une majoration du type

$$v(m; A) \leqslant H(p, d).$$

Soit alors $x \in A$; choisissons (toujours comme dans (2.7)) $m-1$ éléments $u_1, u_2, \ldots, u_{m-1}$ de K^* tels que les u_j^m soient deux à deux distincts. Appliquons l'identité du théorème (8.4) avec $X = x$, $U_1 = u_1, \ldots, U_{m-1} = u_{m-1}$; nous trouvons

$$x = e_1[P_1(u, x)]^m + \ldots + e_h[P_h(u, x)]^m$$

($h = h(p, t)$, les $e_k = \pm 1$, les $P_k(u, x) \in A$; ceci parce que le dénominateur commun

$$u_1 u_2 \ldots u_{m-1} \prod_{i<j} (u_i^m - u_j^m)$$

est un élément non nul de K, donc un élément inversible de A). Ainsi

$$v(m; A) \leqslant h(p, t),$$

avec $t = \varphi(e)$; d'où le lemme (7.22), avec

$$H(p, d) = h\big(p, \varphi(e)\big).$$

Théorème (7.23). *Soit d une variable à valeurs entières $\geqslant 1$. Il existe une fonction $V(d)$, à valeurs entières $\geqslant 1$, et possédant la propriété suivante:*

quelle que soit A, algèbre sur un corps infini (de caractéristique quelconque) et quel que soit l'exposant $d \geqslant 1$, l'inégalité ci-après est satisfaite:

$$v(d; A) \leqslant V(d).$$

Démonstration. Fixons d. Soit p la caractéristique du corps de base; trois cas sont possibles:

$p = 0$:	alors $v(d; A) \leqslant 2^{d-1}$	(voir (7.20));
$p \geqslant d$:	alors $v(d; A) \leqslant d^2$	(voir (7.21));
$0 < p < d$:	alors $v(d; A) \leqslant H(p, d)$	(voir (7.22));

maintenant, l'ensemble des nombres premiers p tels que $p < d$ est fini. Posons $H(d) = \sup_{p<d} H(p, d)$; alors le théorème (7.23) est vérifié avec

$$V(d) = \sup\big(2^{d-1}, d^2, H(d)\big).$$

Donnons, pour $d \geqslant 3$, une majoration de $V(d)$, et d'abord, de $H(p, d) = h\big(p, \varphi(e)\big)$. Reportons-nous à (8.4) (appendice) et considérons la formule de Cramer:

$$(*) \qquad X = Z_1 = D_1 D^{-1}.$$

Faisons la convention provisoire suivante: si n est un entier $\geqslant 1$ et si $x \in B$, l'écriture $x = s(n)$ signifiera que x s'exprime à l'aide de n puissances m-ièmes. On notera que $s(n)s(n') = s(nn')$, et que $s(n)+s(n') = s(n+n')$. Cela étant, on a:

$$D = \binom{m}{1}\binom{m}{2}\ldots\binom{m}{m-1}\Big(\prod_i U_i\Big)^m \prod_{i<j}(U_i^m - U_j^m);$$

d'autre part, D_1 est le déterminant d'ordre $m-1$ dont la j-ième ligne s'écrit

$$(U_j^m + X) - U_j^{m^2} - X^m; \quad \binom{m}{2} U_j^{m(m-2)}; \quad \binom{m}{3} U_j^{m(m-3)}; \quad \ldots; \quad \binom{m}{m-1} U_j^m;$$

dans D_1, on peut mettre en facteur $\binom{m}{2}\binom{m}{3}\ldots\binom{m}{m-1}$, puis, compte tenu de la forme de la première colonne, décomposer le déterminant restant en une somme $D_1' - D_1'' - D_1'''$, chaque terme de cette somme étant un

déterminant d'ordre $m-1$ ayant pour éléments uniquement des puissances m-ièmes. Il est clair que $D_1' = s\big((m-1)!\big)$ et de même pour les deux autres. Ainsi

$$D_1' - D_1'' - D_1''' = s\big(3(m-1)!\big).$$

Revenons alors à la formule (*): après simplification par $\binom{m}{2}\binom{m}{3}\cdots\binom{m}{m-1}$, nous obtenons

$$(**) \qquad X = s(p-1)\,s\big(3(m-1)!\big)\,\frac{1}{\prod_{i<j}(U_i^m - U_j^m)}.$$

En effet, $\dfrac{1}{(\prod_i U_i)^m} = s(1)$; et $\dfrac{1}{\binom{m}{1}} = s(p-1)$, parce que $\dfrac{1}{\binom{m}{1}} = m^{-1}$ appartient au corps premier $\boldsymbol{F}_p$, dans lequel tout élément est évidemment somme de $p-1$ puissances m-ièmes. Mais $\prod_{i<j}(U_i^m - U_j^m)$ est le déterminant de Vandermonde des U_j^m, donc

$$\prod_{i<j}(U_i^m - U_j^m) = s\big((m-1)!\big)$$

et

$$\frac{1}{\prod_{i<j}(U_i^m - U_j^m)} = \frac{\big[\prod(U_i^m - U_j^m)\big]^{m-1}}{\big[\prod(U_i^m - U_j^m)\big]^m} = \big[s\big((m-1)!\big)\big]^{m-1}.$$

Si on porte ce résultat dans (**), on trouve finalement, compte tenu de la définition de $h(p, \varphi(e))$,

$$H(p, d) \leqslant 3(p-1)\big((m-1)!\big)^m.$$

Evaluons maintenant $H(d)$ et pour commencer, majorons m. Evidemment, $p \leqslant d-1$, et $\varphi(e) \leqslant d-1$. D'où $m \leqslant (d-1)^{d-1}-1$. Et il ne semble pas que l'on puisse faire beaucoup mieux: car si p et d sont deux nombres premiers jumeaux ($d = p+2$), on aura $e = d$, et $m = (d-2)^{d-1}-1$.

