JEAN-PAUL CAHEN

Polynômes à valeurs entières

Thèses d'Orsay, 1973

<http://www.numdam.org/item?id=BJHTUP11_1973__0016__P0_0>

ORSAY

T H E S E

Présentée

A l'UNIVERSITE DE PARIS-SUD
CENTRE D'ORSAY

pour obtenir

LE GRADE DE DOCTEUR ES SCIENCES MATHEMATIQUES

par

Jean Paul CAHEN

1ere THESE : "POLYNOMES A VALEURS ENTIERES"
2ème THESE : ENSEMBLES DE HELSON et de MULTIPLICITE

Soutenues le 8 juin 1973 devant la Commission d'examen

JURY : MM. P. SAMUEL Président
D. LAZARD ....
M. LAZARD..... Examinateurs
Y. MEYRR.....

INTRODUCTION

Le polynôme $\frac{1}{2}X(X-1)$ n'est pas à coefficients entiers, mais pour tout élément z de $\mathbb{Z}$, $\frac{1}{2}z(z-1)$ est un entier ; disons que ce polynôme est à valeurs entières. On a pu rencontrer l'exercice (élémentaire) où l'on montre que l'ensemble $\mathbb{Z}_S$ des polynômes à valeurs entières est un $\mathbb{Z}$-module libre et qu'une base en est la suite des polynômes $\binom{X}{n} = \frac{1}{n!}(X)(X-1)\ldots(X-n+1)$. Sur tout domaine d'intégrité A de corps des fractions K, on peut définir les polynômes P à valeurs entières par la propriété $P \in K[X]$, $P(A) \subseteq A$; ils forment bien sûr un anneau que l'on note A_S et $A[X] \subset A_S \subset K[X]$. Dans un passé relativement lointain, en 1919, G. Polya et A. Ostrowski (voir bibliographie) ont établi des conditions pour que, sur l'anneau des entiers d'un corps de nombres, les polynômes à valeurs entières forment encore un module libre avec une base "régulière", c'est-à-dire formée de polynômes de degré croissant. Ceci et cela mis à part, il me semble que la littérature était restée assez discrète autour de ce sujet.

Avec un camarade, Jean-Luc Chabert, nous avons d'abord considéré la question d'un point de vue souvent cher aux mathematiciens : traiter le problème par sa disparition. Nous avons tenté de caractériser les domaines d'intégrité sur lesquels tout polynôme à valeurs entières est à coefficients dans A, soit $A_S = A[X]$. Nous les avons baptisés

anneaux substitutiels. La fermeture intégrale de $\mathbb{Z}$ dans la clôture algébrique de $\mathbb{Q}$ en est un exemple. Pour cela nous avons cherché sur quels A-modules M le polynôme 0 est le seul polynôme à coefficients dans M partout nul sur A. Nous les avons baptisés modules sans torsion polynomiale. Les résultats - Si A est un anneau noetherien, M est sans torsion polynomiale si et seulement si tout idéal premier de son Assassin a un corps résiduel infini. Un domaine d'intégrité noetherien et intégralement clos est substitutiel si et seulement si ses idéaux premiers de hauteur 1 ont tous un corps résiduel infini ... - figurent dans une thèse de troisième cycle commune. Ils sont repris dans un article au Bulletin des Sciences Mathématiques ([Cah. & Cha] dans la bibliographie) qui les complète de résultats nouveaux sur la localisation.

Cet article est le sujet de ma première partie. Mais l'exposition est ici entièrement différente : je remarque que les modules sans torsion polynomiale forment bien la classe des modules libres d'une théorie de torsion, ce qui permet de faire rentrer cette étude dans un cadre plus général. En fait l'objet de cette première partie (ou j'omets les preuves de [Cah. & Cha]) est aussi d'exposer des résultats originaux sur les théories de torsion en algèbre commutative :

- rôle général de l'assassin pour déterminer si un module est "libre" ou sans torsion (chapitre I)
- relation entre dimension dominante [H.H.Storrer] et profondeur au sens classique (chapitre II).

Je donne les démonstrations dans le cadre de la torsion poly-

nomiale, mais sans perte de généralités car leur principe reste celui du cas général (que j'ai développé dans deux publications [(P.J.C. (1)] et [P.J.C. (2)]).

Enfin, cette approche permet de généraliser la notion d'anneau substitutiel au cas non intègre : il s'agit des anneaux sans torsion et divisibles [J. Lambek] pour la théorie de torsion polynomiale. On arrive à la caractérisation, légèrement améliorée : Un anneau noetherien et semi-normal est substitutiel si et seulement si tous ses idéaux premiers de hauteur 0 ou 1 ont un corps résiduel infini.

Pour cette raison, j'ai voulu aussi construire un exemple simple d'anneau noetherien factoriel, de dimension n quelconque mais avec un idéal premier de hauteur 1 de corps résiduel fini (chapitre III, §4).

Dans une deuxième partie, j'ai exposé les travaux de G. Polya et A. Ostrowski de façon moderne. Je les ai également un peu généralisés et j'ai montré que, pour tout anneau de Dedekind, l'anneau A_S des polynômes à valeurs entières est un A-module projectif qu'on peut décomposer en somme d'idéaux fractionnaires de A, selon une suite de polynômes de degré croissant. Le résultat vaut encore dans le cas de plusieurs variables (chapitre IV). Ces idéaux fractionnaires caractéristiques apparaissent déjà dans l'article de G. Polya : il montre précisément que A_S est libre avec une base "régulière" si et seulement si ces idéaux sont principaux. A. Ostrowski à son tour donnait une description précise de ces

idéaux pour les corps de nombres qui sont extension Galloisienne de $\mathbb{Q}$. Les classes de ces idéaux engendrent un sous-groupe $\mathcal{H}(A)$ du groupe des classes d'idéaux de A ; on peut dire que $\mathcal{H}(A)$ mesure à quel point A s'écarte d'avoir une base régulière. J'indique que $\mathcal{H}(A)$ est trivial dans le cas des corps cyclotomiques et je complète la description de $\mathcal{H}(A)$, déjà bien amorcée par G. Polya, dans le cas des corps quadratiques (chapitre V).

Enfin, Jean-Luc Chabert, le premier, a étudié et entièrement déterminé le spectre de l'anneau A_S lorsque A est un anneau de Dedekind. C'est parce que, dans le cas local (lorsque le corps résiduel est fini) les points de ce spectre au-dessus de l'idéal maximal $\mathfrak{m}$ de A sont en bijection avec les éléments du complété $\hat{A}$ de A que j'ai eu l'idée de considérer A_S comme un sous-anneau de l'anneau des fonctions continues $\mathcal{C}$ de $\hat{A}$ dans $\hat{A}$. Je montre que A_S est dense dans cet anneau $\mathcal{C}$ par application du théorème de Stone-Weierstrass ; il en résulte facilement que la fibre au-dessus de $\mathfrak{m}$ de la A-algèbre A_S est en bijection avec la fibre au-dessus de $\mathfrak{m}$ de $\mathcal{C}$, cette fibre - soit $\mathcal{C} \otimes_A \frac{A}{\mathfrak{m}}$ - s'identifie à l'anneau des fonctions localement constantes de $\hat{A}$ dans le corps $\frac{A}{\mathfrak{m}}$. Comme $\hat{A}$ est compact et totalement discontinu, le spectre de cet anneau de fonctions localement constantes est alors classique (on le trouve en exercice dans Bourbaki). C'est cette méthode de détermination du spectre que j'expose dans la troisième partie (chapitre VI). Elle permet de généraliser facilement les résultats aux polynômes à plusieurs variables et aux fractions rationnelles à valeurs entières (chapitre VII). Enfin, je

détermine quels sont les idéaux de type fini de A_S , et je calcule le groupe de Picard dans le cas local. Les idéaux premiers de l'anneau $\mathbb{Z}_S$ ne sont, en particulier, jamais de type fini ; ainsi $\mathbb{Z}_S$ est-il un exemple assez immédiat d'anneau non noetherien.

Bien des résultats de cette thèse sont donc issus d'un travail en commun. De son côté Jean-Luc Chabert présente une thèse qui traite des mêmes problèmes et développe la théorie des anneaux de Fatou. Les deux exposés sont néanmoins tout à fait distincts et bien que quelques résultats figurent dans les deux thèses, elles diffèrent par le fond autant que par la forme. Mais même les résultats qui ne sont traités qu'ici m'ont souvent été inspirés par mon camarade et je tiens à le remercier pour son aide continue ; de mon côté, j'ai participé avec plaisir à l'élaboration de son travail.

Je tiens à remercier chaleureusement mon professeur et directeur de thèse, M. Pierre Samuel qui nous a encouragé avec tant de compréhension à travailler en commun tout en nous conseillant d'exploiter nos résultats dans des directions différentes. Je pense aussi à Mme V. Gautheron et Mme G. Jacob avec qui nous avions entrepris en 1968 un petit groupe de travail. Il est à l'origine de cette thèse et c'est un bon souvenir.

AVERTISSEMENT : Le lecteur aura sans doute déjà deviné qu'ici tout anneau est commutatif et unitaire.

PREMIÈRE PARTIE :

TORSION POLYNOMIALE

CHAPITRE I - THÉORIES DE TORSION

§ 1. MODULES SANS TORSION POLYNOMIALE.

Si A est un anneau et M un A-module, on note $M[X]$ l'ensemble des polynômes formels à coefficients dans M. Un élément P de $M[X]$ est de la forme $P = p_0 + p_1 X + \ldots + p_n X^n$, où les $p_i \in M$. $M[X]$ est, de façon évidente, un $A[X]$-module et aussi un A-module (on peut dire par restriction des scalaires).

Si $P \in M[X]$ et $a \in A$, on peut calculer la valeur de P en a, soit

$$P(a) = p_0 + p_1 a + \ldots + p_n a^n ,$$

c'est un élément de M. Si $P(a) = 0$, $\forall a \in A$, on dit que P est partout nul. C'est le cas du polynôme $X^2 - X$ à coefficients dans le $\mathbb{Z}$-module $\mathbb{Z} / 2\mathbb{Z}$.

On note $X_0(M)$ l'ensemble des polynômes partout nuls

à coefficients dans M. $X_0(M)$ est un sous - A[X]-module de M[X].

Définition 1.1. *Soit* A *un anneau et* M *un* A-*module. Si* $X_0(M) = 0$ *on dit que* M *est un* A-*module sans torsion polynomiale, ou, en abrégé, un* A-*module* s.t.P. [Cah. & Cha. §1].

Les modules s.t.P. sont en effet les modules libres d'une théorie de torsion sur A, puisque on peut montrer facilement

Proposition 1.2. *Soit* A *un anneau. Alors*

a) tout sous module d'un module s.t.P. *est encore* s.t.P.

b) si $0 \to N \to M \to P \to 0$ *est une suite exacte de* A-*modules où* N *et* P *sont* s.t.P. , *alors* M *est* s.t.P.

c) tout produit direct de modules s.t.P. *est un module* s.t.P.

d) toute extension essentielle d'un A-*module* s.t.P. *est encore* s.t.P.

On rappelle [J.Lambek : chapitre 0] qu'une théorie de torsion sur un anneau A est la donnée d'une classe de modules sans torsion ou modules libres et d'une classe de modules de torsion qui se comportent axiomatiquement à la manière de ces mêmes classes, dans leur sens ordinaire, sur un domaine d'intégrité. Ainsi :

1.3. a) Tout sous-module d'un module libre est encore libre.

b) Si $0 \to N \to M \to P \to 0$ est une suite exacte où N et P sont libres, alors M est libre.

c) Tout produit direct de module libres est un module libre.

d) Toute extension essentielle d'un module libre est encore libre.

Egalement :

e) Si $0 \to N \to M \to P \to 0$ est une suite exacte, alors M est un module de torsion si et seulement si il en est de même de N et de P.

f) Toute somme directe de modules de torsion est un module de torsion.

Enfin :

g) Un module F est sans torsion si et seulement si pour tout module de torsion T, $\mathrm{Hom}_A(T,F) = 0$.

h) Un module T est un module de torsion si et seulement si pour tout module sans torsion F, $\mathrm{Hom}_A(T,F) = 0$.

1.3. i) Il existe un radical de torsion T, $T(M)$ est le plus grand sous-module de M qui soit de torsion et alors $\frac{M}{T(M)}$ est sans torsion. On parlera donc ici de la théorie de torsion polynomiale, dont les modules libres sont les modules s.t.P., les modules de torsion seront appelés modules de P-torsion. On parlera du radical de P-torsion.

On pourrait penser aux polynômes à plusieurs variables, mais on obtiendrait la même théorie :

Proposition 1.4. *Soit A un anneau et M un A-module. Alors les propositions suivantes sont équivalentes :*

i) M *est* s.t.P.

ii) Pour tout ensemble d'indices I, le polynôme 0 est le seul polynôme de $M[X_i]_{i\in I}$, nul en tout élément de $A^{(I)}$.

iii) *Le polynôme* 0 *est le seul polynôme de* M[X], *nul en tout élément de* A *sauf peut-être un nombre fini.*

§ 2. PARTITION DU SPECTRE.

Lorsque A est un anneau commutatif, l'étude d'une théorie de torsion sur A est beaucoup simplifiée par l'utilisation du spectre premier [P.J.C. (1)]. On note $\mathrm{Ass}_A(M)$ l'assassin (faible) d'un A-module M, et $\underline{\underline{\mathrm{Ass}}}_A(M)$ l'assassin (fort) (c'est-à-dire l'ensemble des idéaux premiers de A qui sont exactement l'annulateur d'un élément de M). Bien sûr $\underline{\underline{\mathrm{Ass}}}_A(M) \subset \mathrm{Ass}_A(M)$ et les deux notions coïncident sur un anneau Noethérien. On note $\mathrm{Supp}_A(M)$ le support de M.

Proposition 2.1. *Soit* A *un anneau muni d'une théorie de torsion et* M *un* A*-module.*

i) *Si* $\forall \wp \in \mathrm{Ass}_A(M)$, $A/\wp$ *n'est pas un module de torsion, alors* M *est sans-torsion.*

ii) *Si* M *est sans-torsion, alors* $\forall \wp \in \underline{\underline{\mathrm{Ass}}}_A(M)$, $A/\wp$ *est sans-torsion.*

Preuve : i) Si M n'était pas sans-torsion, on trouverait $x \neq 0$ dans le radical de torsion T(M). On aurait $\frac{A}{\mathrm{ann}(x)} \cong Ax \subset T(M)$ et $\frac{A}{\mathrm{ann}(x)}$ serait un A-module de torsion. Si $\wp$ était un idéal premier minimal de ann(x), $\wp$ serait dans $\mathrm{Ass}_A(M)$ et $A/\wp$ serait un quotient de $\frac{A}{\mathrm{ann}(x)}$, donc aussi un module de torsion.

ii) Si M est sans torsion et si $\mathfrak{p} = \mathrm{ann}(x)$, alors $A/\mathfrak{p} \cong Ax \subset M$, donc $A/\mathfrak{p}$ est sans-torsion. [cf. 1.3.a) et 1.3.e)].

Corollaire 2.2. *Soit A un anneau muni d'une théorie de torsion et $\mathfrak{p}$ un idéal premier de A. Alors $A/\mathfrak{p}$ est ou bien un A-module de torsion ou bien un A-module sans torsion.*

Preuve : $\underline{\underline{\mathrm{Ass}}}_A(A/\mathfrak{p}) = \mathrm{Ass}_A(A/\mathfrak{p}) = \{\mathfrak{p}\}$.
Ou encore, $\forall x \neq 0 \in A/\mathfrak{p}$, $Ax \cong A/\mathfrak{p}$.

Théorème 2.3. *1) Toute théorie de torsion sur un anneau A détermine une partition de* Spec A *en deux parties $\mathbb{T}$ et $\mathbb{F}$. $\mathbb{T}$ est stable par spécialisation, $\mathbb{F}$ par générisation.*

2) Si $\mathrm{Ass}_A(M) \subset \mathbb{F}$, M est sans torsion.

3) Si M est sans torsion, $\underline{\underline{\mathrm{Ass}}}_A(M) \subset \mathbb{F}$.

4) Si M est un module de torsion, $\mathrm{Supp}_A(M) \subset \mathbb{T}$.

1) Résulte du corollaire 2.2. si $\mathbb{T}$ désigne l'ensemble des idéaux premiers $\mathfrak{p}$ tels que $A/\mathfrak{p}$ soit un module de torsion. Si alors $\mathfrak{p} \subset \mathfrak{q}$, $A/\mathfrak{q}$ est un quotient de $A/\mathfrak{p}$ et aussi un module de torsion. 2) et 3) reformulent la proposition 2.1. 4) Si $\mathfrak{p} \in \mathrm{Supp}_A(M)$ alors $M_{\mathfrak{p}}$ n'est pas nul, et si $\mathfrak{q} \in \mathrm{Ass}_A(M_{\mathfrak{p}})$ alors $\mathfrak{q} \subset \mathfrak{p}$. Si de plus $\mathfrak{p} \in \mathbb{F}$, alors $\mathrm{Ass}_A(M_{\mathfrak{p}}) \subset \mathbb{F}$, puisque $\mathbb{F}$ est stable par générisation, $M_{\mathfrak{p}}$ est sans torsion, et l'injection canonique $M \to M_{\mathfrak{p}}$ est un élément non nul de $\mathrm{Hom}_A(M, M_{\mathfrak{p}})$. M ne saurait donc être un module de torsion [cf. 1.3.h)].

Remarque : Inversement, on peut montrer qu'à toute partition de Spec A

en deux parties $\mathbb{T}$ et $\mathbb{F}$, telles que $\mathbb{T}$ soit stable par spécialisation, correspond au moins une théorie de torsion et parfois plusieurs [P.J.C. (1)].

Corollaire 2.4. *Soit* A *un anneau Noethérien muni d'une théorie de torsion,* $(\mathbb{T}, \mathbb{F})$ *la partition correspondante de* Spec A *et* M *un* A*-module. Alors*

1) M *est sans torsion si et seulement si* $\mathrm{Ass}_A(M) \subset \mathbb{F}$

2) M *est un module de torsion si et seulement si* $\mathrm{Ass}_A(M) \subset \mathbb{T}$.

Preuve : 1) Parce que $\mathrm{Ass}_A(M) = \underline{\mathrm{Ass}}_A(M)$.

2) Comme $\mathrm{Supp}_A(M)$ est la spécialisation de $\mathrm{Ass}_A(M)$, $\mathrm{Ass}_A(M) \subset \mathbb{T}$ est équivalent à $\mathrm{Supp}_A(M) \subset \mathbb{T}$. Si donc M est un A-module de torsion, $\mathrm{Ass}_A(M) \subset \mathrm{Supp}_A(M) \subset \mathbb{T}$ d'après le théorème 2.3. Inversement, si $\mathrm{Supp}_A(M) \subset \mathbb{T}$, si X est sans torsion (donc $\mathrm{Ass}_A(X) \subset \mathbb{F}$), et si $\varphi \in \mathrm{Hom}_A(M,X)$, on note $\mathrm{Ker}\,\varphi$ le noyau de φ. On a alors

$$\mathrm{Ass}_A\left(\frac{M}{\mathrm{Ker}\,\varphi}\right) \subset \mathrm{Supp}_A\left(\frac{M}{\mathrm{Ker}\,\varphi}\right) \subset \mathrm{Supp}_A(M) \subset \mathbb{T}$$

et puisque $\frac{M}{\mathrm{Ker}\,\varphi}$ s'injecte dans X,

$$\mathrm{Ass}_A\left(\frac{M}{\mathrm{Ker}\,\varphi}\right) \subset \mathrm{Ass}_A(X) \subset \mathbb{F}$$

donc $\mathrm{Ass}_A\left(\frac{M}{\mathrm{Ker}\,\varphi}\right) \subset \mathbb{T} \cap \mathbb{F} = \emptyset$ et $\frac{M}{\mathrm{Ker}\,\varphi} = 0$, d'où $\varphi = 0$ et $\mathrm{Hom}_A(M,X) = 0$. Comme c'est vrai pour tout X, M est un module de torsion [cf. 1.3.h)].

On revient maintenant au cas particulier de la torsion polynomiale. Il nous faut déterminer la partition du spectre.

Proposition 2.5. *Soit* A *un anneau. Les idéaux premiers* $\wp$ *de* Spec A *tels que* $A/\wp$ *soit un* A*-module de* P*-torsion, sont les idéaux premiers de corps résiduel fini. Ils sont tous maximaux.*

Preuve : [Cah. & Cha.] . On voit aisément que $A/\wp$ est un A-module de P-torsion si et seulement si c'est un $A/\wp$-module de P-torsion. Si $A/\wp$ est un corps fini, il est clair qu'il n'est pas s.t.P.; si au contraire, il est de cardinal infini, il est s.t.P., car tout polynôme non nul a au plus un nombre fini de racines, égal à son degré.

Par la suite, si A est un anneau, $\mathbb{T}$ désigne l'ensemble des idéaux premiers de corps résiduels finis, $\mathbb{F}$ l'ensemble des idéaux premiers de corps résiduels infinis. On peut alors appliquer le théorème 2.3. à la torsion polynomiale. On peut ajouter au sujet des modules de P-torsion, la

Proposition 2.6. *Soit* A *un anneau Noethérien et* M *un* A*-module. Alors les assertions suivantes sont équivalentes :*

i) M *est un module de* P*-torsion.*

ii) $\forall x \in M$, $\frac{A}{\mathrm{ann}(x)}$ *est un anneau de cardinal fini.*

Preuve : M est un A-module de P-torsion si et seulement si $\forall x \in M$, $\frac{A}{\mathrm{ann}(x)}$ est un module de P-torsion, c'est-à-dire $\mathrm{Supp}(\frac{A}{\mathrm{ann}(x)}) \subset \mathbb{T}$; tout idéal premier contenant $\mathrm{ann}(x)$ est de corps résiduel fini , et en particulier maximal ; ainsi $\frac{A}{\mathrm{ann}(x)}$ est artinien (car forcément déjà Noethérien), et donc fini.

On a aussi immédiatement

Proposition 2.7. *Soit* A *un anneau. Alors tout* A*-module est* s.t.P. *si et seulement si tout idéal premier de* A *a un corps résiduel infini.* [*Cah. & Cha.*] .

Proposition 2.8. *Soit* A *un anneau intègre de cardinal infini et* M *un* A*-module sans torsion, alors* M *est* s.t.P.

Preuve : Si M est sans torsion au sens classique, alors $Ass_A(M) = (0)$ et $\frac{A}{(0)}$ est de cardinal infini [J.Aczel].

On peut dire que la théorie de torsion polynomiale est plus fine que la théorie classique, ou plus petite [J.Lambek]. Si A est de cardinal fini, au contraire, tout A-module est bien sûr un module de P-torsion.

§ 3. LOCALISATION.

Proposition 3.1. *Soit* A *un anneau muni d'une théorie de torsion,* M *un* A*-module de torsion et* S *une partie multiplicative de* A *, alors* $S^{-1}M$ *est un* A*-module de torsion.*

Preuve : Si $x \in S^{-1}M$, on peut écrire $x = \frac{m}{s}$ où $m \in M$ et $s \in S$ et $ann_A(x) \supset ann_A(m)$; ainsi Ax est un quotient de Am. Si donc M est un A-module de torsion, il en est de même de tout sous-module Am , $m \in M$ et de tout sous module Ax , $x \in S^{-1}M$, de $S^{-1}M$.

Les modules de torsion se comportent donc bien par localisation. Par contre, il n'en est pas de même des modules sans torsion,

ou des modules s.t.P. en particulier.

Exemple : Soit B l'anneau des fonctions localement constantes du corps des entiers p-adiques $\mathbb{Q}_p$ dans la clôture algébrique $\overline{k}$ d'un corps fini k. Soit A le sous anneau de B, formé des fonctions f telles que $f(0) \in k$. Il est facile de voir que A est un A-module s.t.P. : Si $P = f_0 + f_1 X + \ldots + f_n X^n \in A[X]$ et $P \neq 0$, $\exists x \in \mathbb{Q}_p$, $x \neq 0$, tel que $P_x = f_0(x) + f_1(x) X + \ldots + f_n(x) X^n \in \overline{k}[X]$ et $P_x \neq 0$ (car les f_i sont localement constantes). On trouve donc α dans $\overline{k}$ qui ne soit pas racine de P_x, et on trouve aussi une fonction g telle que $g(0) = 0 \in k$, et $g(x) = \alpha$. Ainsi $P(g) \neq 0$. Par contre, si $\mathfrak{p}_0$ désigne l'idéal premier de A, $\mathfrak{p}_0 = \{f \in A \mid f(0) = 0\}$, alors $A_{\mathfrak{p}_0} \cong A/\mathfrak{p}_0 = k$ et c'est clairement un A-module de P-torsion.

On peut néanmoins établir le

Théorème 3.2. *Soit* $u : A \to B$ *un épimorphisme plat d'anneaux,* M *un* B*-module et* P *un polynôme à coefficients dans* M *tel que* $P(A) = 0$, *alors* $P(B) = 0$. [*Cah & Cha. §3. Corollaire 2*].

En particulier :

Corollaire 3.3. *Soit* A *un anneau,* M *un* A*-module, et* S *une partie multiplicative de* A. *Si* $P \in M[X]$ *est partout nul sur* A, *son image dans* $S^{-1}M[X]$ *est partout nulle sur* $S^{-1}A$.

Preuve : L'image de P est encore partout nulle sur A et $A \to S^{-1}A$ est un épimorphisme plat. [Cah. & Cha. proposition 4].

Si $\varphi : A \to B$ est un morphisme d'anneaux, on peut en général définir l'image directe, d'une théorie de torsion sur A, comme étant la théorie de torsion sur B dont les modules de torsion (resp. sans torsion) sont les modules qui, par restriction des scalaires, sont des modules de torsion (resp. sans torsion) sur A. [P.J.C. (2)]. On tire facilement du théorème 3.2., le

Corollaire 3.4. *Soit* $u : A \to B$ *un épimorphisme plat d'anneaux. L'image directe de la théorie de torsion polynomiale sur* A *est la théorie de torsion polynomiale sur* B.

Si A est Noethérien, et si $(S^{-1}X_0)(S^{-1}M)$ est le sous-module de $S^{-1}M[X]$ formé des polynômes partout nuls, sur $S^{-1}A$, on a de façon précise :

Proposition 3.5. *Soit* A *un anneau Noethérien,* M *un* A*-module et* S *une partie multiplicative de* A, *on a alors dans* $S^{-1}M[X]$,

$$S^{-1}[X_0(M)] = X_0(S^{-1}M) = (S^{-1}X_0)(S^{-1}M)$$

Preuve : Evidemment $X_0(S^{-1}M) \subset (S^{-1}X_0)(S^{-1}M)$ et d'après le théorème 3.2., il y a même égalité (si P est nul sur A, il est nul sur $S^{-1}A$). D'après le corollaire 3.3., aussi, $S^{-1}[X_0(M)] \subset (S^{-1}X_0)(S^{-1}M)$. Maintenant, si $P \in S^{-1}M[X]$ et si $P(S^{-1}A) = 0$ écrivons

$P = \frac{p_0}{t} + \frac{p_1}{t} X + \ldots + \frac{p_n}{t^n} X^n$ où les $p_i \in M$, et $t \in S$. On note alors Q le polynôme $p_0 + p_1 X + \ldots + p_n X^n$ de $M[X]$; par hypothèse, $\forall \alpha \in A$, $P(\alpha) = 0$ dans $S^{-1}M$, donc $\exists s_\alpha \in S$ tel que $s_\alpha Q(\alpha) = 0$ dans M. Comme A est Noethérien et que Q prend ses valeurs dans le A-module de type fini engendré par ses coefficients, le sous module de M engendré par $Q(A)$ a un nombre fini de générateurs, disons $Q(\alpha_1), Q(\alpha_2), \ldots, Q(\alpha_k)$. Posant $s = s_{\alpha_1} . s_{\alpha_2} . \ . s_{\alpha_k}$ on a donc $sQ(\alpha) = 0$, $\forall \alpha \in A$. Si $Q' = sQ$, alors $Q' \in X_0(M)$ et comme $P = \frac{Q'}{st}$, $P \in S^{-1}[X_0(M)]$.

Corollaire 3.6. *Soit* A *un anneau Noethérien,* S *une partie multiplicative de* A. *Si* M *est un* A*-module* s.t.P. *alors* $S^{-1}M$ *est un* A*-module* s.t.P. *et un* $S^{-1}A$*-module* s.t.P.

C'est clair [Cah. & Cha. §1. Corollaire 2].

CHAPITRE II - DIMENSION DOMINANTE.

§ 1. P-DIMENSION DOMINANTE.

Si A est un anneau muni d'une théorie de torsion, on peut définir la dimension dominante d'un A-module M, relative à cette théorie [H.H. Storrer]. Pour la théorie de torsion polynomiale, on pose la définition

Définition 1.1. *Soit* A *un anneau, et* M *un* A*-module. On dit que la* P*-dimension dominante de* M, *notée* $\text{P-dom.dim}_A(M)$ *est* n, *si et seulement si il existe une résolution injective de* M :

$$M \to M_0 \to M_1 \to \dots \to M_{n-1}$$

où les M_i *sont* s.t.P.

Ainsi P-dom.dim(M) est un entier n, ou bien le symbole ∞. De façon évidente :

1.2. a) $\text{P-dom.dim}_A(M) \geq 1$ si et seulement si M est s.t.P.

b) $\text{P-dom.dim}_A(M) \geq 2$ si et seulement si M est s.t.P. et le quotient $\tilde{M}/M$ (où $\tilde{M}$ est une enveloppe injective de M) est aussi s.t.P. ; c'est-à-dire M est sans torsion et divisible [J.Lambek, proposition 0.5.] pour la théorie de torsion polynomiale.

En général, le radical de torsion T est un foncteur exact à gauche dans la catégorie des A-modules. Si on note

T_0, T_1, ..., T_n, ... ses foncteurs dérivés (et $T_0 \cong T$) alors la dimension dominante d'un A-module M est aussi le plus petit entier n tel que $T_n(M)$ ne soit pas nul. Ici on va faire usage du foncteur X_0. Si, en effet, M est un A-module et $P \in X_0(M)$, et si $f : M \to N$ est un homomorphisme de A-modules, l'image $\tilde{f}(P)$ (où $\tilde{f}$ est le prolongement canonique de f aux modules de polynômes) est bien sûr un polynôme partout nul, à coefficients dans N. Ainsi X_0 peut être considéré comme un foncteur de la catégorie des A-modules dans elle-même.

Proposition 1.3. *Soit* A *un anneau. Alors le foncteur* X_0 *est exact à gauche.*

Si $0 \to N \xrightarrow{f} M \xrightarrow{g} P$ est une suite exacte, la suite, qui s'en déduit canoniquement, $0 \to N[X] \xrightarrow{\tilde{f}} M[X] \xrightarrow{\tilde{g}} P[X]$, est bien sûr encore exacte. La restriction de $\tilde{f}$ à $X_0(N)$ est encore injective, et puisque $\tilde{g} \circ \tilde{f} = 0$ la restriction de $\tilde{g} \circ \tilde{f}$ à $X_0(N)$ est encore nulle. Si maintenant $P \in X_0(M)$, et $\tilde{g}(P) = 0$, alors $P = \tilde{f}(Q)$, où $Q \in N[X]$, et $\forall a \in A$, $f[Q(a)] = P[f(a)] = 0$, et donc $Q(a) = 0$, car f est injective ; ainsi $Q \in X_0(N)$.

On note X_1, X_2, ..., X_n, ... les foncteurs dérivés de X_0 :

Proposition 1.4. *Soit* A *un anneau et* M *un* A*-module. Alors* $\text{P-dom.dim}_A(M) \geq n$ *si et seulement si* $X_k(M) = 0$, $\forall k < n$.

Preuve : $X_0(M) \neq 0$ si et seulement si M n'est pas s.t.P. donc $P\text{-dom.dim}_A(M) = 0$ [cf.1.2.a)] . Si par contre M est s.t.P., il en est de même de son enveloppe injective $\tilde{M}$. Par ailleurs la suite exacte $0 \to M \to \tilde{M} \to \tilde{M}/M \to 0$, donne lieu à une longue suite exacte

$$0 \to X_0(M) \to X_0(\tilde{M}) \to X_0(\tilde{M}/M) \to X_1(M) \to .....$$

$$.... \to X_k(M) \to X_k(\tilde{M}) \to X_k(\tilde{M}/M) \to X_{k+1}(M) \to ....$$

On en déduit facilement que le nombre de dérivés nuls en $\tilde{M}/M$ est moindre d'une unité que celui de dérivés nuls en M ; comme il est par ailleurs évident que la dimension dominante de $\tilde{M}/M$ est celle de M moins une unité, la proposition peut se prouver sans peine par récurrence.

Remarque : De la même façon si on note $X_0^{(I)}(M)$ l'ensemble des polynômes de $M[X_i]_{i\in(I)}$ nuls en tout élément de $A^{(I)}$, le foncteur $X_0^{(I)}$ est exact à gauche et ses dérivés permettent de calculer la P-dimension dominante.

§ 2. LOCALISATION.

Dans ce paragraphe A désigne un anneau Noethérien et $\mathbb{T}$ l'ensemble des idéaux premiers de corps résiduels finis. Les résultats concernant ici la P-dimension dominante se généralisent fort bien à toute théorie de torsion [P.J.C. (2) §4.] .

Proposition 2.1. *Soit* A *un anneau Noethérien et* M *un* A*-module. Alors,*

a) $\text{P-dom.dim}_A(M) = \text{Inf}_{\wp \in \text{Spec } A} \{\text{P-dom.dim}_{A_\wp}(M_\wp)\}$.

b) $\text{P-dom.dim}_A(M) = \text{Inf}_{\wp \in \mathbb{T}} \{\text{P-dom.dim}_{A_\wp}(M_\wp)\}$.

Preuve : Si $0 \to M \to M_0 \to \ldots \to M_n \to \ldots \to$ est une résolution injective de M, alors $0 \to M_\wp \to (M_0)_\wp \to \ldots \to (M_n)_\wp \to \ldots$ est aussi une résolution injective du $A_\wp$-module $M_\wp$, car A est Noethérien. De plus, si $(X_\wp)_0(M_\wp)$ dénote l'ensemble des polynômes partout nuls du $A_\wp$-module $M_\wp$, on a vu que $(X_\wp)_0(M_\wp) \cong [X_0(M)]_\wp$ [cf. I, proposition 3.5.] . On en conclut facilement que $(X_\wp)_n(M_\wp) \cong [X_n(M)]_\wp$ pour tout n. Ainsi $X_n(M) = 0$ si et seulement si $(X_\wp)_n(M_\wp) = 0$, $\forall \wp \in \text{Spec } A$, ce qui prouve a). Maintenant b) en résulte car si $\wp \notin \mathbb{T}$, tout $A_\wp$-module est s.t.P. [cf. I, proposition 2.7.] et donc $\text{P-dom.dim}_A(M) = \infty$.

§ 3. PROFONDEUR.

En général, si A est un anneau Noethérien et I un idéal de A, on peut toujours considérer la théorie de torsion correspondant à la partition du spectre telle que $A/\wp$ est un module de torsion si et seulement si l'idéal premier $\wp$ contient I [P.J.C. (1)]. On montre alors que la dimension dominante d'un A-module M, relative à cette théorie, est la I-profondeur du A-module M, c'est-à-dire la plus grande longueur d'une M-suite régulière dans I [P.J.C. (2), theorem 2.1].

Dans le cas de la théorie de torsion polynomiale on a en particulier

Lemme 3.1. *Soit* A *un anneau local Noethérien, d'idéal maximal* $\mathfrak{m}$ *de corps résiduel fini, et soit* M *un* A*-module de type fini. Alors* M *est s.t.P. si et seulement si il existe un élément* f_1 *de* $\mathfrak{m}$ *qui ne divise pas* 0 *dans* M .

Preuve : Comme A est Noethérien, M est s.t.P. si et seulement si $\mathfrak{m} \notin \mathrm{Ass}_A(M)$ [cf. I, corollaire 2.4. et proposition 2.5.] ($\mathfrak{m}$ est en effet le seul idéal premier de A de corps résiduel fini). Comme M est de type fini, $\mathrm{Ass}_A(M)$ est un ensemble fini et $\mathfrak{m} \notin \mathrm{Ass}_A(M)$, si et seulement si la réunion des idéaux premiers de $\mathrm{Ass}_A(M)$ est strictement incluse dans $\mathfrak{m}$, c'est-à-dire qu'il existe $f_1 \in \mathfrak{m}$, qui ne divise pas 0 dans M.

Si on note $\mathrm{Prof}_A(M)$, la profondeur d'un A-module M, on a donc la

Proposition 3.2. *Soit* A *un anneau local Noethérien, d'idéal maximal* $\mathfrak{m}$ *de corps résiduel fini, et soit* M *un* A*-module de type fini. Alors* $\text{P-dom.dim}_A(M) = \mathrm{Prof}_A(M)$.

Preuve : Par récurrence. Si $\tilde{M}$ est une enveloppe injective de M, il est clair que $\text{P-dom.dim}_A(M) = \text{P-dom.dim}(\tilde{M}/M) + 1$, et facile de voir que $\mathrm{Prof}_A(M) = \mathrm{Prof}_A(\tilde{M}/M) + 1$ puisque, si M est de type fini, $\mathrm{Prof}_A(M)$ est le plus petit indice n tel que $\mathrm{Ext}^n_A(A/\mathfrak{m}, M) \neq (0)$ [H.Matsumara, theorem 26].

Si on rapproche cette proposition de la proposition 2.1., on a donc le

Théorème 3.3. *Soit* A *un anneau Noethérien et* M *un* A*-module de type fini. Alors*

$$P\text{-dom.dim}_A(M) = \mathrm{Inf}_{\wp \in \mathbb{T}} \{\mathrm{Prof}_{A_\wp}(M_\wp)\} .$$

Remarque : La même formule s'applique à la dimension dominante relative à toute théorie de torsion. Il suffit d'y remplacer $\mathbb{T}$ par l'ensemble des idéaux premiers $\wp$ de A, tels que $A/\wp$ soit un A-module de torsion pour cette théorie [P.J.C. (2), theorem 4.4.].

§ 4. MODULES UNIVERSELLEMENT SANS TORSION POLYNOMIALE.