Ainsi $H(d) \leqslant 3(d-2)\big((\mu-1)!\big)^\mu$ avec $\mu = (d-1)^{d-1}-1$. Or, $H(d)$ est (malheureusement) très grand devant d^2 et même 2^{d-1}. De sorte qu'en fait $V(d) = H(d)$. Finalement

PROPOSITION (7.24). *Pour $d \geqslant 3$, la fonction $V(d)$ introduite au théorème* (7.23) *satisfait à l'inégalité*

$$V(d) \leqslant 3(d-2)\big((\mu-1)!\big)^\mu$$

avec $\mu = (d-1)^{d-1}-1$.

(Rappelons que pour tout anneau A, $v(2; A) \leqslant 3$, et que, si A est un corps, ou d'ailleurs plus généralement une algèbre sur un corps on a même $v(2; A) \leqslant 2$. Inutile donc de se préoccuper de $V(2)$.)

En fait, la majoration établie n'a d'autre intérêt que d'être explicite. Pour un degré aussi faible que $d = 4$, on trouve en effet déjà:

$$V(4) \leqslant 6 \cdot (25!)^{26}.$$

Le seul résultat raisonnable est pour $d = 3$; la proposition (7.24) donne alors en effet $V(3) \leqslant 24$. Mais dans ce cas particulier, on a un résultat plus précis:

THÉORÈME (7.25). *Soit K un corps autre que les deux corps finis $\boldsymbol{F}_2$ et $\boldsymbol{F}_4$. Si A est une K-algèbre, on a l'inégalité*

$$v(3; A) \leqslant 12.$$

Démonstration. Reportons-nous à la démonstration du théorème (7.23). Comme $2^{3-1} = 4$ et $3^2 = 9$, et que d'autre part la condition $p < 3$ n'est satisfaite que par $p = 2$, il s'agit en fait de prouver $H(2, 3) \leqslant 12$. Notons alors que, dans le lemme (7.22), on a $r = 0$, $e = 3$, $\varphi(e) = 2$, $m = 2^2-1 = 3$. La condition $(K^{*m}: 1) \geqslant m-1$ est vérifiée si K est infini. Mais si K est fini, $K = \boldsymbol{F}_{2^f}$, on a (voir (2.2))

$$(K^{*m}: 1) = (2^f-1)/(2^f-1, m) \geqslant (2^f-1)/m = (2^f-1)/3$$

et ceci est supérieur ou égal à $m-1 = 2$ pour $f \geqslant 3$; la condition est finalement satisfaite en caractéristique $p = 2$ par tout corps autre que $\boldsymbol{F}_2$ et $\boldsymbol{F}_4$. Pour calculer maintenant $H(2, 3) = h(2, 2)$, reportons-nous au théorème (8.4) (appendice); nous devons résoudre en Z_1 et Z_2 le système de Cramer

$$\begin{cases} U_1^6 Z_1 + U_1^3 Z_2 = (U_1^3 + X)^3 + U_1^9 + X^3, \\ U_2^6 Z_1 + U_2^3 Z_2 = (U_2^3 + X)^3 + U_2^9 + X^3 \end{cases}$$

(rappelons que nous sommes en caractéristique 2); ce système donne

$$X = Z_1 = D_1 D^{-1}$$

avec

$$D = (U_1^2 U_2)^3 + (U_1 U_2^2)^3,$$

et

$$D_1 = \begin{vmatrix} (U_1^3 + X)^3 + U_1^9 + X^3 & U_1^3 \\ (U_2^3 + X)^3 + U_2^9 + X^3 & U_2^3 \end{vmatrix}.$$

D_1 est manifestement somme de 6 cubes. Quant à

$$D^{-1} = \frac{(U_1^4 U_2^2)^3 + (U_1^2 U_2^4)^3}{[(U_1^2 U_2)^3 + (U_1 U_2^2)^3]^3} \qquad \left(= \frac{D^2}{D^3}\right),$$

il est somme de deux cubes. Donc X est somme de $2 \times 6 = 12$ cubes ce qui signifie précisément

$$H(2, 3) = h(2, 2) = 12.$$

Indiquons enfin une conséquence immédiate du théorème (7.23):

THÉORÈME (7.26). *Quels que soient le corps K et l'entier $d \geqslant 1$, on a*

$$v(d; K) \leqslant V(d).$$

Démonstration. Si K est infini, c'est un cas particulier de (7.17); et si K est fini, on sait (voir (7.16)) que:

$$v(d; K) \leqslant d \leqslant d^2 \leqslant V(d).$$

Passons à l'étude de $w(d; A)$, et commençons par rappeler un résultat prouvé au cours de la démonstration du lemme (7.21):

PROPOSITION (7.27). *Soient A une algèbre sur un corps de caractéristique $p > 0$, et d un entier $\geqslant 1$. Supposons $d \leqslant p$; alors*

$$w(d; A) \leqslant d^2.$$

Plus généralement:

PROPOSITION (7.28). *Soient A une algèbre sur un corps infini de caractéristique > 0, et d un entier $\geqslant 1$. On a alors*

$$w(d; A) \leqslant dV(d).$$

Démonstration. Il suffit d'écrire $w(d; A) \leqslant u(d; A)v(d; A)$, puis $u(d; A) \leqslant u(d; \boldsymbol{F}_p) \leqslant d$, p étant la caractéristique du corps de base, et enfin $v(d; A) \leqslant V(d)$.

PROPOSITION (7.29). *Soient A une algèbre sur un corps de caractéristique 0, et d un entier $\geqslant 1$. Si $u(d; A) < \infty$, on a*

$$w(d; A) \leqslant 2^{d-2}\big(1 + u(d; A)\big).$$

Démonstration. On a déjà vu que tout élément de A s'écrit

$$\sum_{h=0}^{d-1} (-1)^{d-1-h} \binom{d-1}{h} (y+h)^d.$$

Pour $h = d-2, d-4, \ldots$, remplaçons $-1 = (-1)^{d-1-h}$ par une somme de $u(d; A)$ puissances d-ièmes. L'expression ci-dessus se transforme alors en une somme de

$$\left[\binom{d-1}{d-1} + \binom{d-1}{d-3} + \ldots\right] + \left[\binom{d-1}{d-2} + \binom{d-1}{d-4} + \ldots\right] u(d; A)$$

puissances d-ièmes, c'est-à-dire précisément $2^{d-2} + 2^{d-2}u(d; A)$ puissances d-ièmes, C.Q.F.D.