Si P est un élément de M[X] , le sous module (P(A)) de M, engendré par les valeurs de P sur A est bien sûr inclus dans le sous module Coef(P) engendré par les coefficients de P. On a montré dans [Cah. & Cha. proposition 3.] la

Proposition 4.1. *Soit* A *un anneau et* M *un* A*-module. Alors les assertions suivantes sont équivalentes :*

i) *Pour tout polynôme* P *de* M[X] , Coef(P) = (P(A)).

ii) $\forall \wp \in \mathrm{Supp}_A(M)$, $A/\wp$ *est de corps résiduel infini.*

iii) $\forall N \subset M$, M/N *est s.t.P.*

et posé la

Définition 4.2. *Un* A*-module* M *est dit* universellement sans torsion

polynomiale, en abrégé u.s.t.P. s'il vérifie les conditions équivalentes de la proposition 4.1.

Remarque : En général, on peut dire qu'un module M est universellement libre, relativement à une théorie de torsion si $\mathrm{Supp}_A(M) \subset \mathbb{F}$ (où $\mathbb{F}$ est l'ensemble des idéaux premiers tels que $A/\mathfrak{p}$ soit sans torsion). Aussi le résultat suivant (qui résulte facilement de la proposition 1.6. et du théorème 3.3.) se généralise sans peine.

Proposition 4.3. *Soit* A *un anneau Noethérien et* M *un* A*-module. Alors*

a) Si M *est* u.s.t.P., $\text{P-dom.dim}_A(M) = \infty$.

b) Si M *est de type fini et si* $\text{P-dom.dim}_A(M) = \infty$, M *est* u.s.t.P.

Remarque : Le $\mathbb{Z}$-module $\mathbb{Q}$ n'est pas de type fini. $\text{P-dom.dim}_{\mathbb{Z}}(\mathbb{Q}) = \infty$ mais $\mathbb{Q}$ n'est pas u.s.t.P.

CHAPITRE III - ANNEAUX SUBSTITUTIELS

§ 1. DEFINITION.

Si A est un anneau intègre fini, alors A est son propre corps de fractions K, tout polynôme P de K[X] est tel que $P(A) \subset A$. Si, au contraire, A est un anneau intègre de cardinal infini, de corps des fractions K, alors A est un A-module s.t.P. ; de plus, l'ensemble A_s des polynômes P de K[X] , tels que $P(A) \subset A$, se réduit à l'anneau des polynômes A[X] si et seulement si K/A est un A-module s.t.P. Mais K est l'enveloppe injective de A, ainsi $A_s = A[X]$, dans ce cas, si et seulement si A est sans torsion et divisible pour la théorie de torsion polynomiale [J.Lambek, proposition 0.5.] . (On peut dire aussi que A est son propre localisé, pour la localisation correspondant à la théorie de torsion polynomiale [J.Lambek, proposition 0.8.] . Ou encore que $P\text{-dom.dim}_A(A) \geq 2$ [cf. II. 1.2.b)]). On pose la

Définition 1.1. *On dit qu'un anneau* A *est substitutiel si et seulement si il est sans torsion et divisible pour la théorie de torsion polynomiale.*

On a vu que si A est intègre et substitutiel alors $A_s = A[X]$. De façon un peu plus générale

Proposition 1.3. *Soit* A *un anneau intègre substitutiel. Alors pour*

tout anneau intègre B *contenant* A, *si* P *est un polynôme à coefficients dans* B *tel que* $P(A) \subset A$, $P \in A[X]$.

[Cah. & Cha. §4.]

Remarque : A noter l'erreur dans la référence citée: Il faut supposer B intègre sinon le sous module de torsion de B/A , au sens classique ne s'injecte peut-être pas dans K/A. Si par exemple k est un corps fini, l'anneau $A = k[X,Y]$ est substitutiel et s'injecte dans le produit $k[X,Y] \times k = B$. Mais $B/A \cong k$ n'est pas un A-module s.t.P. ce qui met la proposition en défaut.

Proposition 1.3. *Soit* A *un anneau Noethérien et* Tot(A) *l'anneau total des fractions de* A. *Alors* A *est substitutiel si et seulement si* A *est s.t.P. et tout polynôme* P *de* Tot(A)[X] , *tel que* $P(A) \subset A$, *est à coefficients dans* A.

Preuve : La dernière assertion exprime que Tot(A)/A est s.t.P. Si A est substitutiel c'est bien le cas, car Tot(A) est une extension essentielle de A et s'injecte dans une enveloppe injective $\tilde{A}$ de A, $\tilde{A}/A$ est s.t.P. [J.Lambek, proposition 0.5.] . Si inversement A est s.t.P. il en est de même de son localisé Tot(A) et $Ass_A(Tot(A))$ ne contient que des idéaux premiers de corps résiduel infini. Il est facile d'en déduire que tous les idéaux premiers de Tot(A) ont un corps résiduel infini et qu'ainsi tout Tot(A)-module est s.t.P. [cf. I, proposition 2.7.] , donc que $\tilde{A}/Tot(A)$ est s.t.P. Si, de plus, Tot(A)/A est s.t.P. il en est alors de même de $\tilde{A}/A$, à cause de la suite exacte

$0 \to \mathrm{Tot}(A)/A \to \tilde{A}/A \to \tilde{A}/\mathrm{Tot}(A) \to 0$ [cf. I. 1.3.b)] .

On peut aussi caractériser les anneaux substitutiels de façon interne, à l'aide des éléments réguliers, c'est-à-dire qui ne divisent pas 0 dans A

Proposition 1.4. *Soit* A *un anneau Noethérien. Alors* A *est substitutiel si et seulement si il est s.t.P. et si* A/aA *est s.t.P. pour tout élément régulier* a *de* A.

Preuve : A est substitutiel si et seulement si $\text{P-dom.dim}_A(A) \geq 2$ [cf. II. 1.2.b)] . Soit donc a un élément régulier de A, et a* la multiplication par A (dans n'importe quel A-module). De la suite exacte $0 \to A \xrightarrow{a^*} A \to A/aA \to 0$ on tire la longue suite

$$0 \to T(A) \xrightarrow{a^*} T(A) \to T(A/aA) \to T_1(A) \xrightarrow{a^*} T_1(A) \to \ldots$$

où T est le P-radical de torsion, T_1 son premier dérivé. Si A est substitutiel alors $T(A) = T_1(A) = 0$ [cf. II. proposition 1.4. et P.J.C. (2), proposition 1.5.] , donc $T(A/aA) = 0$ et A/aA est s.t.P. Si inversement $T(A/aA) = 0$, alors a* est injective dans $T_1(A)$. Si c'est vrai pour tout élément régulier a, alors les idéaux premiers associés à $T_1(A)$ sont tous inclus dans la réunion (finie) des idéaux premiers associés à A. Ainsi chaque idéal premier associé à $T_1(A)$ est inclus dans un idéal premier associé à A. Si donc A est s.t.P. tous ces idéaux premiers ont un corps résiduel infini et $T_1(A)$ lui-même est s.t.P. Mais $T_1(A)$ est un module de P-torsion, si en effet $0 \to A \to A_0 \to A_1 \to A_2 \to \ldots$ est une résolution injective de A, $T_1(A)$

est l'homologie au rang 1 du complexe $T(A_0) \to T(A_1) \to T(A_2)$ donc un module quotient d'un sous module de $T(A_1)$. Or $T(A_1)$ est un module de torsion et la classe des modules de torsion est fermée par sous-module et module quotient. Ainsi $T_1(A) = 0$. Comme A est s.t.P., $T(A) = 0$ et donc A est substitutiel.

Corollaire 1.5. *Soit* A *un anneau substitutiel et* a *un élément régulier de* A, *alors ou bien* A/aA = (0) *(et* a *est une unité) ou bien* A/aA *est de cardinal infini.*

Preuve : La preuve de la proposition précédente montre que, même si A n'est pas Noethérien, si A est substitutiel alors A/aA est s.t.P. Mais si A/aA n'est pas nul, alors il doit bien sûr avoir un cardinal infini.

§ 2. IDEAUX PREMIERS DE HAUTEUR 1.

A est substitutiel si et seulement si $\text{P-dom.dim}_A(A) \geq 2$, et à cause de la formule

$$\text{P-dom.dim}_A(A) = \text{Inf}_{\mathfrak{p} \in \mathbb{T}} \{\text{Prof}_{A_\mathfrak{p}}(A_\mathfrak{p})\} ,$$

[cf. II, théorème 3.3.] , on a la

Proposition 2.1. *Soit* A *un anneau Noethérien. Alors* A *est substitutiel si et seulement si tout idéal premier, tel que* $\text{Prof}_{A_\mathfrak{p}}(A_\mathfrak{p}) \leq 1$, *a un corps résiduel infini.*

On en tire le critère local

Corollaire 2.2. *Soit* A *un anneau Noethérien. Alors les assertions suivantes sont équivalentes :*

i) A *est substitutiel.*

ii) Pour toute partie multiplicative S *de* A , $S^{-1}A$ *est substitutiel.*

iii) Pour tout idéal maximal $\mathfrak{M}$ *de* A, $A_{\mathfrak{M}}$ *est substitutiel.*

Remarque : Si A est intègre mais non Noethérien et si, pour tout idéal maximal $\mathfrak{M}$, $A_{\mathfrak{M}}$ est substitutiel, alors A est substitutiel. Mais A peut être substitutiel sans qu'un tel localisé ne le soit [Cah. & Cha. §4].

Corollaire 2.3. *Soit* A *un anneau Noethérien. Si* A *est substitutiel alors tout idéal premier de hauteur* 0 *ou* 1 *a un corps résiduel infini.*

Preuve : La hauteur est plus grande que la profondeur.

Si A est un anneau de Cohen Macaulay, hauteur et profondeur coincident et on a alors la réciproque à ce corollaire. De façon plus générale, on note $h(\mathfrak{p})$ la hauteur d'un idéal premier et on considère les propriétés (classiques)

(S_k) : $\mathrm{Prof}_{A_{\mathfrak{p}}}(A_{\mathfrak{p}}) \geq \mathrm{Inf}(k, h(\mathfrak{p}))$.

(R_k) : Si $h(\mathfrak{p}) \leq k$ alors $A_{\mathfrak{p}}$ est local régulier.

Un anneau Noethérien est normal si et seulement si il satisfait aux pro-

(S_2) et (R_1) [H.Matsumara : théorème 29 dit théorème de Serre].

Définition 2.4. *On dit qu'un anneau Noethérien est semi-normal s'il satisfait à la propriété* (S_2).

Proposition 2.5. *Si* A *est Noethérien et semi-normal, alors* A *est substitutiel si et seulement si tout idéal premier de hauteur* 0 *ou* 1 *a un corps résiduel infini.*

Preuve : La propriété S_2 signifie que seuls les idéaux premiers de hauteur 0 ou 1 peuvent être tels que $\mathrm{Prof}_{A_\wp}(A_\wp) \leq 1$.

§ 3. ANNEAUX INTEGRES.

Si A est un anneau intègre et Noethérien, il est semi-normal si et seulement si il est l'intersection de ses localisés en tout idéal premier de hauteur 1 [J.P. Serre III, proposition 9, Remarque] . Même si A n'est pas Noethérien, on a la

Proposition 3.1. *Soit* A *un anneau intègre de cardinal infini et intersection de ses localisés en tout idéal premier de hauteur* 1 . *Alors si tous ces idéaux ont un corps résiduel infini,* A *est substitutiel.*

Preuve. Si $\wp$ est un idéal premier de hauteur 1, tout idéal premier de $A_\wp$ a donc un corps résiduel infini, ainsi tout $A_\wp$-module est

s.t.P. [cf. I, proposition 2.7.] et $A_{\wp}$ est substitutiel. Si K est le corps des fractions de A , $K/A_{\wp}$ est un $A_{\wp}$-module s.t.P. et donc un A-module s.t.P. [cf. I, corollaire 3.4.]. Comme $A = \bigcap_{ht(\wp) = 1} A_{\wp}$, on a l'injection $0 \to K/A \to \prod_{ht(\wp) = 1} K/A_{\wp}$, et K/A est s.t.P.

Si A est Noethérien et intègre on a bien sûr le

Corollaire 3.2. *Un anneau Noethérien, intègre et semi-normal est substitutiel si et seulement si tous ses idéaux premiers de hauteur 1 ont un corps résiduel infini.*

Remarque : Un anneau de valuation de rang 1, non Noethérien, est toujours substitutiel (on le montre directement), mais peut avoir un corps résiduel fini.

Bien sûr les anneaux Noethériens intégralement clos sont semi-normaux. On peut leur appliquer le corollaire 3.2.

§ 4. DEUX EXEMPLES.

Exemple 4.1. *Un anneau intègre Noethérien de dimension 2 qui n'est pas semi-normal. Cet anneau n'est pas substitutiel mais tout idéal premier de hauteur 1 a un corps résiduel infini. Aussi, pour tout a, ou bien A/aA = (0) , ou bien A/aA est de cardinal infini.*

Soit k un corps fini, A le sous anneau de l'anneau des polynômes en deux indéterminées $B = k[u,v]$ formé des polynômes sans terme en u, sans terme en v, ni terme en uv, ainsi :

$$A = k[u^2,u^3,u^2v,uv^2,v^3,v^2] \subset B = k[u,v] .$$

A est Noethérien et intègre ; c'est une k-algèbre de type fini de dimension 2, et tout idéal premier de hauteur 1 est strictement contenu dans un idéal maximal et a un corps résiduel infini. Mais si $\mathfrak{M}$ désigne l'idéal (maximal) de A, de hauteur 2, formé des polynômes sans terme constant :

$$\mathfrak{M} = (u^2,u^3,u^2v,uv^2,v^3,v^2)$$

alors $A/\mathfrak{M}$ est fini. De plus, u^2v^2 ne divise pas u^3v^3 dans A, mais $\mathfrak{M}u^2v^2$ est inclus dans u^3v^3, ainsi $\mathfrak{M}$ annule u^3v^3 modulo u^2v^2 : $\mathfrak{M} \in \mathrm{Ass}_A(A/u^2v^2A)$. A n'est donc pas semi-normal. A n'est pas substitutiel puisque, $A/\mathfrak{M}$ étant fini, A/u^2v^2A n'est pas s.t.P. bien que u^2v^2 soit un élément régulier de A.

Exemple 4.2. *Un anneau A Noethérien et intégralement clos, de dimension $n+1$ mais avec un idéal premier $\mathfrak{P}$ de hauteur 1 tel que $A/\mathfrak{P}$ soit fini.*

- D'abord on construit une valuation discrète de $\mathbb{Q}(X_1,\ldots,X_n)$ de corps résiduel fini. On choisit un nombre premier p et on note $\mathbb{Q}_p$ le corps p-adique (complétion de $\mathbb{Q}$ pour la valuation p-adique), v_p la valuation discrète de $\mathbb{Q}_p$. On choisit n éléments $\alpha_1,\ldots,\alpha_n$ de $\mathbb{Q}_p$ qui

sont algébriquement indépendants sur $\mathbb{Q}$. Le sous corps $\mathbb{Q}(\alpha_1,\ldots,\alpha_n)$ de $\mathbb{Q}_p$ est isomorphe à $\mathbb{Q}(X_1,\ldots,X_n)$ et la restriction de v_p à $\mathbb{Q}(\alpha_1,\ldots,\alpha_n)$ définit donc une valuation discrète v de $\mathbb{Q}(X_1,\ldots,X_n)$, si on note α le n-tuple $(\alpha_1,\ldots,\alpha_n)$ on a

$$v(f/g) = v_p\ (\ f(\alpha)/g(\alpha)) \qquad \forall f/g \in \mathbb{Q}(X_1,\ldots,X_n)$$

Le corps résiduel de v est inclus dans celui de v_p, c'est donc le corps $\mathbb{F}_p$ à p éléments. On note V l'anneau de la valuation v

$$V \subset \mathbb{Q}(X_1,\ldots,X_n).$$

- Si on note S la partie multiplicative de $\mathbb{Z}$ engendrée par p :

$$S = \{p,p^2,\ldots,p^n,\ldots\}$$

alors $S^{-1}\mathbb{Z} \cong \mathbb{Z}[1/p]$. Comme V ne contient pas $1/p$, V ne contient pas $\mathbb{Z}[1/p]$ et l'intersection

$$A = \mathbb{Z}[1/p][X_1,\ldots,X_n] \cap V$$

est propre.

A est un anneau de Krull parce que c'est l'intersection de deux anneaux de Krull, et comme V intersecte $\mathbb{Z}[1/p][X_1,\ldots,X_n]$ proprement, v est une valuation essentielle de A [Bbki.VII.§1., corollaire 2]. Il y a un idéal premier $\wp$ de hauteur 1 dans A tel que $A_\wp = V$ et donc $A/\wp$ est le corps $\mathbb{F}_p$ à p-éléments.

- On peut d'ailleurs montrer directement que l'idéal pA est premier, même maximal de corps résiduel $\mathbb{F}_p$. Comme $p \in \wp$, on doit avoir $pA = \wp$. En effet, si $f \in A$, f est un polynôme à coefficients dans $\mathbb{Z}[1/p]$ et

$v(f) \geq 0$. Ainsi $f(\alpha)$ est un élément de l'anneau $\mathbb{Z}_p$ des entiers p-adiques, et il y a un entier i, $0 \leq i \leq p-1$, tel que $f(\alpha) - i$ soit dans l'idéal maximal $p\mathbb{Z}_p$ de $\mathbb{Z}_p$. Ainsi le polynôme $\frac{f-i}{p}$ est encore à coefficients dans $\mathbb{Z}[1/p]$ et $v(\frac{f-i}{p}) \geq 0$ donc $(f-i) \in p.A$. Les entiers $0,1,\ldots,i,\ldots,p-1$ forment un système de représentants de A modulo pA.

- La dimension de Krull de A est $n+1$. On choisit un premier $q \neq p$ et on considère dans $\mathbb{Z}[1/p][X_1,\ldots,X_n]$ la chaine d'idéaux :

$$(0) \subsetneq (X_1) \subsetneq (X_1,X_2) \subsetneq \ldots \subsetneq (X_1,\ldots,X_n) \subsetneq (q,X_1,\ldots,X_n)$$

par intersection avec A, elle donne une chaine d'idéaux premiers de A

$$0 \subset \mathcal{P}_1 \subset \mathcal{P}_2 \subset \ldots \subset \mathcal{P}_n \subset \mathfrak{M}$$

Maintenant il est clair que pour tout polynôme f de $\mathbb{Z}[1/p][X_1,\ldots,X_n]$ il y a un entier n tel que $p^n f \in A$, il suffit de choisir n supérieur à $-v(f)$.

Il y a donc un entier n_1 tel que $p^{n_1}X_1$ soit dans $\mathcal{P}_1$ mais pas dans (0), un entier n_2 tel que $p^{n_2}X_2$ soit dans $\mathcal{P}_2$ mais pas dans $\mathcal{P}_1$, ainsi de suite, la chaîne d'idéaux premiers de A :

$$0 \subsetneq \mathcal{P}_1 \subsetneq \mathcal{P}_2 \subsetneq \ldots \subsetneq \mathcal{P}_n \subsetneq \mathfrak{M}$$

est propre, quant à $\mathfrak{M}$ il contient q, mais q n'est pas dans $\mathcal{P}_n$ qui ne contient que des polynômes sans terme constant.

La dimension de A est exactement $(n+1)$ car A est un sous anneau de $\mathbb{Q}(X_1,\ldots,X_n)$.

- $V = A_{\mathfrak{P}}$ est Noethérien. Par ailleurs $S^{-1}A = A[1/p]$ est Noethérien car $S^{-1}A = S^{-1}(\mathbb{Z}[1/p][X_1,\ldots,X_n]) \cap S^{-1}V$ et $S^{-1}(\mathbb{Z}[1/p][X_1,\ldots,X_n]) = \mathbb{Z}[1/p][X_1,\ldots,X_n]$ car p est déjà inversible dans $S^{-1}\mathbb{Z} = \mathbb{Z}[1/p]$, et $S^{-1}V = \mathbb{Q}(X_1,\ldots,X_n)$ car $1/p$ n'est pas dans V donc $S^{-1}V$ contient strictement V.

Ainsi $S^{-1}A = (S^{-1}\mathbb{Z})[X_1,\ldots,X_n] = \mathbb{Z}[1/p][X_1,\ldots,X_n]$.

- Si $\mathfrak{M}$ est un idéal maximal de A, ou bien $p \in \mathfrak{M}$ mais alors $\mathfrak{M} = \mathfrak{p} = pA$, ou bien $\mathfrak{M}$ ne rencontre pas S. On peut dire que les deux anneaux $S^{-1}A$ et $A_{\mathfrak{P}}$ forment un "recouvrement" de A.

Comme ce recouvrement est fini, il est aisé de conclure que A est Noethérien.

- Enfin on peut montrer que A est un anneau factoriel. Il suffit de prouver que tout idéal premier de hauteur 1 est principal.

C'est vrai pour $\mathfrak{p}$, car $\mathfrak{p} = pA$. Maintenant si $\mathfrak{q}$ est un idéal premier de hauteur 1, distinct de $\mathfrak{p}$, $S^{-1}\mathfrak{q}$ est principal dans $S^{-1}A$ car $S^{-1}A$ est factoriel. En effet, $S^{-1}A$ est un localisé de l'anneau factoriel $\mathbb{Z}[X_1,\ldots,X_n]$. On trouve donc q dans A tel que $(q)S^{-1}A = S^{-1}\mathfrak{q}$. Si $v(q) = n$, qp^{-n} est encore un élément de A, et on a encore $(qp^{-n})S^{-1}A = S^{-1}\mathfrak{q}$ puisque p est inversible dans $S^{-1}A$. Mais cette fois aussi $(qp^{-n}).A_{\mathfrak{p}} = \mathfrak{q}.A_{\mathfrak{p}} = A_{\mathfrak{p}}$, donc $(qp^{-n})A = \mathfrak{q}$ et $\mathfrak{q}$ est principal engendré par qp^{-n}.

Remarque : Un résultat général de [J.Ohm] montre à quelles conditions un anneau, intersection d'anneaux de valuation discrète, est Noethérien. On peut l'appliquer à l'exemple ci-dessus. Enfin [P.Eakin] a indépendamment construit notre exemple, dans le cas de dimension 2.

DEUXIEME PARTIE :

STRUCTURE ADDITIVE

CHAPITRE IV - MODULE DES POLYNOMES A VALEURS ENTIERES.

§ 1. ANNEAU DE VALUATION DISCRETE.

Dans ce paragraphe A désigne un anneau de valuation discrète, v la valuation correspondante de son corps K, supposée normée, π une uniformisante, soit un générateur de l'idéal maximal $\mathfrak{M}$ de A, N la norme de $\mathfrak{M}$, soit le cardinal du corps résiduel $k = A/\mathfrak{M}$. En fait, si N n'est pas fini, on se contente de noter $N = \infty$. Si $P \in K[X]$, $v(P)$ désigne la plus petite des valuations des coefficients de P et $P(A)$ le sous module engendré par les valeurs de P sur A. En général tout idéal fractionnaire I de A est une puissance de l'idéal maximal $\mathfrak{M}$ de A, on note $v(I)$ cette puissance, ainsi $v(P) = v[Coef(P)]$ [cf. notations II. §4] et comme $P(A) \subset Coef(P)$, alors $v(P) \leq v[P(A)]$.

Inversement, on va établir l'existence d'une fonction $S_N(n)$ de l'entier n, qui ne dépend que de N, et telle que

$v(P) \leq v[P(A)] \leq v(P) + S_N(n)$, pour tout polynôme P de degré n. La fonction S_N limite la proportion dans laquelle K s'écarte d'un A-module u.s.t.P. [cf. II. §4] et bien sûr $S_\infty(n) = 0$, $\forall n$. On suppose donc que N est fini. La suite est alors une légère généralisation de résultats de [G.Polya] .

Soit $(a_0, a_1, \ldots, a_{n-1})$ un système de représentants de A modulo $\mathfrak{M}$, où $a_0 = 0$, on le prolonge de la façon suivante :

- On écrit tout entier n sous la forme :

$$n = i_0 + i_1 N + \ldots + i_h N^h \qquad \text{où} \quad \forall j \in \{0,\ldots,h\},$$

$$\text{alors} \quad 0 \leq i_j \leq N - 1$$

(c'est-à-dire qu'on écrit n dans son développement en base N).

- et on pose :

$$a_n = a_{i_0} + a_{i_1} \pi + \ldots + a_{i_h} \pi^h$$

Il en résulte :

- que $(a_0, a_1, \ldots, a_{N^h-1})$ est un système de représentants de A modulo $\mathfrak{M}^h$ pour tout h

- que $v(a_n - a_{n'})$ est la plus grande puissance de N qui divise $(n - n')$. Si on note $v_N(x)$ la plus grande puissance de N qui divise un entier x (et on prend garde qu'en général v_N n'est pas une valuation) alors $v(a_n - a_{n'}) = v_N(n - n')$.

On peut alors considérer la suite des polynômes :

$$f_0 = 1 \quad , \quad f_1 = (X-a_0), \ldots, f_n = (X-a_0)(X-a_1)\ldots(X-a_{n-1}), \ldots$$

Lemme 1.1. [G.Polya] . *Pour tout entier* n. $f_n(a_n)$ *engendre l'idéal* $f_n(A)$ *et* $v[f_n(a_n)] = \sum_{h=1}^{n} v_N(h) = \sum_{\alpha=1}^{\infty} [n/N^\alpha]$ *où* $[n/N^\alpha]$ *désigne la partie entière de* n/N^α .

Preuve : Résumons et adaptons le preuve de [G.Polya]. Il nous suffit d'établir que $v[f_n(\xi)] \geq v[f_n(a_n)]$, $\forall \xi \in A$. Ou bien $f_n(\xi) = 0$, mais alors $v[f_n(\xi)] = \infty$ et c'est gagné, ou bien $v[f_n(\xi)] = p < \infty$. Comme $a_0, a_1, \ldots, a_n, \ldots,$ forment un système de représentants modulo $\mathfrak{M}^h$, on peut pour h grand, trouver a_n suffisamment proche de ξ pour avoir $v[f_n(a_m)] = p$. Comme $p < \infty$, $f_n(a_m) \neq 0$ et $m \geq n$. On a alors :

$$p = v[f_n(a_m)] = v[(a_m-a_0)(a_m-a_1)\ldots(a_m-a_{n-1})]$$

$$= \sum_{h=0}^{n-1} v(a_m-a_h) = \sum_{h=0}^{n-1} v_N(m-h)$$

$$p = \sum_{h=1}^{m} v_N(h) - \sum_{h=1}^{m-n} v_N(h) \quad ,$$

tandis que $v[f_n(a_n)] = \sum_{h=1}^{n} v_N(h)$.

Sans démontrer l'égalité purement arithmétique :

$$\sum_{h=1}^{\lambda} v_N(h) = \sum_{\alpha=1}^{\infty} [\lambda/N^\alpha]$$

on en tire

$$p = \sum_{\alpha=1}^{\infty} [m/N^\alpha] - \sum_{\alpha=1}^{\infty} [m-n/N^\alpha] \geq \sum_{\alpha=1}^{\infty} [(m - (m-n))/N^\alpha]$$

donc $p \geq \sum_{\alpha=1}^{\infty} [n/N^{\alpha}] = v[f_n(a_n)]$.

Pour tout entier N, on définit la fonction $S_N(n)$ de l'entier n par la formule

$$S_N(n) = \sum_{h=1}^{n} v_N(h) = \sum_{\alpha=1}^{\infty} [n/N^{\alpha}] .$$

On note A_s l'anneau des polynômes à valeurs entières :

$$A[X] \subset A_s = \{P \in K[X] \mid P(A) \subset A\} \subset K[X].$$

Proposition 1.2. *Le A-module A_s est libre, une base en est la suite de polynômes $g_0, g_1, \ldots, g_n, \ldots$ où $g_n = f_n / \pi^{S_N(n)}$, $\forall n \in N$.*

Preuve : d'après [G.Polya]. On montre aussi cette proposition au §3 pour plusieurs variables.

Corollaire 1.3. *Pour tout polynôme P de $K[X]$ de degré n, on a les inégalités*

$$v(P) \leq v[P(A)] \leq v(P) + S_N(n).$$

Preuve : On peut écrire $P = \sum_{i=0}^{n} \lambda_i g_i$ où $\lambda_i \in K$. Bien sûr $P.\pi^{-v[P(A)]} \in A_s$, ainsi $\lambda_i \pi^{-v[P(A)]} \in A$, d'après la proposition 1.2., et donc $v(\lambda_i) \geq v[P(A)]$.

Comme $v[P] \geq \operatorname{Inf}_{i=1}^{n} \{v(\lambda_i g_i)\}$, donc $v(P) \geq v[P(A)] + \operatorname{Inf}_{i=1}^{n} \{v(g_i)\}$,

comme $v(g_i) = -S_N(i)$ et que $S_N(i) \leq S_N(n)$, $\forall i \leq n$, alors :

$$v(P) \geq v([P(A)]) - S_N(n).$$

Terminons ce paragraphe par une approximation de $S_N(n)$. On a $S_N(n) = \sum_{\alpha=1}^{\infty} [n/N^\alpha]$; si on pose $\ell = [\log_N(n)]$ (ainsi $N^\ell \leq n$ mais $N^{\ell+1} > n$) , on a alors aussi :

$$\sum_{\alpha=1}^{\ell} (n/N^\alpha - 1) \leq S_N(n) \leq \sum_{\alpha=1}^{\ell} (n/N^\alpha).$$

Ainsi $n/N-1\ [1 - (1/N)^\ell] - \ell \leq S_N(n) \leq n/N-1$

ou encore $S_N(n) \sim n/N-1$, si $n \to \infty$.

§ 2. ANNEAU DE DEDEKIND.

Maintenant A désigne un anneau de Dedekind de corps des fractions K ; à tout idéal maximal $\mathfrak{m}$ de A, correspond une valuation $v_{\mathfrak{m}}$ de K , d'anneau $A_{\mathfrak{m}}$; on note $N(\mathfrak{m})$ le cardinal de $A/\mathfrak{m}$. Si I est un idéal fractionnaire de A, on note $v_{\mathfrak{m}}(I)$ la puissance de $\mathfrak{m}$ dans la décomposition de I en produits d'idéaux maximaux (c'est aussi la puissance de $\mathfrak{m}A_{\mathfrak{m}}$ égale au localisé $I_{\mathfrak{m}}$).

Proposition 2.1. *Pour tout idéal maximal $\mathfrak{m}$ de A , et tout polynôme P de K[X] , de degré n, P(A) est un idéal fractionnaire de A et on a :*

$$v_{\mathfrak{m}}(P) \leq v_{\mathfrak{m}}[P(A)] \leq v_{\mathfrak{m}}(P) + S_{N(\mathfrak{m})}(n).$$

Preuve : Si d est un dénominateur commun des coefficients de P, alors $dP \in A[X]$, donc $dP(A) \subset A$, et $P(A)$ est un idéal fractionnaire. Comme $(P(A))_{\mathfrak{M}} = P(A_{\mathfrak{M}})$ [cf. I. théorème 3.2.] , on peut appliquer le corollaire 1.3.

Lemme 2.2. *Pour tout entier* n *il n'y a qu'un nombre fini d'idéaux maximaux de* A *tels que* $N(\mathfrak{M}) \leq n$.

Preuve : Ou bien A est un corps fini, ou bien $\exists x \in A,\ x \neq 0$ tel que $(x^{n-1} - 1) \neq 0$. Mais comme x ou $(x^{n-1} - 1)$ est dans tout idéal $\mathfrak{M}$ de norme n, ces idéaux sont en nombre fini.

Il est donc consistant de poser la

Définition 2.3. *On appelle idéaux caractéristiques de* A *, les idéaux de la suite* (I_n) *où* $v_{\mathfrak{M}}(I_n) = - S_{N(\mathfrak{M})}(n)$,
pour tout idéal maximal de A .

Si $a_{0,\mathfrak{M}}, a_{1,\mathfrak{M}}, \ldots, a_{n,\mathfrak{M}}, \ldots$ est une suite prolongée de représentants de $A_{\mathfrak{M}}$, comme au §1., on sait alors trouver dans A, des éléments $b_{i,n}$, pour $i \in \{0,\ldots,n\}$, tels que :

$$v_{\mathfrak{M}}[b_{i,n} - a_{i,m}] > S_{N(\mathfrak{M})}(n) \quad , \quad \forall n \ , \ \forall i \in \{0,\ldots,n\} \ , \quad \text{et}$$

$\mathfrak{M}$ tel que $S_{N(\mathfrak{M})}(n) \neq 0$ (il y a un nombre fini de tels idéaux) [Bbki VII. §2. proposition 2] .

On pose alors

$$f_0 = 1 \ , \ f_1 = X, \ldots, \ f_n = (X - b_{0,n}) \ldots (X - b_{n-1,n})$$

et si $f_{0,\mathfrak{m}}, f_{1,\mathfrak{m}}, \ldots, f_{n,\mathfrak{m}}$ est la suite de polynômes correspondant à la suite $a_{0,\mathfrak{m}}, a_{1,\mathfrak{m}}, \ldots, a_{n,\mathfrak{m}}$ de $A_{\mathfrak{m}}$, on a alors

$$v_{\mathfrak{m}}[f_{n,\mathfrak{m}} - f_n] > S_{N(\mathfrak{m})}(n) \quad , \quad \text{soit}$$

$$v_{\mathfrak{m}}[f_n(A)] = v_{\mathfrak{m}}[f_n(b_{n,n})] = v_{\mathfrak{m}}[f_{n,m}(a_{n,\mathfrak{m}})] = S_{N(\mathfrak{m})}(n)$$

pour tout $\mathfrak{m}$ tel que $S_{N(\mathfrak{m})}(n) \neq 0$, tandis que si $S_{N(\mathfrak{m})}(n) = 0$, alors bien sûr $v_{\mathfrak{m}}[f_n(A)] = S_{N(\mathfrak{m})}(n) = 0$ [cf. proposition 2.1.] car $v_{\mathfrak{m}}(f_n) = 0$ puisque f_n est un polynôme unitaire de $A[X]$.

$$\text{En conclusion} \quad f_n(A) = I_n^{-1} = \prod_{\mathfrak{m}} \mathfrak{m}^{S_{N(\mathfrak{m})}(n)} \quad .$$

Théorème 2.4. *Le A-module A_s est projectif et admet la décomposition interne, en somme d'idéaux fractionnaires de A :*

$$A_s = I_0 f_0 \oplus I_1 f_1 \oplus \ldots \oplus I_n f_n \oplus \ldots$$

Preuve : $I_n f_n(A) = A$, donc $I_n f_n \subset A_s$ et

$$I_0 f_0 \oplus I_1 f_1 \oplus \ldots \oplus I_n f_n \oplus \ldots \subset A_s \ .$$

Si inversement $P \in A_s$, on peut écrire $P = \sum_{i=0}^{n} \lambda_i f_i$ où $\lambda_i \in K$. λ_n est le coefficient directeur de P et

$$v_{\mathfrak{m}}(\lambda_n) \geq v(P) \geq v[P(A)] - S_{N(\mathfrak{m})}(n) \ , \quad \forall \mathfrak{m} \ \text{[cf. proposition 2.1.]}$$

Mais $P(A) \subset A$ donc $v[P(A)] \geq 0$, ainsi $v_{\mathfrak{m}}(\lambda_n) \geq v_{\mathfrak{m}}(I_n)$ pour tout $\mathfrak{m}$ et $\lambda_n \in I_n$. Comme $I_n f_n \subset A_s$, $P - \lambda_n f_n \in A_s$, on peut recommencer, prouver que $\lambda_{n-1} \in I_{n-1}$, ainsi de suite que $\lambda_j \in I_j$, $\forall j \leq n$.

Corollaire 2.5. *Soit* (g_n) *une suite de polynômes de* $K[X]$, *où* g_n *est de degré* n *et de coefficient directeur* x_n . *Les conditions suivantes sont équivalentes :*

i) $v_{\mathfrak{m}}[g_n(A)] = v_{\mathfrak{m}}(x_n) + S_{N(\mathfrak{m})}(n)$, $\forall \mathfrak{m}$

ii) $A_s = \oplus_n J_n g_n$ *où* J_n *est un idéal fractionnaire de* A.

Dans ces conditions, on a de plus :

a) $v_{\mathfrak{m}}(x_n) = v_{\mathfrak{m}}(g_n)$, $\forall \mathfrak{m}$ (*et si* g_n *est unitaire alors* $g_n \in A[X]$)

b) $J_n = x_n^{-1} I_n$ (*et si* g_n *est unitaire alors* $J_n = I_n$).

Preuve : D'abord i) entraîne a) puisque $v_{\mathfrak{m}}(x_n) \geq v_{\mathfrak{m}}(g_n)$ d'une part et $v_{\mathfrak{m}}[g_n(A)] = v_{\mathfrak{m}}(x_n) + S_{N(\mathfrak{m})}(n) \leq v_{\mathfrak{m}}(g_n) + S_{N(\mathfrak{m})}(n)$ d'autre part. [cf. proposition 2.1.] , et i) => ii) , on montrerait que $A_s = \oplus_n (x_n^{-1} I_n) g_n$ comme on a montré le théorème 2.4., en utilisant l'égalité $g_n(A) = x_n I_n^{-1}$. ii) => i). Si inversement $A_s = \oplus J_n g_n$, alors en particulier $J_n g_n \subset A_s$, donc $\forall \alpha \in J_n$, $\alpha g_n \in A_s$ et $\alpha g_n = \lambda_0 f_0 + \ldots + \lambda_n f_n$ où $\lambda_n \in I_n$. En comparant les termes de degré n on a $\alpha x_n \in I_n$ ainsi $J_n x_n \subset I_n$. Comme inversement $I_n f_n \subset A_s$ on a aussi $I_n \subset J_n x_n$ et donc $J_n x_n = I_n$. Soit b).

Mais de $J_n g_n \subset A_s$ on tire aussi $J_n g_n(A) \subset A$ donc

$$v_{\mathfrak{m}}[g_n(A)] \geq v_{\mathfrak{m}}(x_n) + S_{N(\mathfrak{m})}(n).$$

Comme d'autre part

$$v_{\mathfrak{m}}[g_n(A)] \leq v_{\mathfrak{m}}(g_n) + S_{N(\mathfrak{m})}(n) \leq v_{\mathfrak{m}}(x_n) + S_{N(\mathfrak{m})}(n) ,$$

cela prouve le corollaire.

Remarque : [G.Polya] introduit l'idéal I_n de la façon suivante : l'ensemble des coefficients directeurs des polynômes de A_s, de degré inférieur ou égal à n, forme bien évidemment un idéal ; d'après le théorème 2.4., il s'agit bien de l'idéal I_n.

§ 3. PLUSIEURS VARIABLES.