Remarque. Tornheim donne (pour un corps K de caractéristique 0, mais sa méthode s'applique sans modification à une algèbre sur K) la majoration

$$w(d; K) \leqslant (d+1)u(d; K)g(d),$$

$g(d)$ étant la constante de Waring pour les entiers naturels, (voir [26]). On sait que, pour d assez grand,

$$g(d) = 2^d - 2 + [(\tfrac{3}{2})^d];$$

l'ordre de grandeur du second membre de la majoration de Tornheim est donc $(d+1)2^d \cdot u(d; K)$.

Nous allons maintenant démontrer un résultat annoncé au paragraphe 2:

THÉORÈME (7.30). *Il existe un corps L (de caractéristique 0, ordonnable) ayant la propriété suivante: quel que soit l'exposant pair d, on a*

$$w(d; L) = \infty.$$

Démonstration. Ce théorème n'est en fait qu'une amélioration de (7.11). Désignons encore par $(K_{(m)})_{m \geqslant 0}$ une suite de corps satisfaisant à la condition

$$u(2; K_{(m)}) = 2^m$$

(voir (6.9)), et soit par ailleurs $\mathscr{D}$ un ultrafiltre non-principal sur l'ensemble $\boldsymbol{N}$ des entiers $m \geqslant 0$. Considérons l'ultraproduit

$$L = \prod K_{(m)}/\mathscr{D}$$

(voir [17]; rappelons qu'il s'agit du quotient de l'anneau $A = \prod K_{(m)}$ par l'idéal $\mathfrak{I}_{\mathscr{D}}$ de A ainsi défini: un élément (x_m) de A appartient à $\mathfrak{I}_{\mathscr{D}}$ si et seulement si l'ensemble

$$\{m \mid m \geqslant 0 \text{ et } x_m = 0\}$$

est un élément de $\mathscr{D}$). L est un corps, et nous allons justement prouver que, quel que soit l'exposant pair $d \geqslant 2$, on a $w(d; L) = \infty$.

Soit donc d, pair et $\geqslant 2$.

LEMME (7.31). *Quel que soit $m \geqslant 0$, et quel que soit m_0 tel que $0 \leqslant m_0 \leqslant m$, il existe un élément de $K_{(m)}$ qui est somme de 2^{m_0} puissances d-ièmes, mais qui n'est pas somme de $2^{m_0}-1$ puissances d-ièmes.*

Démontrons ce lemme. Puisque $u(2; K_{(m)}) < \infty$, le théorème (6.15) prouve que $u(d; K_{(m)}) < \infty$; et en fait, puisque d est multiple de 2 et que toute somme de puissances d-ièmes est donc une somme de carrés, on a la suite d'inégalités

$$2^{m_0} \leqslant 2^m = u(2; K_{(m)}) \leqslant u(d; K_{(m)}) < \infty.$$

Ecrivons alors $-1 = u_1^d + u_2^d + \ldots + u_h^d$, avec $h = u(d; K_{(m)})$: il est clair que l'élément $u_1^d + u_2^d + \ldots + u_{2^{m_0}}^d$ est somme de 2^{m_0} puissances d-ièmes, mais non de $2^{m_0}-1$, et le lemme est démontré.

Revenons au théorème lui-même, et désignons par π la projection canonique

$$A = \prod K_{(m)} \to L = \prod K_{(m)}/\mathscr{D}.$$

Il s'agit de prouver, pour tout $n > 0$, que $w(d; L) > n$. Soit m_0 le plus petit entier m tel que $2^m > n$; d'après le lemme (7.31), il existe, pour tout $m \geqslant m_0$, un élément $a_m \in K_{(m)}$ qui est somme de 2^{m_0} puissances d-ièmes, mais non de $2^{m_0}-1$ puissances d-ièmes. Pour tout $m < m_0$, posons par ailleurs $a_m = 0$; désignons enfin par x l'élément $\pi\big((a_m)\big) \in L$. Il est clair que x est somme de 2^{m_0} puissances d-ièmes: car c'est vrai de a_m, quel que soit m. Ainsi $x \in L_d^+$. Mais x n'est pas somme de n puissances d-ièmes (ce qui implique $w(d; L) > n$ et prouve donc le théorème). En effet, si x était somme de n puissances d-ièmes, il existerait $J \in \mathscr{D}$ (J nécessairement infini, parce que $\mathscr{D}$ est non-principal) tel que, pour tout $m \in J$, a_m soit somme de n puissances d-ièmes; mais le choix des a_m et l'inégalité $n < 2^{m_0}$ impliqueraient alors

$$J \subset \{0, 1, \ldots, m_0-1\},$$

ce qui est absurde, l'ensemble de droite étant fini.

Notons pour terminer ce paragraphe qu'une égalité du type $w(d; K) = \infty$, où K est un corps, est impossible si d est impair: car alors, d'après (7.1) et (7.26),

$$w(d; K) = v(d; K) \leqslant V(d).$$

Notons également que

si K est de caractéristique $\neq 0$, $w(d; K) \leqslant dV(d)$ quel que soit d (voir (7.28));

si K est de caractéristique 0 non-ordonnable, on a la double inégalité $u(d; K) \leqslant U\big(u(2; K), d\big) < \infty$, quel que soit d (voir (6.16)), et par conséquent

$$u(2; K) \leqslant u(d; K) \leqslant w(d; K) \leqslant u(d; K)v(d; K) \leqslant U\big(u(2; K), d\big)V(d).$$

On peut donc (pour les corps) dresser le tableau suivant (qui résume complètement la question concernant v et w):

K / d	non-ordonnable		ordonnable
	$p > 0$	$p = 0$ $u(2; K) < \infty$	$p = 0$ $u(2; K) = \infty$
impair	$w \leqslant V(d)$ $v \leqslant V(d)$	$w \leqslant V(d)$ $v \leqslant V(d)$	$w \leqslant V(d)$ $v \leqslant V(d)$
pair	$w \leqslant dV(d)$ $v \leqslant V(d)$	$u(2; K) \leqslant w$ et $w \leqslant \big(Uu(2; K), d\big)V(d)$ (w est donc fini, mais peut être arbitrairement grand: voir (6.9)); $v \leqslant V(d)$	w peut être fini (faire $K = Q$), ou infini (faire $K = L$); $v \leqslant V(d)$

5. Etude de $w(d; A)$ pour un anneau local hensélien A. Applications. Rappelons d'abord quelques résultats relatifs au problème de Waring pour un anneau $\mathfrak{P}$-adique. Soit d un entier $\geqslant 1$.