On s'intéresse maintenant aux polynômes à plusieurs variables. On note $A_{s,m}$ le sous anneau de $K[X_1,\ldots,X_m]$ formé par les polynômes P tels que $P(A^m) \subset A$.

On note $\underline{n} = (n_1,\ldots,n_m) \in \mathbb{N}^m$ un m-tuple d'entiers,

$\underline{X}^{\underline{n}}$ le monôme $X_1^{n_1} X_2^{n_2} \ldots X^{n_m}$ tout polynôme s'écrit :

$P = \sum_{\underline{n} \in \Lambda} \lambda_{\underline{n}} \underline{X}^{\underline{n}}$ où Λ est un ensemble fini de m-tuples.

On munit $\mathbb{N}^m$ de l'ordre (partiel) :

$$\underline{n} \leq \underline{n}' \iff n_i \leq n_i' \quad \forall i \in \{1,\ldots,m\} .$$

On suppose d'abord que A est local, $a_0,a_1,\ldots,a_n,\ldots$ désigne la suite de représentants construite au §1, et

$$f_0 = 1, \quad f_1 = (X - a_0),\ldots,f_n = (X - a_0) \ldots (X - a_{n-1}), \ldots$$

est la suite correspondante de polynômes, on pose :

$$f_{\underline{n}} = \prod_{i=1}^{m} f_{n_i}(X_i)$$

et

$$S_N(\underline{n}) = \sum_{i=1}^{m} S_N(n_i)$$

il est clair d'après le lemme 1.1. que

$$v[f_{\underline{n}}(\underline{\xi})] \geq v[f_{\underline{n}}(a_{\underline{n}})] = S_N(\underline{n}) \qquad \forall \underline{\xi} \in A^m \quad \text{et}$$

$$\text{où} \quad a_{\underline{n}} = (a_{n_1},\ldots,a_{n_m})$$

Ainsi avec ces notations :

Proposition 3.1. *Si* A *est local,* $A_{s,m}$ *est un* A*-module libre de base* $(g_{\underline{n}})_{\underline{n} \in \mathbb{N}^m}$, *où* $g_{\underline{n}} = f_{\underline{n}} / \pi^{S_N(\underline{n})}$

Preuve : Comme $f_{\underline{n}}(A^m) \subset \pi^{S_N(\underline{n})} A$, alors le A-module libre de base $(g_{\underline{n}})_{\underline{n} \in \mathbb{N}^m}$ est inclus dans $A_{s,m}$.

Inversement, comme tout polynôme $f_{\underline{n}}$ s'écrit : $f_{\underline{n}} = X^{\underline{n}} + \sum_{\underline{k}<\underline{n}} \alpha_{\underline{k}} X^{\underline{k}}$, les polynômes $f_{\underline{n}}$ forment une base du K-espace vectoriel $K[X_1,\ldots,X_m]$, c'est aussi le cas des polynômes $g_{\underline{n}}$. Si P est un polynôme de $K[X_1,\ldots,X_m]$ on peut écrire :

$$P = \sum_{\underline{n}\in\Lambda} \lambda_{\underline{n}} g_{\underline{n}} \ .$$

Si $\exists \underline{n} \in \Lambda$ tel que $\lambda_{\underline{n}} \notin A$, alors on considère un élément minimal $\underline{k}$ pour cette propriété ; alors $\forall \underline{n} < \underline{k}$, $\lambda_{\underline{n}} \in A$, donc $\lambda_{\underline{n}} g_{\underline{n}} \in A_{s,m}$. Si on avait $P \in A_{s,m}$, alors on aurait

$$Q = P - \sum_{\underline{n}<\underline{k}} \lambda_{\underline{n}} g_{\underline{n}} \in A_{s,m} \ .$$

Par ailleurs $Q = \sum_{\underline{n}\in\Lambda'} \lambda_{\underline{n}} g_{\underline{n}}$, et $\forall \underline{n} \in \Lambda'$, $\underline{n} \neq \underline{k}$, $\exists i \in \{1,\ldots,m\}$ tel que $n_i > k_i$, donc $(X_i - a_{k_i})$ est un facteur de $f_{\underline{n}}$. Ainsi

$$Q(a_{\underline{k}}) = \lambda_{\underline{k}} g_{\underline{k}}(a_{\underline{k}}) + 0$$

mais $Q(a_{\underline{k}}) \in A$ et $g_{\underline{k}}(a_{\underline{k}})$ est une unité de A. On devrait avoir $\lambda_{\underline{k}} \in A$. Contradiction. Donc $P \notin A_{s,m}$.

On revient maintenant au cas global,

Proposition 3.2. *Soit* A *un anneau de Dedekind alors pour tout polynôme* $P = \sum_{\underline{n}\in\Lambda} \lambda_{\underline{n}} X^{\underline{n}}$ *de* $K[X_1,\ldots,X_m]$ *et tout idéal maximal* $\mathfrak{M}$ *de* A *on a :*

$$v_{\mathfrak{M}}(P) \leq v_{\mathfrak{M}}[P(A^{\mathfrak{M}})] \leq v_{\mathfrak{M}}(P) + \mathrm{Max}_{\underline{n}\in\Lambda}\{S_{N(\mathfrak{M})}(\underline{n})\} \quad .$$

On démontrerait cette proposition comme le corrolaire 1.3. et la proposition 2.1., en notant que si $P = \sum_{\underline{n}\in\Lambda} \lambda_{\underline{n}} X^{\underline{n}}$ d'une part et $P = \sum_{\underline{n}\in\Lambda'} \lambda_{\underline{n}} g_{\underline{n}}$ d'autre part, alors Λ et Λ' ont les mêmes éléments maximaux.

On note

$$f_{\underline{n}} = \prod_{i=1}^{m} f_{n_i}(X_i) \quad \text{où} \quad f_{n_i} = (X_i - b_{0,n_i})\ldots(X_i - b_{n_{i-1},n_i})$$

et $I_{\underline{n}} = \prod_{i=1}^{m} I_{n_i}$.

On démontrerait comme au §2 la

Proposition 3.3. *Soit* A *un anneau de Dedekind. Le* A*-module* $A_{s,m}$ *est projectif et admet la décomposition en somme directe :*

$$A_{s,m} = \oplus_{\underline{n}\in\mathbb{N}^m} I_{\underline{n}} f_{\underline{n}} \quad .$$

Corollaire 3.4. *Soit* A *un anneau de Dedekind . Alors*

$$A_{s,m} \cong \otimes^{m} A_{s} \quad , \quad \forall m.$$

CHAPITRE V - GROUPE DE POLYA-OSTROWSKI

Dans tout ce chapitre on suppose que A est un anneau de Dedekind de corps des fractions K.

§ 1. DEFINITION.

Définition 1.1. *On appelle groupe de Polya-Ostrowski de* A, *et on note* $\mathfrak{H}(A)$, *le sous groupe du groupe des classes* $\mathfrak{C}(A)$, *engendré par les classes des idéaux caractéristiques* I_n *de* A.

Remarque : $\mathfrak{H}(A)$ est aussi bien engendré par tous les idéaux $I_{\underline{n}}$, où $\underline{n}$ parcourt l'ensemble des m-tuples d'entiers; en effet $I_{\underline{n}}$ est un produit d'idéaux caractéristiques et $I_n = I_{(n,0,\ldots,0)}$.

Maintenant on note $A_s^{(d)}$ le sous-ensemble de A_s formé des polynômes de A_s de degré inférieur ou égal à d (resp. $A_{s,m}^{(\underline{d})}$, où $\underline{d}$ est un m-tuple d'entiers $\underline{d} = (d_1,d_2,\ldots,d_m)$, le sous ensemble de $A_{s,m}$ formé des polynômes de degré en X_i inférieur ou égal à d_i). C'est un sous A-module de A_s (resp. un sous A-module de $A_{s,m}$) :

Proposition 1.2. *Les assertions suivantes sont équivalentes :*

i) *le groupe* $\mathfrak{H}(A)$ *est trivial.*

ii) *tous les idéaux* I_n *sont principaux.*

iii) A_s *est libre et possède une base de polynômes* (f_n) *où* f_n *est de degré* n.

iv) tous les modules $A_s^{(d)}$ *sont des A-modules libres.*

v) tous les modules $A_{s,m}^{(d)}$ *sont libres.*

Preuve : C'est clair après les théorème 2.4., corollaire 2.5. et proposition 3.3. du chapitre IV. En général on a les décompositions :

$$A_s^{(d)} = \oplus_{j=0}^{d} I_j f_j$$

$$A_{s,m}^{(d)} = \oplus_{j \leq d} I_j f_j$$ (avec les notations du chapitre précédent).

Remarque : A_s est toujours libre car c'est un module projectif de rang infini [Bbki VII. §4. Exercices].

§ 2. RESULTATS GENERAUX.

Proposition 2.1. [A.Ostrowski] $\mathcal{H}(A)$ *est le sous groupe de* $\mathcal{C}(A)$ *engendré par les classes des produits d'idéaux premiers de même norme finie.*

Preuve : Comme $I_n = \prod \mathfrak{m}^{S_{N(\mathfrak{m})}(n)}$, les idéaux de même norme apparaissent dans le même produit. Si maintenant N est un entier, et la norme de certains idéaux premiers (N est donc puissance d'un nombre premier) $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_k$ alors I_N/I_{N-1}, dont la classe est encore dans $\mathcal{H}(A)$, est de la forme $\mathfrak{a}\,\mathfrak{m}_1\,\mathfrak{m}_2 \ldots \mathfrak{m}_k$ où $\mathfrak{a}$ est un produit d'idéaux premiers de norme strictement inférieure à n. On peut supposer, par hypothèse de récurrence, que la classe de $\mathfrak{a}$ est dans $\mathcal{H}(A)$, ainsi la classe de $\mathfrak{m}_1\,\mathfrak{m}_2 \ldots \mathfrak{m}_k$ est aussi dans $\mathcal{H}(A)$.

Proposition 2.2. *Soit* L *une extension algébrique finie de* K , B *l'anneau des éléments de* L , *entiers sur* A, $(I_n(A))$ *la suite des idéaux caractéristiques de* A *et* $(I_n(B))$ *la suite des idéaux caractéristiques de* B, *alors* $I_n(B)^{-1}$ *divise* $I_n(A)^{-1}B$.

Preuve : Si $\mathfrak{M}$ est un idéal maximal de B, alors $v_{\mathfrak{M}}[I_n(B)^{-1}] = S_{N(\mathfrak{M})}(n)$; et si $\mathfrak{p} = \mathfrak{M} \cap A$, $v_{\mathfrak{p}}[I_n(A)^{-1}] = S_{N(\mathfrak{p})}(n)$. Ainsi $v_{\mathfrak{M}}[I_n(A)^{-1}B] = e(\mathfrak{M},\mathfrak{p})\, S_{N(\mathfrak{p})}(n)$ où $e(\mathfrak{M},\mathfrak{p})$ est l'indice de ramification de $\mathfrak{M}$ sur $\mathfrak{p}$, et donc

$$v_{\mathfrak{M}}[I_n(A)^{-1}B] \geq S_{N(\mathfrak{p})}(n) \geq S_{N(\mathfrak{M})}(n) = v_{\mathfrak{M}}[I_n(B)^{-1}]$$

car $N(\mathfrak{M}) \geq N(\mathfrak{p})$.

Corollaire 2.3. *Si* A *est l'anneau des entiers d'un corps de nombres, alors* $n!I_n$ *est un idéal entier de* A , *ou encore* $n!A_S^{(n)} \subset A[X]$.

Preuve : Il est facile de vérifier que $I_n(\mathbb{Z}) = \frac{1}{n!}\,\mathbb{Z}$.

Proposition 2.4. *Si* L *est une extension galoisienne finie de* K , *où* A *est principal, et si* B *est l'anneau des éléments de* L , *entiers sur* A, *alors* $\mathcal{H}(A)$ *est engendré par les classes des produits d'idéaux premiers au-dessus d'un premier de* B *ramifié.*

Preuve : Les idéaux de même norme sont groupés dans un même produit. Par conjugaison, tous les idéaux au-dessus d'un idéal premier non ramifié ont même norme, et leur produit est un idéal principal.

Cette proposition généralise le même résultat, dû à Ostrowski, pour l'anneau des entiers B d'une extension galoisienne finie de $\mathbb{Q}$. On voit comment on peut ainsi engendrer concrètement $\mathcal{H}(B)$ par un nombre fini de classes.

Corollaire 2.5. *Avec les hypothèses de la proposition 2.4., si l'extension* L/K *est de degré* n, *alors l'exposant de* $\mathcal{H}(B)$ *divise* n.

Preuve : Si $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_k$ sont au-dessus d'un idéal premier ramifié, avec l'indice de ramification e, alors $(\mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_k)^e$ est principal, or e divise n.

§ 3. CORPS CYCLOTOMIQUES, CORPS QUADRATIQUES.

Proposition 3.1. *Soit* A *l'anneau des entiers du corps cyclotomique* $\mathbb{Q}(\sqrt[n]{1})$, *alors* $\mathcal{H}(A)$ *est trivial.*

Preuve : D'après la proposition 2.4., il nous faut prouver que le produit des idéaux premiers de A, au-dessus de chaque nombre premier p qui divise n, est un idéal principal. Soit donc p un nombre premier, K le corps $\mathbb{Q}(\sqrt[p^r]{1})$ (où p^r est la plus grande puissance de p qui divise n), et B l'anneau des entiers de K. p est totalement ramifié dans B, on peut écrire $pB = (z - 1)^e B$ où $e = p^r(p - 1)$, et z est une racine primitive p^r-ème de l'unité. L'idéal premier principal $(z - 1)B$ de B, est le seul au-dessus de (p) [Samuel §5.2.]. Par ailleurs $\mathbb{Q}(\sqrt[n]{1})$ est aussi une extension galoisienne

de K, l'idéal $(z - 1)B$ n'y est pas ramifié donc le produit des idéaux $\mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_k$ de A, au-dessus de (p), est l'idéal principal $\mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_k = (z - 1)A$.

Les résultats de G.Polya et A. Ostrowski sont tout à fait suffisants pour étudier le cas des corps quadratiques. De façon concrète, on a, pour un radical négatif :

Proposition 3.2. *Soit* A *l'anneau des entiers de* $\mathbb{Q}(\sqrt{d})$ *où* d *est un entier négatif sans facteur carré, alors* $\mathcal{H}(A)$ *est trivial dans les seuls cas suivants :* $d = -1$, $d = -2$, *et* $d = -p$ *où* p *est premier ,* $p \equiv 3 \pmod 4$.

Preuve : Si $d = -1$ ou $d = -2$ alors $\mathcal{C}(A)$ lui-même est trivial. Si $d = -p$ où $p \equiv 3 \pmod 4$, alors seul p est ramifié et le seul idéal au-dessus de p est principal, engendré par $\sqrt{p}$ [Samuel §5.4.].

Dans tous les autres cas il y a plus d'un idéal premier ramifié, on peut tirer d'un théorème de Hilbert [D.Hilbert, Satz 106] que l'un d'eux n'est pas principal. On peut aussi en donner une preuve facile :

- Si $d = -p$ et $p \equiv 1 \pmod 4$ alors 2 est aussi ramifié et $2A = \mathfrak{P}^2$, et la classe de $\mathfrak{P}$ est un générateur de $\mathcal{H}(A)$. $\mathfrak{P}$ n'est pas principal, sinon, comme $A = \mathbb{Z}[\sqrt{d}]$ on aurait $\mathfrak{P} = (u + v\sqrt{d})A$ où $u,v \in \mathbb{Z}$, donc aussi $\mathfrak{P} = (u - v\sqrt{d})A$ par conjugaison, soit $2A = (u + v\sqrt{d})(u - v\sqrt{d})A$ d'où on tire $2 = u^2 + pv^2$ qui est impossible en nombres entiers.

- Si $d = -p_1 p_2 \dots p_r$, où $r > 1$, alors $p_1, p_2, \dots, p_r$ sont ramifiés, et pour tout i, $p_i A = \mathfrak{P}_i^2$. La classe de chaque $\mathfrak{P}_i$ est dans $\mathcal{H}(A)$, aucun n'est principal ; sinon $\mathfrak{P}_i$ pourrait être engendré par un élément de la forme $\frac{u + v\sqrt{d}}{2}$ et aussi par $\frac{u - v\sqrt{d}}{2}$, on aurait donc $4p_i = u^2 - dv^2$. Comme p_i divise d, p_i diviserait u^2 donc u, on aurait $u = u'p_i$ où $u' \in \mathbb{Z}$ et $4 = u'^2 p_i + \prod_{j \neq i} p_j v^2$. Il est facile de voir que cette égalité est impossible en nombres entiers.

De façon beaucoup plus complète, on peut déduire du théorème de Hilbert [D. Hilbert. Satz 105 - Satz 106] .

Proposition 3.3. *Soit* K *un corps quadratique et* A *l'anneau des entiers de* K. *Alors si le discriminant de* K *a* t *diviseurs premiers, le groupe* $\mathcal{H}(A)$ *est le groupe d'exposant* 2 *à* t-1 *générateurs et* 2^{t-1} *éléments dans le cas imaginaire et dans le cas réel si la norme de l'unité fondamentale est* -1 , $\mathcal{H}(A)$ *est le groupe d'exposant* 2 *à* t-2 *générateurs et* 2^{t-2} *éléments dans le cas réel si la norme de l'unité fondamentale est* +1.

Il résulte de cette proposition et de la preuve de la précédente, que si $K = \mathbb{Q}(\sqrt{-p})$, où p est premier et $p \equiv 1 \pmod 4$ alors $\mathcal{H}(A)$ est le groupe à 2 éléments. Ainsi, quand par exemple $p = 17$, $\mathcal{H}(A)$ est strictement contenu dans $\mathcal{C}(A)$ (en effet 3 est décomposé : $3A = \mathfrak{Q}_1 \mathfrak{Q}_2$, et si $\mathfrak{Q}_1$ était d'ordre 2 dans $\mathcal{C}(A)$, l'équation $9 = u^2 + 17v^2$ serait soluble en nombres entiers tels que $v \neq 0$).

Corollaire 3.4. *Si* $K = \mathbb{Q}(\sqrt{d})$ *où* d *est un nombre positif sans facteur carré, alors* $\mathcal{H}(A)$ *n'est trivial que dans les cas suivants :* $d = 2$; $d = p$, p *premier,* $p \equiv 1 \pmod 4$; $d = p$, p *premier ,* $p \equiv 3 \pmod 4$ *et l'unité fondamentale de* A *est de norme* $+1$; $d = p_1 p_2$, p_1 *et* p_2 *premiers,* $d \equiv 1 \pmod 4$ *et l'unité fondamentale de* A *est de norme* $+1$.

§ 4. UN CONTRE-EXEMPLE.

On montre ici que lorsque K n'est pas une extension galoisienne de $\mathbb{Q}$, $\mathcal{H}(A)$ n'est pas nécessairement engendré par les produits d'idéaux premiers au-dessus d'un premier p ramifié et que l'exposant de $\mathcal{H}(A)$ ne divise pas nécessairement le degré $n = [K : \mathbb{Q}]$.