(I) Si $\boldsymbol{Z}_p$ désigne l'anneau des entiers rationnels p-adiques, on sait depuis longtemps que $(\boldsymbol{Z}_p)_d = \boldsymbol{Z}_p$, et que

$$w(d; \boldsymbol{Z}_p) \leqslant 4d-1,$$

(voir par exemple [18], Satz 31, où le résultat est exprimé sous forme de congruence).

(II) Birch a démontré récemment le résultat suivant (voir [3]) quel que soit l'anneau $\mathfrak{P}$-adique A, on a $w(d; A) \leqslant d^{16d^2}$; Ramanujam (voir [23]) a prouvé par une autre méthode que l'on a plus précisément

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

(III) Signalons également une conséquence implicite de la proposition 1 de [23]: pour tout anneau $\mathfrak{P}$-adique A absolument non-ramifié (et de caractéristique résiduelle p), on

$$w(d; A) \leqslant \begin{cases} 4d & (\text{si } p = 2), \\ 2d & (\text{si } p > 2). \end{cases}$$

Nous allons pour notre part prouver ceci:

THÉORÈME (7.32). *Soient A un anneau $\mathfrak{P}$-adique quelconque et d un exposant premier. Alors*

$$w(d; A) \leqslant \begin{cases} 6 & (si\ d = 2), \\ 2d-1 & (si\ d > 2). \end{cases}$$

En fait, ce théorème est un cas particulier d'un résultat relatif aux anneaux henséliens, que nous allons démontrer maintenant (théorème (7.34)).

LEMME (7.33). *Soit A un anneau local hensélien de caractéristique résiduelle $p > 0$. Alors*

$$w(p; A) \leqslant \begin{cases} 6 & (si\ p = 2), \\ 2p-1 & (si\ p > 2). \end{cases}$$

Démonstration. Soient $\boldsymbol{Z}_{(p)}$ le localisé de $\boldsymbol{Z}$ en (p) et B le hensélisé de $\boldsymbol{Z}_{(p)}$. Puisque A est hensélien de caractéristique résiduelle p, l'homomorphisme canonique $\boldsymbol{Z} \to A$ se prolonge en un homomorphisme $h : B \to A$. Distinguons alors deux cas:

1er cas: $p = 2$. Je dis tout d'abord que

$$u(2; A) \leqslant 4.$$

Considérons en effet le polynôme $X^2-X+2 \in B[X]$, cas particulier du polynôme X^p-X+p introduit dans la démonstration de (6.19); d'après ce qu'on a vu alors, ce polynôme admet dans B deux racines. Soit a l'une d'entre elles; on peut écrire $a^2-a+2=0$; après transformation, ceci devient

$$-1 = (2a-1)^2+2^2+1^2+1^2,$$

d'où $u(2;B) \leqslant 4$ et a fortiori $u(2;A) \leqslant 4$, (appliquer (6.1) à l'homomorphisme $h: B \to A$). Maintenant, d'après (7.9) tout élément de A_2 s'écrit $x^2+(y+1)^2-y^2$: remplaçant -1 par une somme de quatre carrés, on voit bien que $w(2;A) \leqslant 6$.

2e cas: $p>2$. A est une B-algèbre (grâce à h), donc un quotient d'une algèbre de polynômes $C = B[\boldsymbol{T}]$, $\boldsymbol{T}$ désignant une famille d'indéterminées suffisamment grande. D'après (7.2), (i), il suffit de prouver l'inégalité $w(p;C) \leqslant 2p-1$. On va pour cela appliquer (7.2), (iii) à l'anneau C et à son idéal pC. Tout d'abord, $w(p;C/pC)=1$, car C/pC est l'algèbre des polynômes en $\boldsymbol{T}$ sur le corps premier $\boldsymbol{F}_p$ de caractéristique p. D'autre part, tout élément de pC est somme de $2p-2$ puissances p-ièmes: en effet, on sait (par application au polynôme $X^{p-1}-1$ du lemme de Hensel) que B, et a fortiori C, contient les racines $(p-1)$-ièmes de l'unité, $\zeta_1, \zeta_2, \ldots, \zeta_{p-1}$; par un calcul de fonctions symétriques, on vérifie alors que, pour tout $x \in C$, on a l'égalité

$$(-1)^p p(p-1)x = \sum_{j=1}^{p-1} \left((\zeta_j - x)^p + x^p\right);$$

le second membre est somme de $2p-2$ puissances p-ièmes; comme $p-1$ est inversible dans B, l'assertion se trouve établie. Cela étant, (7.2), (iii) nous permet d'écrire

$$w(d;B) \leqslant w(p;B/pB)+(2p-2) = 1+(2p-2), \qquad \text{C.Q.F.D.}$$

THÉORÈME (7.34). *Soit A un anneau local hensélien à corps résiduel fini. Si d est un exposant premier, on a la majoration*

$$w(d;A) \leqslant \begin{cases} 6 & (\text{si } d=2), \\ 2d-1 & (\text{si } d>2). \end{cases}$$

Démonstration. Soit p la caractéristique du corps résiduel k. Si $d=p$, l'inégalité résulte du lemme (7.33). Maintenant, si $d \neq p$, on a $(d,p)=1$, et d'autre part (voir proposition (7.16)) $w(d;K) \leqslant d$. D'après (2.16), il résulte de là que

$$w(d;A) \leqslant d+1.$$

Mais $d+1 \leqslant 6$ si $d=2$, $d+1 \leqslant 2d-1$ si $d>2$. Le théorème est démontré.

REMARQUE (7.35). Compte tenu de (7.23), ce raisonnement donne aussi le résultat suivant:

il existe une fonction $W(d)$ à valeurs entières $\geqslant 1$, ne dépendant que du nombre premier d, et telle que, quel que soit A, anneau local hensélien de caractéristique résiduelle >0, on ait:

$$w(d;A) \leqslant W(d).$$

Indiquons quelques applications du théorème (7.34).

THÉORÈME (7.36). *Soient A un anneau fini et d un exposant premier; on a la majoration*

$$w(d;A) \leqslant \begin{cases} 6 & (\text{si } d=2), \\ 2d-1 & (\text{si } d>2). \end{cases}$$

Démonstration. A se décompose en produit direct fini d'anneaux locaux eux-mêmes finis:

$$A = A_1 \times A_2 \times \ldots \times A_n;$$

il suffit donc de démontrer le théorème (7.36) lorsque A est local: mais dans ce cas, A est évidemment hensélien (il est complet pour sa structure uniforme naturelle, qui est discrète) et (7.36) est une conséquence particulière de (7.34).

THÉORÈME (7.37). *Soient A un anneau et d un exposant premier. Si l'anneau quotient $A/d!A$ est un produit fini d'anneaux locaux henséliens, on a l'inégalité*

$$v(d;A) \leqslant \begin{cases} 3 & (\text{si } d=2), \\ 2^{d-1}+2d-1 & (\text{si } d>2). \end{cases}$$

Démonstration. Si $d=2$, l'inégalité provient en fait de (7.9) (et l'hypothèse sur $A/d!A$ ne sert à rien). Supposons donc $d>2$; d est impair, et d'après (7.3.2) on a l'inégalité

$$v(d;A) \leqslant 2^{d-1}+v(d;A/d!A);$$

il s'agit de prouver que $v(d;A/d!A) \leqslant 2d-1$, ou encore que $w(d;A/d!A) \leqslant 2d-1$, puisque d est impair (voir (7.1)). Mais cette dernière inégalité résulte de (7.4), de (7.34) et de l'hypothèse faite sur $A/d!A$.

COROLLAIRE (7.38). *Soient A un anneau et d un exposant premier. Si l'anneau quotient $A/d!A$ est fini, on a l'inégalité:*

$$v(d;A) \leqslant \begin{cases} 3 & (\text{si } d=2), \\ 2^{d-1}+2d-1 & (\text{si } d>2). \end{cases}$$

Démonstration. Il suffit de remarquer que tout anneau fini est produit direct fini d'anneaux locaux henséliens (fait déjà utilisé dans la démonstration du théorème (7.36)).

REMARQUE (7.39). R. M. Stemmler a démontré le résultat suivant (voir [25]): si A est un anneau d'entiers algébriques et si d est un exposant premier, on a la majoration

$$v(d; A) \leqslant 2^{d-1} + \frac{d-1}{3} + 1.$$

Le corollaire (7.38) montre que (à une légère modification près de la quantité majorante) ce résultat est en fait valable pour une classe d'anneaux beaucoup plus vaste que celle des anneaux d'entiers algébriques. En particulier, il est valable si A est un ordre d'entiers algébriques non intégralement clos.

Autre conséquence du théorème (7.37):

COROLLAIRE (7.40). *Soit $\boldsymbol{T}$ une famille quelconque d'indéterminées, et soit A l'anneau de séries formelles $\boldsymbol{Z}[[\boldsymbol{T}]]$. On a l'inégalité*:

$$v(d; A) \leqslant \begin{cases} 3 & (si\ d = 2), \\ 2^{d-1} + 2d - 1 & (si\ d > 2). \end{cases}$$

Démonstration. Si $\prod p_i^{n_i}$ est la décomposition du nombre $d!$ en facteurs premiers, on a:

$$A/d!A \simeq \prod (\boldsymbol{Z}/p_i^{n_i}\boldsymbol{Z})[[\boldsymbol{T}]],$$

de sorte que $A/d!A$ est un produit fini d'anneaux locaux henséliens (en fait, complets).

REMARQUE (7.41). Si l'exposant premier d est > 2, et si $\boldsymbol{T}$ est finie, disons $\boldsymbol{T} = (T_1, T_2, \ldots, T_n)$, le corollaire (7.40) donne l'égalité

$$(*) \qquad v\big(d; \boldsymbol{Z}[[T_1, T_2, \ldots, T_n]]\big) \leqslant 2d-1;$$

qui rappelle l'inégalité

$$(**) \qquad v(d; \boldsymbol{Z}[T_1, T_2, \ldots, T_n]) \leqslant M_2(d)$$

de la proposition (7.12) (inégalité dont nous ignorons si elle est vraie ou fausse). L'idée peut venir d'essayer de démontrer (**) à l'aide de (*), et de prouver ainsi l'assertion (a) de (7.12) lorsque l'exposant d est premier. Et la méthode qui semble s'imposer est alors la suivante:

> étant donné un anneau filtré F, de gradué associé G, essayer de ramener (en un certain sens) le problème de Waring dans F au problème de Waring dans G.

Malheureusement, ceci ne semble guère possible, comme le démontre l'exemple suivant:

EXEMPLE (7.42). Posons:

$k = \boldsymbol{F}_2$;

$F = \boldsymbol{Z}$, filtré par les puissances de l'idéal (2);

$F' = k[[T]]$, filtré par les puissances de l'idéal (T).

On a $G \simeq G' \simeq k[T]$ (G et G' sont les gradués associés à F et F'). Or, pour l'exposant $d = 2$, on a

$$G_d \simeq G'_d \simeq k[T^2], \quad \text{et} \quad F_d = \boldsymbol{Z} = F,$$

mais

$$F'_d = k[[T^2]] \neq F';$$

et pour l'exposant $d = 3$, on a

$$F_d = \boldsymbol{Z} = F, \quad F'_d = k[[T]] = F',$$

mais G_d (ou G'_d) $\simeq k[T^3, T+T^2] \neq k[T] \simeq G$ (ou G').