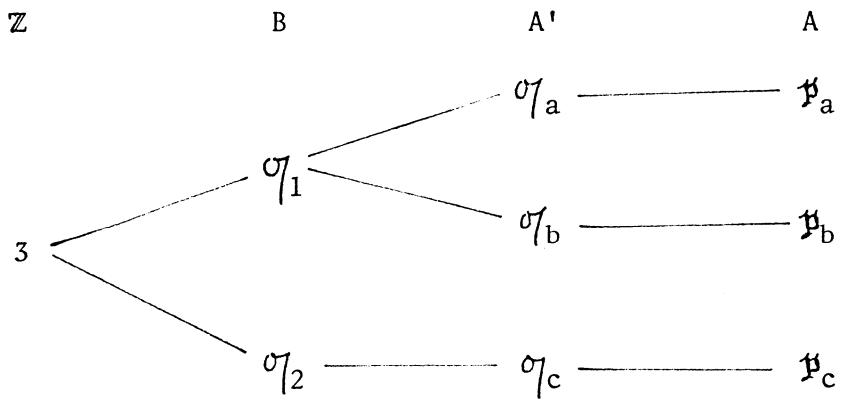
On étudie le cas $K = \mathbb{Q}(\xi)$ où ξ est racine de l'équation $X^4 + p = 0$ où p est premier et $p \equiv 1 \pmod 4$. On note F le corps $F = \mathbb{Q}(\xi^2) = \mathbb{Q}(\sqrt{-p})$ dont K est une extension quadratique, B l'anneau des entiers de F et A l'anneau des entiers de K. Par ailleurs l'anneau $A' = \mathbb{Z}[\xi] \cong \mathbb{Z}[X] / (X^4 + 1)$ est un sous-anneau de A (il se trouve ici que $A' = A$, mais ce fait ne nous est pas utile.).

On voit par le calcul du discriminant $d = 4^4 p^3$ [P.Samuel §2.7. : un exemple de calcul de discriminant] , que seuls 2 et p sont ramifiés dans A ; il est immédiat que l'idéal principal ξA est le seul idéal premier au-dessus de p ; et comme $(X + 1)^4 \cong X^4 + 1 \pmod 2$,

2 est déjà totalement ramifié dans A' , il n'y a donc dans A qu'un seul idéal premier $\mathfrak{P}$ au-dessus de 2, on a : $\mathfrak{P}^4 = 2A$. Mais comme on va le voir, $\mathcal{H}(A)$ n'est pas en général engendré par la classe de $\mathfrak{P}$, son exposant ne divise pas 4. On choisit $p = 29$. Comme $p \equiv 2 \pmod 3$, 3 est décomposé dans $B = \mathbb{Z}[\xi^2]$ en deux idéaux $\mathfrak{o}_1$ et $\mathfrak{o}_2$, chacun donc de norme 3. La décomposition de 3 dans $A' = \mathbb{Z}[\xi]$ est donnée par la décomposition de $X^4 + 29 \pmod 3$:

$$X^4 + 29 = (X + 1)(X + 2)(X^2 + 1) \pmod 3$$

il y a donc trois idéaux $\mathfrak{o}_a, \mathfrak{o}_b$ et $\mathfrak{o}_c$ dans A' , qui contient B. Deux sont nécessairement au-dessus de $\mathfrak{o}_1$, le troisième au-dessus de $\mathfrak{o}_2$. Comme $\mathbb{Z}/3\mathbb{Z}[X] / (X^2 + 1)$ est de cardinal 9, la norme de $\mathfrak{o}_c$ est 9 , de A' à A il ne peut pas y avoir de nouvelles décomposition : dans A il y a trois idéaux $\mathfrak{P}_a, \mathfrak{P}_b$ et $\mathfrak{P}_c$ au-dessus de 3, les deux premiers sont de norme 3, le dernier de norme 9.



Les classes de $\mathfrak{P}_a$ $\mathfrak{P}_b$ et de $\mathfrak{P}_c$ sont donc dans $\mathcal{H}(A)$ [cf. proposition 2.1.], pour finir ce contre exemple il nous suffit d'établir que $\mathfrak{P}_c^4$ n'est pas principal dans A. Si c'était le cas on aurait en effet

$\mathfrak{p}_c^4 = \lambda A$ (où $\lambda \in A$) donc aussi $\mathfrak{p}_c^4 = \sigma(\lambda)A$ (où σ est la conjugaison de l'extension quadratique, donc galoisienne, K/F). On aurait donc $\mathfrak{p}_c^8 = \lambda\sigma(\lambda)A$, mais $\lambda\sigma(\lambda) \in B$ et $\mathfrak{p}_c = \mathfrak{q}_2 B$, $\mathfrak{q}_2^8$ serait donc principal dans B. Mais $\mathfrak{q}_2^6$ est principal dans B. On a en effet la solution $\mathfrak{q}_2^6 = 2 + 5\sqrt{-29}$ qui donne par conjugaison $\mathfrak{q}_1^6 = 2 - 5\sqrt{-29}$, puisqu'on vérifie que $\mathbb{Z} \cap \mathfrak{q}_1^6 \mathfrak{q}_2^6 = 3^6 = 2^2 + 29.5^2$. De ce fait, $\mathfrak{q}_2^2$ devrait être principal, mais ceci n'est pas car l'équation $\mathbb{Z} \cap \mathfrak{q}_1^2 \mathfrak{q}_2^2 = 9 = u^2 + 29v^2$ est, elle, impossible en nombres entiers tels que $v \neq 0$!

TROISIEME PARTIE :

STRUCTURE MULTIPLICATIVE

CHAPITRE VI - SPECTRE PREMIER

On s'intéresse maintenant à un anneau de Dedekind A. On veut déterminer le spectre de l'anneau A_S. Les résultats, obtenus ici par une nouvelle méthode, sont originellement dus à [J.L.Chabert].

§ 1. PREMIERS RESULTATS FACILES.

Pour étudier le spectre de l'anneau A_S, on étudie tour à tour la fibre au-dessus de (0) et celle au-dessus de chaque idéal maximal.

La fibre au-dessus de (0) ne pose vraiment aucun problème. On a les inclusions $A[X] \subset A_S \subset K$, ainsi $A_S \otimes_A K \cong K[X]$ et donc

Proposition 1.1. *Soit* A *un anneau de Dedekind ; la fibre au-dessus*

de (0) *de l'anneau* A_s *se compose de :*

- *l'idéal* (0) *de hauteur* 0.

- *d'une famille d'idéaux premiers de hauteur* 1 , *en bijection avec l'ensemble des polynômes irréductibles, non constants de* K[X], *définis à la multiplication par un élément non nul de* K *près ; à un polynôme* P *correspond* $\tilde{P} = A_s \cap (P)\ K[X]$, *soit*

$$\tilde{P} = \{f \in A_s \mid f = P\varphi \quad \text{où} \quad \varphi \in K[X]\} .$$

Si maintenant $\mathfrak{m}$ est un idéal maximal de A, de corps résiduel k, la fibre au-dessus de $\mathfrak{m}$ de A_s correspond au spectre de l'anneau $A_s \otimes_A k = A_s \otimes_A A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}}$. Mais à cause de l'isomorphisme $(A_s)_{\mathfrak{m}} \cong (A_{\mathfrak{m}})_s$ [cf. I proposition 3.5.] , il s'agit aussi du spectre de l'anneau $(A_{\mathfrak{m}})_s \otimes k$. C'est-à-dire que les idéaux premiers de A_s, au-dessus de $\mathfrak{m}$, sont en bijection avec les idéaux premiers de $(A_{\mathfrak{m}})_s$ au-dessus de $\mathfrak{m}A_{\mathfrak{m}}$. Il est d'ailleurs également immédiat que les idéaux premiers au-dessus de (0) de A_s sont en bijection avec les idéaux premiers au-dessus de (0) de $(A_{\mathfrak{m}})_s$ et que les inclusions entre les idéaux premiers de A_s sont respectées dans le spectre de $(A_{\mathfrak{m}})_s$. On peut donc se ramener au cas local. Les paragraphes suivants sont donc consacrés à l'étude de la fibre au-dessus de $\mathfrak{m}$ d'un anneau de valuation discrète A, d'idéal maximal $\mathfrak{m}$. Mais cette étude est triviale si le corps résiduel $k = A/\mathfrak{m}$ est infini, puisqu'alors $A_s \cong A[X]$.

§ 2. FONCTIONS CONTINUES A VALEURS ENTIERES.

On suppose donc maintenant que A est l'anneau d'une valuation discrète v de K, de corps résiduel k fini. On note π une uniformisante, c'est-à-dire un générateur de l'idéal maximal $\mathfrak{M}$ de A. On considère la complétion $\hat{A}$ de A, pour la topologie définie par v, ainsi que $\hat{v}$, $\hat{\mathfrak{M}}$, $\hat{K}$ les complétés de v, $\mathfrak{M}$ et K. Un polynôme P peut être considéré comme la fonction qui à x associe $P(x)$, et cette fonction est bien sûr continue. Plus précisément, on note $\mathfrak{C}(\hat{A},\hat{K})$ l'ensemble des fonctions continues de $\hat{A}$ dans $\hat{K}$; $\mathfrak{C}(\hat{A},\hat{K})$ est un anneau, qu'on peut munir de la topologie de la convergence uniforme, et on a les inclusions :

$$A_S \subset \hat{K}[X] \subset \mathfrak{C}(\hat{A},\hat{K})$$

mais de plus,

Proposition 2.1. *$\hat{K}[X]$ est dense dans $\mathfrak{C}(\hat{A},\hat{K})$ muni de la topologie de la convergence uniforme.*

Preuve : C'est une application du théorème de Stone-Weierstrass [N. Bourbaki, V. §5. Exercices] . $\hat{K}$ est en effet un corps complet pour une valuation de hauteur 1, $\hat{A}$ est totalement discontinu et compact puisque $\hat{v}$ est discrète, complète et de corps résiduel fini. Il est clair de plus que $\hat{K}[X]$ contient les fonctions constantes de $\hat{A}$ dans $\hat{K}$ et sépare les points (X, à lui seul, sépare les points) ; donc toutes les hypothèses du théorème sont satisfaites.

Maintenant on appelle fonction continue à valeurs entières un élément f de $\mathfrak{C}(\hat{A},\hat{K})$ tel que $f(\hat{A}) \subset \hat{A}$. Ces fonctions forment un sous anneau de $\mathfrak{C}(\hat{A},\hat{K})$, que l'on note $\mathfrak{C}$, ou $\mathfrak{C}(\hat{A},\hat{A})$, et qu'on munit de la topologie induite. Bien sûr A_s est inclus dans $\mathfrak{C}$; si en effet $P \in A_s$, $P(A) \subset A$ et comme A est dense dans $\hat{A}$ et que $\hat{A}$ est fermé dans $\hat{K}$, alors $P(\hat{A}) \subset \hat{A}$. On a même de façon évidente $A_s = K[X] \cap \mathfrak{C}$.

Proposition 2.2. *A_s est dense dans $\mathfrak{C}$.* (voir aussi [AMICE] ou [MAHLER]).

Preuve : D'abord il est clair que $K[X]$ est dense dans $\hat{K}[X]$, donc dans $\mathfrak{C}(\hat{A},\hat{K})$, et comme $\mathfrak{C}$ est bien sûr ouvert dans $\mathfrak{C}(\hat{A},\hat{K})$, puisque $\hat{A}$ est ouvert dans $\hat{K}$, alors $A_s = K[X] \cap \mathfrak{C}$ est dense dans $\mathfrak{C}$.

Enfin, il convient de traduire la proposition 2.2. :

Corollaire 2.3. *Pour toute fonction g de $\mathfrak{C}$ (c'est-à-dire une fonction continue de $\hat{A}$ dans $\hat{K}$ telle que $g(\hat{A}) \subset \hat{A}$), et tout entier n, il existe un polynôme f dans A_s tel que*

$$\hat{v}[(f - g)(x)] > n \quad , \quad \forall x \in \hat{A}$$

§ 3. FIBRE AU-DESSUS DE $\mathfrak{m}$.

Comme A_s est dense dans $\mathfrak{C}$, on détermine d'abord la fibre de l'anneau $\mathfrak{C}$ au-dessus de $\mathfrak{m}$. A cause des inclusions $A \subset \hat{A} \subset \mathfrak{C}$, les idéaux premiers de $\mathfrak{C}$ au-dessus de $\mathfrak{m}$ sont précisément

ceux qui sont au-dessus de $\hat{\mathfrak{m}}$, c'est-à-dire qu'ils correspondent bijectivement aux éléments du spectre de $\mathfrak{C} \otimes_{\hat{A}} k$.

Lemme 3.1. *La fibre de $\mathfrak{C}$ au-dessus de $\mathfrak{m}$ correspond bijectivement au spectre de l'anneau $\mathfrak{C}(\hat{A},k)$, des fonctions localement constantes de $\hat{A}$ dans le corps k.*

Preuve : Bien sûr $\mathfrak{C} \otimes_{\hat{A}} k \cong \mathfrak{C}/\hat{\mathfrak{m}}\mathfrak{C}$. Mais $\hat{\mathfrak{m}}$ est un idéal principal de $\hat{A}$, engendré par l'uniformisante π, et $\hat{\mathfrak{m}}\mathfrak{C} = \pi\mathfrak{C}$. Si f est un élément de $\mathfrak{C}$, πf peut être interprêté comme un élément de $\mathfrak{C}(\hat{A},\hat{\mathfrak{m}})$, c'est-à-dire une fonction continue de $\hat{A}$ dans $\hat{\mathfrak{m}}$; inversement si $g \in \mathfrak{C}(\hat{A},\hat{\mathfrak{m}})$, il est clair que g/π a un sens et est un élément de $\mathfrak{C}$ ainsi $\hat{\mathfrak{m}}\mathfrak{C} = \pi\mathfrak{C} = \mathfrak{C}(\hat{A},\hat{\mathfrak{m}})$ et $\mathfrak{C} \otimes_{\hat{A}} k \cong \mathfrak{C} / \mathfrak{C}(\hat{A},\hat{\mathfrak{m}}) = \mathfrak{C}(\hat{A},\hat{A}) / \mathfrak{C}(\hat{A},\hat{\mathfrak{m}})$. Maintenant on a une application canonique Ψ de $\mathfrak{C}(\hat{A},\hat{A})$ dans $\mathfrak{C}(\hat{A},k)$ qui à toute fonction continue f de $\hat{A}$ dans $\hat{A}$, fait correspondre la fonction $\Psi(f)$ dont la valeur en x, est l'image $\overline{f(x)}$ de $f(x)$ dans le corps résiduel k. $\Psi(f)$ est localement constante, car f est continue. Le noyau de Ψ est précisément $\pi\mathfrak{C} \cong \mathfrak{C}(\hat{A},\hat{\mathfrak{m}})$ et ainsi $\mathfrak{C}(\hat{A},\hat{A}) / \mathfrak{C}(\hat{A},\hat{\mathfrak{m}}) \cong \mathfrak{C}(\hat{A},k)$ et donc $\mathfrak{C} \otimes_{\hat{A}} k \cong \mathfrak{C}(\hat{A},k)$.

$\mathfrak{C}(\hat{A},k)$ est l'anneau des fonctions localement constantes d'un espace topologique compact et totalement discontinu, à valeurs dans un corps commutatif. Son spectre est classique [N.Bourbaki, II, §4 , Exercices] .

Proposition 3.2. *Les idéaux premiers de* $\mathcal{C}$ *au-dessus de* $\mathfrak{m}$ *sont en bijection avec les points de* $\hat{A}$, *à un point* $a \in \hat{A}$, *correspond l'idéal* $\mathfrak{M}_a = \{f \in \mathcal{C} \mid f(a) \in \hat{\mathfrak{m}}\}$. *Tous ces idéaux sont maximaux et de corps résiduel* k .

C'est une application facile du spectre de $\mathcal{C}(\hat{A},k)$ et des isomorphismes mis en évidence au lemme 3.1.

On revient maintenant à la fibre de A_s au-dessus de $\mathfrak{m}$. On peut d'abord faire une observation facile.

Proposition 3.3. *Tous les idéaux premiers de* A_s *au-dessus de* $\mathfrak{m}$ *sont maximaux et de corps résiduel* k .

Preuve : Soient $a_1,a_2,\ldots,a_n$ des représentants de A modulo $\mathfrak{m}$, si $f \in A_s$, alors $g = \prod_{i=1}^{n} (f - a_i) / \pi$ est encore dans A_s, car pour tout x, f(x) est congru à un des a_i modulo $\mathfrak{m}$. Ainsi $\prod_{i=1}^{n} (f - a_i) = \pi g$ est dans $\mathfrak{m}A_s$ et dans tout idéal premier de A_s au-dessus de $\mathfrak{m}$ et chacun de ces idéaux premiers contient au moins l'un des facteurs $(f - a_i)$. Ainsi $a_1,a_2,\ldots,a_n$ forment aussi un système de représentants de A_s modulo tout idéal premier au-dessus de $\mathfrak{m}$.

De cette proposition, il résulte que tous les idéaux de $A_s / \pi A_s$ sont à la foix minimaux et maximaux et se relèvent donc dans l'anneau $\mathcal{C}(\hat{A},k) = \mathcal{C} / \pi\mathcal{C}$ (qui contient $A_s / \pi A_s$) [N. Bourbaki, II. §2. proposition 16] . Ainsi tout idéal de A_s ou de $\mathfrak{m}$ se

relève en un idéal de $\mathfrak{C}$ au-dessus de $\mathfrak{m}$. Il s'agit en fait d'une bijection :

Théorème 3.4. *Les idéaux premiers de* A_s *au-dessus de* $\mathfrak{m}$ *sont en bijection avec les points de* $\hat{A}$. *A un point* $a \in \hat{A}$ *correspond l'idéal*

$$\eta_a = \{f \in A_s \mid f(a) \in \hat{\mathfrak{m}}\} .$$

η_a *est maximal et* $A_s / \eta_a \cong k$.

Preuve : Il résulte de ce qui précède que tout idéal premier au-dessus de $\mathfrak{m}$ est du type η_a. De plus, si $a \neq b$, alors $\mathfrak{M}_a \neq \mathfrak{M}_b$ dans $\mathfrak{C}$, il existe donc une fonction continue g telle que $g(a) \in \hat{\mathfrak{m}}$ mais $g(b) \notin \hat{\mathfrak{m}}$. Il existe donc un polynôme $f \in A_s$, tel que

$$\hat{v}[f(x) - g(x)] > 0, \quad \forall x \in \hat{A}$$

[cf. corollaire 2.3.] et ainsi $f(a) \in \hat{\mathfrak{m}}$ mais $f(b) \notin \hat{\mathfrak{m}}$, d'où $f \in \eta_a$ mais $f \notin \eta_b$ et $\eta_a \neq \eta_b$.

Remarque : Si $\bar{a}$ est la classe d'un élément a de $\hat{A}$, modulo $\hat{\mathfrak{m}}$, alors $\eta_a \cap A[X]$ est l'idéal maximal et de hauteur 2 de $A[X]$, constitué par les polynômes de $A[X]$ dont l'image canonique dans $k[X]$ est divisible par $(X - \bar{a})$.

§ 4. INCLUSIONS.

Avec les notations des paragraphes précédents, on a la

Proposition 4.1. *Pour tout polynôme* P *de* $K[X]$, *l'idéal premier* $\tilde{P}$ *de* A_s *est inclus dans* η_a *si et seulement si* $P(a) = 0$.

Preuve : Sans changer l'idéal $\tilde{P}$, on peut supposer que $P \in A[X]$, en multipliant au besoin P par un élément non nul de K. Alors

- ou bien $P(a) = 0$, et alors $\forall f \in \tilde{P}$, $f = P\varphi$ où $\varphi \in K[X]$ donc $f(a) = 0$ et a fortiori $f(a) \in \hat{\mathfrak{m}}$, soit $f \in \eta_a$. Donc $\tilde{P} \subset \eta_a$.