CONCLUSION. Nous ne sommes pas plus avancés. Par exemple, nous ne savons même pas si

$$(***) \qquad v(3; \boldsymbol{Z}[T]) < \infty.$$

La détermination de $v(3; \boldsymbol{Z}[T])$ serait évidemment cruciale pour notre problème. Notons que, si $k = \boldsymbol{F}_2$, l'inégalité (***) équivaut à la suivante:

$$v(3; k[T]) < \infty.$$

Car, comme $k[T]$ est quotient de $\boldsymbol{Z}[T]$, on a

$$v(3; k[T]) \leqslant v(3; \boldsymbol{Z}[T]);$$

d'autre part, d'après (7.3.2),

$$v(3; \boldsymbol{Z}[T]) \leqslant 4 + v\big(3; (\boldsymbol{Z}/6\boldsymbol{Z})[T]\big).$$

Mais

$$(\boldsymbol{Z}/6\boldsymbol{Z})[T] \simeq (\boldsymbol{Z}/2\boldsymbol{Z})[T] \times (\boldsymbol{Z}/3\boldsymbol{Z})[T],$$

et

$$v\big(3; (\boldsymbol{Z}/3\boldsymbol{Z})[T]\big) = 1;$$

d'après (7.4), on a donc

$$v\big(3; (\boldsymbol{Z}/6\boldsymbol{Z})[T]\big) = v(3; k[T]);$$

et finalement

$$v(3; \boldsymbol{Z}[T]) \leqslant 4 + v(3; k[T]).$$

Voici une autre application du théorème (7.34):

PROPOSITION (7.43). *Soient A un anneau local séparé complet à corps résiduel fini, et d un exposant premier tel que A_d soit noethérien et A de type fini sur A_d.*

Alors, si $(T_1, T_2, \ldots, T_n)$ *est une famille finie d'indéterminées et si* $B = A[[T_1, T_2, \ldots, T_n]]$, *l'anneau* B_d *est lui-même noethérien.*

Démonstration. On peut naturellement se ramener au cas où $n = 1$: écrivons donc $B = A[[T]]$. Il est clair que B est, comme A, local séparé complet à corps résiduel fini. En particulier, il est compact et hensélien. Je dis d'autre part qu'on a l'inclusion

$$A_d[[T^d]] \subset B_d.$$

En effet, soit $y = \sum_{i\geqslant 0} c_i T^{id}$ (les $c_i \in A_d$) un élément quelconque de $A_d[[T^d]]$. Pour tout $n \geqslant 0$, on a évidemment

$$y_n = \sum_{i=0}^{n} c_i T^{id} \in (A[T])_d,$$

et a fortiori $y_n \in B_d$. Posons alors $M = 6$ (si $d = 2$) et $M = 2d-1$ (si $d > 2$); d'après (7.39) on a $w(d; B) \leqslant M$, et la relation $y_n \in B_d$ montre qu'il existe $F_{n,1}, F_{n,2}, \ldots, F_{n,M} \in B$ tels que

$$y_n = F_{n,1}^d + F_{n,2}^d + \ldots + F_{n,M}^d.$$

B étant compact, il existe (raisonnement classique) une suite d'entiers $0 < n_1 < n_2 < \ldots < n_q < \ldots$ et des éléments $F_1, F_2, \ldots, F_M$ de B tels que, pour $j = 1, 2, \ldots, M$,

$$\lim_{q\to\infty} F_{n_q,j} = F_j.$$

Alors

$$y = \lim_{q\to\infty} y_{n_q} = F_1^d + F_2^d + \ldots + F_M^d \in B_d,$$

ce qui prouve l'inclusion annoncée. Cette inclusion montre que B_d est un sous-$A_d[[T^d]]$-module de B. Or, A_d étant noethérien et A étant de type fini sur A_d (par hypothèse), $A_d[[T^d]]$ est noethérien, et B est de type fini sur $A_d[[T^d]]$, donc noethérien en tant que $A_d[[T^d]]$-module. Il en est alors de même pour le sous-module B_d, et a fortiori pour l'anneau B_d, C.Q.F.D.

Naturellement, le raisonnement ci-dessus s'appliquerait également dans toute situation où, d n'étant pas premier, on saurait cependant que $w(d; B) < \infty$. Notons qu'on peut par exemple appliquer (7.43) lorsque A est un anneau $\mathfrak{P}$-adique. Ainsi, quel que soit p premier, l'anneau $(\mathbf{Z}_p[[T]])_p$ est noethérien, ce que rien jusqu'à présent ne nous permettait d'affirmer.

Terminons par une remarque relative au théorème (7.36); ce théorème affirme: quel que soit d premier, il existe un nombre $M(d)$ tel que, pour tout anneau fini A, on ait la majoration $w(d; A) \leqslant M(d)$.

Problème. *Existe-t-il pour tout* d *un nombre* $M(d)$ *tel que, quel que soit* A *fini,* $w(d; A) \leqslant M(d)$?

C'est le problème de Waring généralisé, pour la classe $\mathscr{A}$ des anneaux finis. Nous ignorons la réponse (naturellement: sinon nous aurions mis cette réponse dans l'énoncé du théorème (7.36)). La seule chose certaine (et qui est triviale) c'est que, quels que soient $d \geqslant 1$ et A fini, on a

$$w(d; A) < \infty.$$

Nous sommes portés à croire que la réponse à ce problème est positive, et que la solution se trouve dans l'étude de la structure des anneaux locaux finis. *Les résultats de Birch–Ramanujam et de Stemmler apparaîtraient alors comme des conséquences du simple fait que si* A *est un anneau* $\mathfrak{P}$*-adique ou un anneau d'entiers algébriques, l'anneau* $A/d!\,A$ *est fini.*

Appendice

TROIS IDENTITÉS FONDAMENTALES

Théorème (8.1) (Hilbert–Hausdorff). *Quels que soient l'entier* $m \geqslant 1$ *et l'exposant* $d \geqslant 1$, *il existe des entiers* $c_{i,h}$ $(1 \leqslant i \leqslant m;\ 1 \leqslant h \leqslant 2d+1)$, *et des entiers positifs* $q \neq 0, q_1, q_2, \ldots, q_{2d+1}$, *tels que l'on ait l'identité suivante*:

$$q(X_1^2 + X_2^2 + \ldots + X_m^2)^d = \sum_h q_h (c_{1,h} X_1 + \ldots + c_{m,h} X_m)^{2d}.$$

Cette identité, dont l'existence avait été conjecturée par Hurwitz, a été établie pour la première fois en 1909 par Hilbert (pour prouver la conjecture de Waring: voir [12]); divers auteurs en ont, par la suite, donné de nouvelles démonstrations: citons en particulier celles de Hausdorff (voir [11]) et de Stridsberg.

Théorème (8.2). *Quel que soit l'exposant* $d \geqslant 1$, *on a l'identité suivante*:

$$d!X + \frac{(d-1)d!}{2} = \sum_{h=0}^{d-1} (-1)^{d-1-h} \binom{d-1}{h} (X+h)^d, \tag{8.2.1}$$

qui peut s'écrire également sous la forme

$$d!X = \sum_{h=0}^{d-1} (-1)^{d-1-h} \binom{d-1}{h} [(X+h)^d - h^d]. \tag{8.2.2}$$

L'identité (8.2.1) se trouve dans [10] (théorème 402); quant à l'identité (8.2.2), on peut la déduire de (8.2.1) de la façon suivante: dans (8.2.1), on fait $X = 0$, et on retranche membre à membre de (8.2.1) l'égalité ainsi obtenue.

COROLLAIRE (8.3). *Soient A un anneau et d un entier $\geqslant 1$. On a l'inclusion suivante:*

$$d!A \subset A_d.$$

THÉORÈME (8.4). *Soient p un nombre premier, t un entier $\geqslant 1$, et désignons par m l'entier p^t-1. Soient d'autre part $F = \boldsymbol{F}_p$ le corps fini à p éléments, $U_1, U_2, \ldots, U_{m-1}, X$ des indéterminées, $L = F(U)$ le corps des fractions rationnelles en $U = (U_1, U_2, \ldots, U_{m-1})$ à coefficients dans F, et $B = L[X]$ l'anneau des polynômes en X à coefficients dans le corps L. Il existe alors un entier $h = h(p, t)$, des coefficients $e_1 = \pm 1$, $e_2 = \pm 1$, $\ldots, e_h = \pm 1$, et, dans B, des éléments $P_1(U, X), P_2(U, X), \ldots, P_h(U, X)$, de dénominateur commun*

$$U_1 U_2 \ldots U_{m-1} \prod_{i<j} (U_i^m - U_j^m),$$

le tout satisfaisant à l'identité suivante:

$$X = e_1[P_1(U, X)]^m + e_2[P_2(U, X)]^m + \ldots + e_h[P_h(U, X)]^m.$$

Démonstration. Considérons le système linéaire de $m-1$ équations à $m-1$ inconnues $Z_1, Z_2, \ldots, Z_{m-1}$ ayant pour j-ième équation

$$\binom{m}{1} U_j^{m(m-1)} Z_1 + \binom{m}{2} U_j^{m(m-2)} Z_2 + \ldots + \binom{m}{m-1} U_j^m Z_{m-1} = (U_j^m + X)^m - U_j^{m^2} - X^m.$$

Soit B_m (resp. L_m) le sous-anneau de B (resp. L) engendré par les puissances m-ièmes des éléments de B (resp. L); les coefficients du système linéaire envisagé sont dans L_m, et les seconds membres dans B_m. Le déterminant D du système se calcule facilement:

$$D = \binom{m}{1}\binom{m}{2} \ldots \binom{m}{m-1} (U_1 U_2 \ldots U_{m-1})^m \prod_{i<j} (U_i^m - U_j^m)$$

(c'est à peu de chose près un déterminant de Vandermonde). Mais $D \neq 0$: il suffit pour le prouver de montrer que dans F, aucun des coefficients binomiaux $\binom{m}{i}$ n'est nul, ou encore que dans l'anneau local $\boldsymbol{Z}_p$, tous les $\binom{m}{i}$ sont inversibles, ce qui résulte immédiatement de la formule

$$\binom{m}{i} = \frac{m(m-1)\ldots(m-i+1)}{1 \cdot 2 \cdot \ldots \cdot i}$$

et du fait que $m = p^t - 1$. Le système envisagé est donc un système de Cramer à coefficients dans B_m, et à déterminant non nul dans L_m, donc inversible dans B_m. Ce système admet dans B_m une solution et une seule, et il est immédiat que cette solution est:

$$Z_1 = X,\ Z_2 = X^2,\ \ldots,\ Z_{m-1} = X^{m-1}.$$

De là $X \in B_m$, ce qui équivaut à l'existence d'une identité telle que celle de l'énoncé, sans toutefois la précision relative au dénominateur commun: cette précision résulte de la formule de Cramer explicite

$$X = Z_1 = D_1 D^{-1}$$

et de la valeur de D donnée plus haut. Le théorème est ainsi démontré.

Le théorème (8.4) est utilisé au chapitre 2 et au chapitre 7 pour l'étude des sommes de puissances d-ièmes dans des corps quelconques. L'idée de mettre ce théorème en évidence et la méthode de démonstration proposée ici nous ont été suggérées par un article de Tornheim ([26], théorème 2). Toutefois, Tornheim, qui étudie des sommes de puissances d-ièmes dans des corps de caractéristique $p > 0$, n'obtient de résultats qu'en supposant l'existence d'une relation entre d et p ($d < p$, ou $p \nmid d$) ou bien en supposant le corps parfait. Le théorème (8.4) permet au contraire d'obtenir des résultats complets sans faire aucune hypothèse de ce genre, et par conséquent d'éliminer tous les ennuis dus à la caractéristique.