- ou bien $P(a) \neq 0$, et donc $\hat{v}[P(a)] = n < \infty$. Comme P est une fonction continue de $\hat{A}$ dans $\hat{K}$, $\hat{v}[P(x)] = n$ en tout élément x d'une boule $a + \hat{\mathfrak{m}}^r$ où $r \in \mathbb{N}$. Mais comme $a + \hat{\mathfrak{m}}^r$ est ouvert et fermé, la fonction g de $\hat{A}$ dans $\hat{K}$ telle que

  . $g(x) = 1 / \pi^n$, $\forall x \in a + \hat{\mathfrak{m}}^r$

  . $g(x) = 1$, $\forall x \notin a + \hat{\mathfrak{m}}^r$

est une fonction continue. Comme $K[X]$ est dense dans $\mathcal{C}(\hat{A},\hat{K})$, il existe $\varphi \in K[X]$ tel que $\hat{v}[(\varphi - g)(x)] > 0$, $\forall x \in \hat{A}$, soit $\hat{v}[\varphi(x)] = \hat{v}[g(x)]$, $\forall x \in \hat{A}$. Ainsi $\hat{v}[\varphi P(x)] = 0$, $\forall x \in a + \hat{\mathfrak{m}}^r$ et $\hat{v}[\varphi P(x)] \geq \hat{v}[P(x)] \geq 0$, $\forall x \notin a + \hat{\mathfrak{m}}^r$, car $P \in A[X]$; donc $\varphi P \in \mathcal{C}$, et même $\varphi P \in \mathcal{C} \cap K[X] = A_s$, et même encore $\varphi P \in \tilde{P}$. Mais $\varphi P \notin \eta_a$, car $\hat{v}[\varphi P(a)] = 0$ et $\varphi P(a) \notin \hat{\mathfrak{m}}$.

Corollaire 4.2. *Si* a *est un élément de* $\hat{A}$ *transcendant sur* K *alors* η_a *est un idéal premier de hauteur* 1.

Corollaire 4.3. *Si* a *est un élément de* $\hat{A}$ *algébrique sur* K, η_a *est un idéal premier de hauteur* 2, *contenant un seul idéal premier*

de hauteur 1 *à savoir l'idéal* $\tilde{P}_a$ *où* P_a *est le polynôme minimal de* a *dans* K[X].

§ 5. VALUATIONS.

On complète la description du spectre en montrant que tous les localisés de A_s sont des anneaux de valuation [J.L.Chabert].

Pour tout élément a de $\hat{A}$, on définit sur K[X] une fonction v_a, à valeurs dans $\mathbb{Z} \cup \{\infty\}$, en posant :

$$v_a(f) = \hat{v}[f(a)].$$

On a alors de façon évidente :

$$v_a(fg) = v_a(f) + v_a(g) ,$$

$$v_a(f + g) \geq \mathrm{Inf}\{v_a(f), v_a(g)\} ,$$

et $v_a(f) = \infty$, si et seulement si $f(a) = 0$.

Proposition 5.1. *Si* a *est un élément de* $\hat{A}$, *transcendant sur* K, *alors on peut prolonger* v_a *à* K(X) ; v_a *est une valuation discrète de rang* 1, *extension immédiate de* v *à* K(X), *d'anneau* $(A_s)_{\eta_a}$.

Preuve : Si a est transcendant, $f(a) = 0$ si et seulement si $f = 0$, v_a est donc clairement une valuation discrète qu'on peut prolonger à K(X) en posant $v_a(f/g) = \hat{v}[f(a) / g(a)]$. Il est évident que $(A_s)_{\eta_a}$ est inclus dans l'anneau de v_a. Réciproquement, si $P/Q \in K(X)$ et $v_a(P/Q) \geq 0$, on veut montrer que $P/Q \in (A_s)_{\eta_a}$.

Bien sûr on peut supposer que P et Q sont dans A_s. Comme $v_a(P/Q) \geq 0$, si $v_a(Q) = \hat{v}[Q(a)] = n$ (et $n \geq 0$, puisque $Q \in A_s$, $n < \infty$ puisque a est transcendant), alors $v_a(P) = \hat{v}[P(a)] \geq n$. On reprend l'argument de la proposition 4.1. : comme P et Q sont des fonctions continues, la valuation des valeurs qu'elles prennent reste constante dans une petite boule $a + \hat{\mathfrak{m}}^r$ autour de a. La fonction de $\hat{A}$ dans $\hat{A}$, définie par :

$$g(x) = 1/\pi^n \ , \quad \forall x \in a + \hat{\mathfrak{m}}^r$$

$$g(x) = 1 \ , \quad \forall x \in a + \hat{\mathfrak{m}}^r \ ,$$

est continue, pour un polynôme $R \in K[X]$, "suffisamment proche", $\hat{v}[R(x)] = \hat{v}[g(x)]$, $\forall x \in \hat{A}$, ainsi, par construction, RP et RQ sont dans A_s (car $\hat{v}[RP(x)] \geq 0$, $\hat{v}[RQ(x)] \geq 0$, $\forall x \in \hat{A}$) mais $\hat{v}[RQ(a)] = -n + n = 0$, et $RQ \notin \eta_a$ donc $P/Q = RP/RQ \in (A_s)_{\eta_a}$.

Maintenant si a est un élément de $\hat{A}$, algébrique sur K, v_a n'est plus une valuation. Mais si P_a est un polynôme minimal de a sur K, on peut écrire de façon unique toute fraction rationnelle sous la forme

$$f = P_a^{v_{P_a}(f)} \varphi_f \ ,$$

où v_{P_a} est la valuation P_a-adique de f et φ_f une fraction rationnelle irréductible, dont numérateur et dénominateur sont premiers à P_a. On définit une fonction de $K(X)$ dans $\mathbb{Z} \times \mathbb{Z} \cup \{\infty\}$, ordonné lexicographiquement, en posant

$$w_a(f) = (v_{P_a}(f) \ , \ \hat{v}[\varphi_f(a)]).$$

Proposition 5.2. *Si* a *est un élément de* $\hat{A}$ *algébrique sur* K , *de polynôme minimal* P_a, w_a *est une valuation discrète de rang* 2 *de* K(X) *et d'anneau* $(A_s)_{\eta_a}$.

Preuve : Il n'est pas difficile de vérifier que w_a est une valuation. Bien sûr $(A_s)_{\eta_a}$ est inclus dans l'anneau de w_a. Réciproquement si $f \in K(X)$ et $w_a(f) \geq 0$, alors $f = P_a^{v_{p_a}} \varphi_f$ et $v_{p_a}(f) \geq 0$, tandis que $\varphi_f = R/S$. On peut de plus, supposer que $P_a^{v_{p_a}}$ R et S sont dans A_s. On applique de nouveau la démonstration de la proposition précédente , comme $\hat{v}[S(a)] = n < \infty$ et $\hat{v}[P_a^{v_{p_a}} R(a)] \geq n$ (et peut être $\hat{v}[P_a^{v_{p_a}} R(a)] = \infty$, si $v_{p_a}(f) > 0$), on peut trouver un polynôme $T \in K[X]$, tel que $TP_a^{v_{p_a}(f)} R$ et TS soient dans A_s , mais $\hat{v}[TS(a)] = 0$, donc $TS \notin \eta_a$, ainsi $f \in (A_s)_{\eta_a}$.

Enfin, il est immédiat qu'on a la

Proposition 5.3. *Pour tout polynôme irréductible* P *de* K[X] , *le localisé* $(A_s)_{\tilde{p}}$ *est l'anneau de la valuation* P-*adique de* K(X).

[J.L.Chabert] a montré que les localisés de A_s sont les seuls anneaux de valuation qui le contiennent dans K(X).

§ 6. CORPS RESIDUELS.

Pour tout idéal de la forme η_a, le corps résiduel

A_s/η_a est isomorphe à k [cf. théorème 3.4.] . De plus :

Proposition 6.1. *Si* P *est un polynôme irréductible de* K[X] , *alors*

- *ou bien* P *n'a pas de racine dans* $\hat{A}$, $\tilde{P}$ *est maximal et* $A_s/\tilde{p} \cong K[X] / (P)$
- *ou bien* P *est contenu dans autant d'idéaux maximaux de la forme* η_{a_i} *que* P *a de racines* a_i *dans* $\hat{A}$; *alors* $B = A_s/\tilde{P}$ *est un anneau intègre semi-local, de dimension* 1 , *intégralement clos, de corps des fractions* L = K[X] / (P) , *contenant la fermeture intégrale* $\overline{A}$ *de* A *dans* L *et intersection de certains des anneaux de valuations qui sont extension immédiate de* v *à* L .

Preuve : Les inclusions résultent du §4. Il est clair aussi que le corps des fractions de $A_s/\tilde{P}$ est L, ce qui termine la démonstration dans le cas où P n'a pas de racine dans $\hat{A}$. Si par contre P a des racines $a_1, a_2, \ldots, a_n$ dans A, alors $\tilde{P} \subset \eta_{a_i}$ et on note $\overline{\eta}_{a_i}$ l'idéal $\eta_{a_i}/\tilde{P}$ de $A_s/\tilde{P}$. Le localisé $(A_s/\tilde{P})_{\overline{\eta}_{a_i}}$ est isomorphe au quotient de l'anneau de valuation de rang 2, $(A_s)_{\eta_{a_i}}$ par son idéal de hauteur 1, $(\tilde{P})_{\eta_{a_i}}$, c'est donc l'anneau d'une valuation discrète de rang 1 de son corps des fractions L ; on vérifie qu'il s'agit de la valuation $\overline{w}_{a_i}$ qui à tout $\overline{f}$ de L assigne la valeur

$$\overline{w}_{a_i}(\overline{f}) = v_{a_i}(f) = \hat{v}[f(a_i)]$$

où f est un relèvement de $\overline{f}$ dans K[X] ($\overline{w}_{a_i}(\overline{f})$ ne dépend pas

du choix de f, puisque $P_{a_i}(a_i) = 0$ donc $\hat{v}[P_{a_i}(a_i)] = \infty$). Il est clair que $\overline{w}_{a_i}$ est une extension immédiate de v à L : - même groupe des valeurs - le quotient par l'idéal maximal, isomorphe à A_s/η_{a_i}, est k . Ainsi les localisés de B en ses idéaux maximaux, en nombre fini, sont les anneaux de certaines extensions immédiates de v à L. B, qui est l'intersection de ces anneaux, est donc intégralement clos et contient $\overline{A}$ qui est l'intersection de toutes les extensions de v à L.

On montre sur un exemple que certaines extensions immédiates de v à L, peuvent ne pas figurer parmi les valuations essentielles de B :

Exemple 6.2. On prend pour A l'anneau $\mathbb{Z}_5$ de la valuation 5-adique de $\mathbb{Q}$, et pour P le polynôme :

$$P = 5^2 X^3 + X + 1 .$$

Modulo l'idéal maximal, on a :

$$\overline{P} = X + 1 \qquad \text{dans} \qquad \mathbb{Z}/5\mathbb{Z}$$

et d'après le lemme de Hensel, on a dans $\hat{\mathbb{Z}}_5$:

(*) $P = (X + a)R$ où $a \in \hat{\mathbb{Z}}_5$ relève 1, R est de degré 2.

Ainsi P a au moins une racine dans $\hat{A} = \hat{\mathbb{Z}}_5$. on va montrer qu'il n'en a qu'une, ainsi $B = A_s/\tilde{P}$ est un anneau local ; mais on va aussi montrer que la valuation 5-adique a trois extensions immédiates dans $L = \mathbb{Q}[X] / (P)$.

On considère en effet le polynôme

$$P_1 = 5^2(y/5)^3 + (y/5) + 1 = y^3/5 + y/5 + 1$$

et aussi le polynôme

$$P_2 = 5P_1 = y^3 + y + 5.$$

Si dans la clôture algébrique de $\mathbb{Q}$, les racines de P sont a,b,c, celles de P_2 sont $5a, 5b, 5c$. Modulo l'idéal maximal on a :

$$\overline{P}_2 = y^3 + y = y(y + 2)(y + 3) \quad , \quad \text{dans } \mathbb{Z}/5\mathbb{Z},$$

d'après le lemme de Hensel, les trois racines simples de $\overline{P}_2$ se relèvent dans $\hat{A} = \hat{Z}_5$; en d'autres termes, les trois racines $5a, 5b, 5c$ de P_2 sont distinctes et dans $\hat{\mathbb{Z}}_5$, ainsi les trois racines a,b,c de P sont dans la complétion $\hat{\mathbb{Q}}_5$ de $\mathbb{Q}$. On en déduit que la valuation 5-adique de $\mathbb{Q}$ a trois prolongements à L [N.Bourbaki. VI, §8, proposition 2] , et comme P est de degré 3, ces prolongements sont nécessairement des extensions immédiates (à cause de la formule $\Sigma\, e_i f_i = n$). Néanmoins B est local, car seule la racine a de P (d'après (*)) est dans $\hat{A}$; si en effet b était aussi dans $\hat{A}$, on aurait

$$P = 5^2 X^3 + X + 1 = 5^2(X - a)(X - b)(X - c),$$

dans $\hat{\mathbb{Q}}_5[X]$, mais comme $5c$, racine de P_2, est dans $\hat{\mathbb{Z}}_5$, on aurait dans $\hat{A}[X]$:

$$5^2 X^3 + X + 1 = 5(X - a)(X - b)(5X - 5c)$$

ou encore

$$5X^3 + X/5 + 1/5 = (X - a)(X - b)(5X - 5c) \in \hat{A}[X]$$

mais ce n'est pas vrai car $1/5 \notin \hat{Z}_5$.

§ 7. CORPS DE NOMBRES ALGEBRIQUES.

On passe facilement du local au global. Si A est un anneau de Dedekind, il résulte immédiatement de ce qui précède que pour tout polynôme irréductible P de K[X] , l'anneau $B = A_S/\tilde{P}$ est un anneau intégralement clos, de corps des fractions L = K[X] / (P) , et contenant la fermeture intégrale $\overline{A}$ de A dans L. Pour chaque idéal maximal $\mathfrak{m}$ de A, $\tilde{P}$ est contenu dans autant d'idéaux de A_S au-dessus de $\mathfrak{m}$, que P a de racines dans la complétion $\hat{A}_{\mathfrak{m}}$ de $A_{\mathfrak{m}}$. Lorsque A est l'anneau des entiers d'un corps de nombres, on veut montrer qu'il y a toujours une infinité d'idéaux maximaux $\mathfrak{m}$ de A, tels que P a des racines dans $\hat{A}_{\mathfrak{m}}$: dans ce cas, donc, l'idéal $\tilde{P}$ n'est jamais maximal.

Proposition 7.1. *Soit* A *l'anneau des entiers d'un corps de nombres* K , P *un polynôme irréductible de* K[X] . *Pour une infinité d'idéaux maximaux* $\mathfrak{m}$ *de* A , *l'idéal* $\tilde{P}$ *de* A_S *est contenu dans un idéal maximal de* A_S *au-dessus de* $\mathfrak{m}$.

Preuve : Dans la clôture algébrique de K , les racines de P sont en nombre fini ; il faut donc montrer qu'une même racine a appartient à une infinité de complétés $\hat{A}_{\mathfrak{m}}$. Il suffit de montrer que a appartient à $\hat{K}_{\mathfrak{m}}$, pour une infinité d'idéaux maximaux $\mathfrak{m}$ de A. Si en effet $a \in \hat{K}_{\mathfrak{m}}$, alors L = K(X) / (P) s'injecte canoniquement dans $\hat{K}_{\mathfrak{m}}$, la valuation $v_{\mathfrak{m}}$, d'anneau $A_{\mathfrak{m}}$, admet une extension immédiate $v'_{\mathfrak{m}}$ dans L, laquelle admet à son tour l'extension immédiate $\hat{v}_{\mathfrak{m}}$ dans $\hat{K}_{\mathfrak{m}}$. Comme

L est une extension finie de K, pour tout idéal $\mathfrak{m}$, sauf un nombre fini, $v'_{\mathfrak{m}}(a) = 0$ et donc aussi $\hat{v}_{\mathfrak{m}}(a) = 0$. Ainsi pour tout idéal $\mathfrak{m}$, tel que $a \in \hat{K}_{\mathfrak{m}}$, sauf un nombre fini, a est en fait dans $\hat{A}_{\mathfrak{m}}$. Comme on vient de le remarquer, si $a \in \hat{K}_{\mathfrak{m}}$, $v_{\mathfrak{m}}$ admet une extension immédiate dans $L = K(X) / (P)$ et ainsi $\mathfrak{m}$ est décomposé dans L ; réciproquement si $\mathfrak{m}$ est totalement décomposé dans L, $v_{\mathfrak{m}}$ admet nécessairement une extension immédiate dans L et ainsi P a une racine a dans $\hat{K}_{\mathfrak{m}}$ [N. Bourbaki. VI, §8, proposition 2.] . La proposition résulte donc du résultat classique suivant :

Si A *est l'anneau des entiers d'un corps de nombres* K , L *une extension finie de* K, *alors il y a une infinité d'idéaux premiers de* A *totalement décomposés dans* L .

On veut montrer ce résultat classique de façon simple.

- D'abord, il suffit de montrer que pour toute extension F finie de $\mathbb{Q}$, une infinité de valuations p-adiques ont une extension immédiate dans F. Si en effet K est un corps de nombres, L une extension finie de K alors soit F une extension galoisienne finie de Q contenant L. Une infinité de valuations p-adiques, celles qui ont une extension immédiate dans F , y sont donc totalement décomposées. A fortiori, les extensions de ces valuations p-adiques dans K sont totalement décomposées dans L.

- On peut écrire $F \cong \mathbb{Q}[X] / (P)$, où P est un polynôme irréduc-

tible de $\mathbb{Q}[X]$, qu'on peut toujours supposer à coefficients dans $\mathbb{Z}$. Il suffit de montrer que P a une racine dans $\hat{\mathbb{Z}}_p$, pour une infinité de premiers p.

- Pour montrer que P a une racine dans $\hat{\mathbb{Z}}_p$, on va montrer que P a une racine simple modulo p ; on peut alors appliquer le lemme de Hensel ; en fait, on peut ne pas s'inquiéter de la simplicité de cette racine, en effet P n'a des racines doubles modulo p que pour un nombre fini de p : si P' désigne le polynôme dérivé de P, comme P est irréductible, on peut trouver U et V dans $\mathbb{Z}[X]$ tels que :

$$UP + VP' = q, \quad q \in \mathbb{Z},$$

par réduction modulo p cela montre que $\bar{P}$ et $\bar{P}'$ sont premiers entre eux dans $\mathbb{Z}/p\,\mathbb{Z}[X]$, sauf pour les p, en nombre fini, tels que P, P' U, V ou q est nul modulo p.