Bibliographie

[1] E. Artin, *Ueber die Zerlegung definiter Funktionen in Quadrate*, Hamb. Abh. 5 (1927), p. 100–115.

[2] P.T. Bateman and R.M. Stemmler, *Waring's problem for algebraic number fields*, Illinois Math. Journal 6 (1962), p. 142–156.

[3] B.J. Birch, *Waring's problem for $\mathfrak{P}$-adic number fields*, Acta Arith. 9 (1964), p. 169–176.

[4] N. Bourbaki, *Algèbre*, Paris.

[5] — *Algèbre commutative*, Paris 1961.

[6] J. Cassels, *Representation of rational functions as sums of squares*, Colloque C.N.R.S. (Clermont, 1964), p. 55–65.

[7] C. Chevalley, *Démonstration d'une hypothèse de M. Emil Artin*, Abh. Math. Sem. Hansischen Universität 11, (1936), p. 73–75.

[8] H. Davenport and D.J. Lewis, *Homogeneous additive equations*, Proceedings Roy. Soc., A, 274 (1963), p. 443–460.

[9] V.B. Demyanov, *Sur la représentation de zéro par des formes du type $\sum a_i X_i^n$*, C.R. Acad. Sc. U.R.S.S. 105 (1956), p. 203–205.

[10] G.H. Hardy and E.M. Wright, *The theory of numbers*, Oxford 1960.

[11] F. Hausdorff, *Zur Hilbertsche Lösung des Waringschen Problems*, Math. Annalen 67 (1909), p. 301–305.

[12] D. Hilbert, *Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen*, Math. Annalen 67 (1909), p. 281–300.

[13] J.R. Joly, *Groupes procycliques*, C.R. Acad. Sc. Paris 261 (1965), p. 13–16.

[14] — *Sur quelques propriétés des corps de Brauer*, C.R. Acad. Sc. Paris 261 (1965), p. 299–302 (+ Rectification).

[15] — *Sur les puissances d-ièmes des éléments d'un anneau commutatif*, C.R. Acad. Sc. Paris 261 (1965), p. 3259–3262.

[16] — *Sur le problème de Waring pour un exposant premier dans certains anneaux locaux*, C.R. Acad. Sc. Paris 262 (1966), p. 1438–1441.

[17] S. Kochen, *Ultraproducts in the theory of models*, Annals of Math. 74 (1961), p. 221–261.
[18] E. Landau, *Additive Zahlentheorie*, Cambridge Tracts (Tract 31), Cambridge 1937.
[19] S. Lang, *Algebraic numbers*, New York 1964.
[20] M. Nagata, *Local Rings*, New York 1962.
[21] O.T. O'Meara, *Introduction to Quadratic Forms*, Berlin 1963.
[22] L.G. Peck, *Diophantine equations in algebraic number fields*, Amer. J. Math. 71 (1949), p. 387–402.
[23] C.P. Ramanujam, *Sums of m-th powers in $\mathfrak{P}$-adic rings*, Mathematika 10 (1963), p. 137–146.
[24] J.P. Serre, *Corps Locaux*, Paris 1962.
[25] R.M. Stemmler, *The easier Waring Problem in algebraic number fields*, Acta Arith. 6 (1961), p. 447–468.
[26] L. Tornheim, *Sums of n-th powers in fields of prime characteristic*, Duke Math. J. 4 (1938), p. 359–362.
[27] G. Whaples, *Galois cohomology of additive polynomials and n-th power mapping of fields*, Duke Math. J. 24 (1957), p. 143–150.
[28] O. Zariski and P. Samuel, *Commutative Algebra*, New York.

Addendum: j'ajoute à cette bibiographie la mention de l'article suivant que vient de une signaler Monsieur Schinzel:

W. J. Ellison, *A "Waring's Problem" for homogeneous forms*, Proc. Comb. Phil. Soc. 65 (1969), p. 663-672.

FACULTÉ DES SCIENCES DE GRENOBLE
INSTITUT DE MATHÉMATIQUES PURES

Reçu le 15.5.1969

ACTA ARITHMETICA
XVII (1970)

Caractérisation des ensembles normaux dans Z

par

F. Dress et M. Mendès France (Bordeaux)

"Art is the Tree of Life
Science is the Tree of Death."
William Blake

1. Introduction. On rappelle que si $\Lambda = (\lambda_n)$ est une suite infinie de nombres réels, on dit que $x \in \boldsymbol{R}$ est Λ-normal si la suite $x\Lambda$ est équirépartie (mod 1). On note $B(\Lambda)$ l'ensemble des nombres Λ-normaux, et l'on dit qu'un ensemble $E \subset \boldsymbol{R}$ est un ensemble normal s'il existe une suite Λ telle que $E = B(\Lambda)$. Une intersection dénombrable d'ensembles normaux s'appelle un ensemble normal au sens large.

Il est clair qu'un ensemble E normal (resp. normal au sens large) satisfait aux conditions suivantes:

(i) $0 \notin E$;

(ii) Pour tout $q \in \boldsymbol{Z}^* = \boldsymbol{Z} - \{0\}$, on a $qE \subset E$;

(iii) E est mesurable au sens de Borel.

Savoir si ces conditions sont suffisantes semble être un problème difficile. Nous l'avons résolu dans le cas où E est un sous-ensemble de $\boldsymbol{Z}^*$ (il en existe!) grâce à une idée de D. Cantor (communication privée).

2. Résultat obtenu. Soit $m \in \boldsymbol{Z}$. On désigne par $D(m)$ l'ensemble des diviseurs de m ($m \neq 0$), et on pose $D(0) = \emptyset$. On démontre alors le théorème suivant:

Théorème. *Soit B un sous-ensemble de $\boldsymbol{Z}^*$. Les conditions suivantes sont équivalentes*:

(1) *B est normal au sens large*;

(2) *B est normal*;

(3) *Pour tout $q \in \boldsymbol{Z}^*$, on a $qB \subset B$*;

(4) *Il existe une suite infinie (m_n) de nombres entiers, telle que*

$$B = \bigcap_{n=1}^{\infty} \left(\boldsymbol{Z}^* - D(m_n)\right)$$