- Si P n'avait des racines que modulo des premiers en nombre fini :

$$p_1, p_2, \ldots, p_n$$

alors pour tout élément x de $\mathbb{Z}$, $P(x)$ ne serait divisible que par ces premiers ; si par ailleurs :

$$P = a_0 + a_1 X + \ldots + a_k X^k$$

ou bien a_0 est nul, mais comme P est irréductible alors :

$$P = X, \quad \text{et} \quad \mathbb{Q}[X] / (P) = \mathbb{Q} \qquad \text{(cas trivial)}$$

ou bien on pose, en notant v_{p_i} la valuation p_i-adique :

$$v_{p_i}[a_0] = m_i, \quad \forall i \in (1, \ldots, n)$$

il est clair que si x, dans $\mathbb{Z}$, est tel que :

$$(*) \qquad v_{p_i}[x] > m_i \quad , \qquad \forall i \in (1,\ldots,n)$$

alors :

$$v_{p_i}[P(x)] = v_{p_i}[a_0] = m_i$$

on a donc :

$$P(x) = \pm \prod_{i=1}^{n} (p_i)^{m_i}$$

si x parcourt les éléments de $\mathbb{Z}$ qui remplissent la condition (*) , la valeur absolue $|P(x)|$ reste fixe ;pourtant on peut trouver une suite d'éléments de $\mathbb{Z}$, avec la condition (*) qui tendent vers l'infini (par exemple les puissances successives d'un tel élément) donc $|P(x)|$ devrait tendre aussi vers l'infini. On a donc une contradiction.

CHAPITRE VII - STRUCTURE MULTIPLICATIVE (FIN)

§ 1. PLUSIEURS VARIABLES.

On s'intéresse maintenant aux polynômes à plusieurs variables qui sont à valeurs entières. Comme au chapitre IV, §3, on note $A_{s,m}$ le sous anneau de $K[X_1,\ldots,X_m]$ formé par les polynômes P tels que $P(A^m) \subset A$.

Pour déterminer les idéaux premiers de $A_{s,m}$ on se restreint au cas local comme au chapitre précédent, dont on garde toutes les notations. On suppose aussi que le corps résiduel k de A est fini, sinon $A_{s,m} = A[X_1,\ldots,X_m]$. Encore une fois, on considère $A_{s,m}$ comme une A-algèbre.

La fibre au-dessus de (0) correspond au spectre de $A_{s,m} \otimes_A K = K[X_1,\ldots,X_m]$. Sans démonstration enonçons donc, surtout pour fixer les notations,

Proposition 1.1. *La fibre au-dessus de* (0) *de* $A_{s,m}$ *est en bijection avec les idéaux premiers de* $K[X_1,\ldots,X_m]$ *; à un idéal premier* $\mathfrak{P}$ *de* $K[X_1,\ldots,X_m]$ *correspond l'idéal premier* $\tilde{\mathfrak{P}} = \mathfrak{P} \cap A_{s,m}$ *de* $A_{s,m}$, *de même hauteur.*

Pour la fibre au-dessus de $\mathfrak{M}$ on suit la démarche du

chapitre précédent : on montre, mot pour mot de la même façon, que $A_{s,m}$ est dense dans l'anneau des fonctions continues $\mathcal{C}(\hat{A}^m, \hat{K})$. On conclut :

Proposition 1.2. *La fibre au-dessus de* $\mathfrak{m}$ *de* $A_{s,m}$ *est en bijection avec les points de* $\hat{A}^m$ *; à un point* $\underline{a} = (a_1, a_2, \ldots, a_m)$ *de* $\hat{A}^m$ *, correspond l'idéal* $\eta_{\underline{a}} = \{f \in A_{s,m} \mid f(a) \in \hat{\mathfrak{m}}\}$,

$\eta_{\underline{a}}$ *est maximal et* $A_s/\eta_{\underline{a}} \cong k$.

Corollaire 1.3. *Soit* $\underline{a}$ *un élément de* $\hat{A}^m$ *et* $\overline{\underline{a}} = (\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m) \in k^m$, *le* m*-tuple formé par les classes modulo* $\hat{\mathfrak{m}}$ *des éléments* $a_1, a_2, \ldots, a_m$ *de* $\hat{A}$ *, alors l'idéal* $\eta_{\underline{a}} \cap A[X]$, *est l'idéal maximal , de hauteur* $m + 1$ *de* $A[X]$, *formé des polynômes* f *de* $A[X]$, *dont la classe résiduelle* $\overline{f}$ *dans* $A/\mathfrak{m}[X]$, *est telle que* $\overline{f}(\overline{\underline{a}}) = 0$.

Si $\underline{a} \in \hat{A}^m$, on note $\mathfrak{p}_{\underline{a}}$ l'idéal premier de $K[X_1, \ldots, X_m]$ formé des polynômes nuls en $\underline{a}$. Comme

$$K[X_1, \ldots, X_m] / \mathfrak{p}_{\underline{a}} \cong K(a_1, \ldots, a_m),$$

il est clair que si $K(a_1, \ldots, a_m)$ est de degré de transcendance d sur K, alors $\mathfrak{p}_{\underline{a}}$ est de hauteur $m-d$.

Proposition 1.4. $\tilde{\mathfrak{p}}$ *est inclus dans* $\eta_{\underline{a}}$ *si et seulement si, pour tout* f_i *d'une famille de générateurs* $f_1, f_2, \ldots, f_k$ *de* $\mathfrak{p} \subset K[X_1, \ldots, X_m]$, *alors* $f_i(\underline{a}) = 0$.

Ainsi $\tilde{\mathfrak{p}} \subset \eta_{\underline{a}}$ si et seulement si $\mathfrak{p} \subset \mathfrak{p}_{\underline{a}}$.

Corollaire 1.5. *Si* d *est le degré de transcendance de* $K(a_1,\ldots,a_m)$ *sur* K *alors* $\eta_{\underline{a}}$ *est de hauteur* $m + 1 - d$ *dans* $A_{s,m}$.

Corollaire 1.6. *Si* $a_1,a_2,\ldots,a_m$ *sont algébriquement indépendants sur* K , *alors* $\eta_{\underline{a}}$ *est de hauteur* 1 , $(A_{s,m})_{\eta_{\underline{a}}}$ *est l'anneau de la valuation discrète* $v_{\underline{a}}$ *de* $K(X_1,\ldots,X_m)$ *qui à* f *associe la valeur*

$$v_{\underline{a}}(f) = \hat{v}[f(\underline{a})]$$

et $v_{\underline{a}}$ *est une extension immédiate de* v .

Plus généralement, pour tout $\underline{a}$, $\eta_{\underline{a}}/\wp_{\underline{a}}$ est un idéal maximal de hauteur 1 de l'anneau $B = A_{s,m}/\tilde{\wp}_{\underline{a}}$. Le localisé de B en cet idéal maximal est l'anneau de la valuation $\overline{w}_{\underline{a}}$ de $L = K[X_1,\ldots,X_m] / \wp_{\underline{a}}$ qui à un élément $\overline{f}$ de L associe la valeur, $\overline{w}_{\underline{a}}(\overline{f}) = \hat{v}[f(\underline{a})]$ pour un quelconque relèvement f de $\overline{f}$. $w_{\underline{a}}$ est une extension immédiate de v à L. Dans le cas où $\wp_{\underline{a}}$ est de hauteur 1, c'est-à-dire où $K(a_1,\ldots,a_m)$ est de degré de transcendance $m - 1$ sur K, alors $\wp_{\underline{a}}$ est principal engendré par un polynôme irréductible $P_{\underline{a}}$ de $K[X_1,\ldots,X_m]$ et $(A_{s,m})_{\eta_{\underline{a}}}$ est l'anneau d'une valuation de rang 2 de $K(X_1,\ldots,X_m)$, à valeurs dans $\mathbb{Z} \times \mathbb{Z}$, ordonné avec l'ordre lexicographique , et obtenue (comme au chapitre précédent, §5) par composition de la valuation $P_{\underline{a}}$-adique et de la fonction d'ordre $v_{\underline{a}}$, où $v_{\underline{a}}(f) = \hat{v}[f(\underline{a})]$.

Corollaire 1.7. *Si* $\wp$ *est un idéal premier de* $K[X_1,\ldots,X_m]$ *dont les générateurs n'ont pas de racine commune dans* $\hat{A}^m$, *et si de plus* $\wp$ *est maximal, alors* $\tilde{\wp}$ *est maximal et*

$A_{s,m} / \tilde{\mathfrak{P}} = L = K[X_1,\ldots,X_m] / \mathfrak{P}$.

Pour avoir un exemple, il suffit de considérer l'idéal $\mathfrak{P}$ engendré par $P_1, P_2,\ldots,P_m$, où P_i est un polynôme irréductible de la variable X_i, sans racine dans $\hat{A}$.

Corollaire 1.8. *Si $\mathfrak{P}$ est un idéal maximal de $K[X_1,\ldots,X_m]$ dont les générateurs ont des racines communes dans $\hat{A}$, celles-ci sont en nombre fini, $B = A_s/\tilde{\mathfrak{P}}$ est un anneau intégralement clos, semi-local, de corps des fractions $L = K[X_1,\ldots,X_m] / \mathfrak{P}$ et contenant la fermeture intégrale $\overline{A}$ de A dans L ; c'est l'intersection des anneaux de certaines extensions immédiates de v à L.*

En général si $\mathfrak{P}$ n'est pas maximal, $\mathfrak{P}$ peut être contenu dans une infinité d'idéaux du type $\eta_{\underline{a}}$ de hauteurs diverses : Si on fait $\mathfrak{P} = (X_1)$ dans $\mathbb{Q}[X_1,\ldots,X_m]$ (dans le cas où A est l'anneau $\mathbb{Z}_p$ de la valuation p-adique dans $\mathbb{Z}$) alors pour tout élément $\underline{a}_{(i)} = (0,0,\ldots,0,a_{i+1},\ldots,a_m)$ de $\mathbb{Z}_p^m$, où $a_{i+1},\ldots,a_m$ sont algébriquement indépendants sur $\mathbb{Q}$ (il y a donc une infinité de choix) $\mathfrak{P}$ est inclus dans $\eta_{\underline{a}_{(i)}}$ et $\eta_{\underline{a}_{(i)}}$ est de hauteur $i + 1$.

§ 2. FRACTIONS RATIONNELLES A VALEURS ENTIERES.

On s'intéresse maintenant aux fractions rationnelles à valeurs entières : si A est un anneau intègre de corps des fractions K, il s'agit des éléments f de $K(X)$, tels que $f(a) \in A$ pour

tout a où f a un sens. Bien sûr ces éléments forment un anneau. On le note A_R.

Proposition 2.1. *Pour tout anneau intègre* A , *qui n'est pas un corps, et toute fraction rationnelle à valeurs entières* $f \in A_R$, f *est partout définie sur* A .

Preuve : On écrit $f = P/Q$ sous sa forme irréductible et où $P, Q \in A[X]$. Si il y avait un élément a de A tel que f(a) ne soit pas défini, donc $Q(a) = 0$, alors on aurait $P(a) \neq 0$ (P/Q est irréductible). On pourrait trouver $b \in A$, tel que $P(a) / b \notin A$ (ou bien P(a) est une unité et alors b est n'importe quel élément non inversible de A, ou bien P(a) n'est pas inversible et on peut faire, par exemple , $b = P(a)^2$). On peut aussi trouver $c \in A$, tel que $Q(a + cb) \neq 0$, en effet Q n'a qu'un nombre fini de racines et A est de cardinal infini (A n'est pas un corps). Comme $P,Q \in A[X]$, alors $P(a + cb) = P(a) + ucb$ et $Q(a + cb) = 0 + vcb$ où $u,v \in A$, donc $P(a + cb) / Q(a + cb) = (P(a) + ucb)/ vcb$. Si f était dans A_R, comme f est définie en (a + cb) on aurait $f(a + cb) = (P(a) + ucb)/ vcb \in A$ donc $[P(a) / b] + uc \in A$, a fortiori, et donc aussi $P(a) / b \in A$ contrairement au choix de b.

Proposition 2.2. *Si* A *est l'anneau des entiers d'un corps de nombres alors* $A_R = A_S$.

Preuve : $A_S \subset A_R$. Inversement, si $f \in A_R$, alors, pour tout idéal maximal $\mathfrak{m}$ de A, f est une fonction continue (partout définie) de A dans $\hat{A}_{\mathfrak{m}}$, pour la topologie $\mathfrak{m}$-adique. Comme A est dense dans $\hat{A}_{\mathfrak{m}}$, f est aussi une fonction continue de $\hat{A}_{\mathfrak{m}}$ dans $\hat{A}_{\mathfrak{m}}$, ainsi $f \in (\hat{A}_{\mathfrak{m}})_R$ et en particulier, si $f = P/Q$ alors Q n'a pas de racine dans $\hat{A}_{\mathfrak{m}}$. Ceci étant vrai pour tout $\mathfrak{m}$, Q doit être une constante [cf. VI. proposition 7.1. et démonstration].

On s'intéresse maintenant au cas d'un anneau de valuation discrète A. On garde les notations du chapitre précédent et on veut étudier le spectre de A_R. On peut remarquer que $A_R \neq A_S$, par exemple $\pi/\pi + X^2 \in A_R$ (où π désigne encore une uniformisante de A). On peut donc aussi remarquer, d'après la proposition précédente :

Remarque 2.3. *Si* A *est un anneau intègre et* $\mathfrak{m}$ *un idéal maximal de* A, *alors* $(A_R)_{\mathfrak{m}}$ *peut différer de* $(A_{\mathfrak{m}})_R$.

Comme au chapitre précédent, on s'intéresse ici au cas où le corps résiduel k de A est de cardinal fini.

Cas de la fibre au-dessus de (0).

On introduit la partie multiplicative T de K[X], formée des polynômes qui n'ont pas de racine dans la complétion $\hat{A}$ de A,

Lemme 2.4. $A_R \otimes_A K = T^{-1} K[X]$.

Preuve : $A_R \otimes_A K \subset T^{-1}K[X]$ d'après la proposition 2.1., et si inversement $P / Q \in T^{-1}K[X]$, où $P \in A[X]$, $Q \in T$, alors Q , en tant que fonction de $\hat{A}$ dans $\hat{K}$ est continue ; comme Q ne s'annule pas et que $\hat{A}$ est compact, $\hat{v}[Q]$ reste bornée, ainsi il existe $n \in \mathbb{N}$ tel que $\pi^n / Q \in A_R$, et donc $\pi^n P / Q \in A_R$; ainsi $P/Q \in A_R \otimes_A K$.

Proposition 2.5. *Soit* A *l'anneau d'une valuation discrète de corps résiduel fini, la fibre au-dessus de* (0) *de* A_R *se compose de*

- *l'idéal* (0) , *de hauteur* 0
- *une famille d'idéaux premiers de hauteur* 1, *en bijection avec la famille des polynômes de* $K[X]$, *non constants, irréductibles, avec une racine au moins dans* $\hat{A}$, *et définis à la multiplication par un élément non nul de* K *près ; à un polynôme* P *correspond l'idéal* $\tilde{\tilde{P}}$

$$\tilde{\tilde{P}} = (P)T^{-1}K[X] \cap A_R = \{f \in A_R \mid f = Pg \ , \quad g \in T^{-1}K[X]\} \ .$$

Cas de la fibre au-dessus de $\mathfrak{m}$.

On a les inclusions évidentes $A_s \subset A_R \subset \mathcal{C}(\hat{A},\hat{A})$; ainsi, d'après le chapitre précédent.

Proposition 2.6. *Soit* A *l'anneau d'une valuation discrète de corps résiduel fini, les idéaux premiers de* A_R *au-dessus de* $\mathfrak{m}$ *sont en bijection avec les points de* $\hat{A}$ *; à un point* $a \in \hat{A}$, *correspond l'idéal*

$$\mu_a = \{f \in A_R \mid f(a) \in \hat{\mathfrak{m}}\}$$

μ_a *est maximal et* $A_s/\mu_a \cong k$.

Bien sûr $A_s \cap \mu_a$ est l'idéal η_a de A_s [cf. VI. théorème 3.4.].

Proposition 2.7. *Soit* A *l'anneau d'une valuation discrète de corps résiduel fini, l'idéal* $\tilde{\tilde{P}}$ *de* A_R *est inclus dans* μ_a *si et seulement si* $P(a) = 0$.

Preuve : Bien sûr, si $P(a) = 0$ alors $\tilde{\tilde{P}} \subset \mu_a$. Si inversement $\tilde{\tilde{P}} \subset \mu_a$ alors $\tilde{\tilde{P}} \cap A_s \subset \mu_a \cap A_s$ donc $\tilde{P} \subset \eta_a$ et $P(a) = 0$ [cf. VI. proposition 4.1.]

Ainsi : aucun idéal du type $\tilde{\tilde{P}}$ n'est maximal dans A_R, car seuls les polynômes de $K[X]$ qui ont une racine dans $\hat{A}$, donnent lieu à un idéal premier de A_R

- les idéaux μ_a et η_a ont même hauteur (dans A_R et A_s respectivement)

- comme $A_s \cap \mu_a = \eta_a$, alors $(A_R)_{\eta_a} = (A_s)_{\eta_a}$ est l'anneau de valuation décrit au chapitre VI., §5, discrète de rang 1 si a est transcendant, discrète de rang 2 si a est algébrique sur K.

- $A_R/\tilde{\tilde{P}} = A_s/\tilde{P}$ car c'est l'intersection des mêmes anneaux de valuation de $L = K(X) / (P)$.

§3. IDEAUX DE TYPE FINI.

On détermine ici, simultanément, les idéaux premiers de type fini des anneaux A_s et A_R, dans le cas où A est un anneau de

valuation discrète de corps résiduel fini. On en déduit quelques résultats plus généraux. On remarque d'abord :

Proposition 3.1. *Soit* A *l'anneau d'une valuation discrète de corps résiduel fini. Les anneaux* A_S *et* A_R *sont des anneaux de Prüfer.*

Preuve : Le localisé de A_S (ou A_R) en tout idéal maximal est en effet un anneau de valuation discrète de rang 1 ou 2 [cf. VI. §5] .

Par globalisation, on a :

Corollaire 3.2. *Soit* A *l'anneau des entiers d'un corps de nombres. Alors les anneaux* A_S *et* A_R *sont des anneaux de Prüfer.*

(dans ce cas $A_S = A_R$)

On peut remarquer que si A est un anneau de valuation discrète de corps résiduel infini, alors $A_S = A[X]$ n'est pas un anneau de Prüfer.

Au sujet des anneaux de Prüfer, on rappelle ici

Proposition 3.3. *Un idéal fractionnaire d'un anneau de Prüfer est inversible si et seulement si il est de type fini.*

[N.Bourbaki. VII. §2. Exercice 12]

L'étude des idéaux premiers de type fini est donc aussi celle des idéaux premiers inversibles.

Proposition 3.4. *Soit* A *l'anneau d'une valuation discrète de corps résiduel fini. Alors pour tout élément du complété* $\hat{A}$ *de* A , *l'idéal* η_a *de* A_s *(resp.* μ_a *de* A_R *) n'est pas de type fini.*

Preuve : Soient s éléments de η_a (resp. de μ_a) $f_1, f_2, \ldots, f_s$. On a donc $\hat{v}[f_i(a)] > 0$, $\forall i \in \{1,\ldots,s\}$, et comme les fonctions f_i sont continues et en nombre fini, il existe une boule de centre a, d'où on extrait $b \in \hat{A}$, $b \neq a$, tel que $\hat{v}[f_i(b)] > 0$, $\forall i \in \{1,\ldots,s\}$, ainsi les f_i sont aussi dans η_b (resp. dans μ_b) et n'engendrent pas η_a (resp. μ_a).

Proposition 3.5. *Soit* A *l'anneau d'une valuation discrète de corps résiduel fini, et* P *un polynôme irréductible de* K[X] . *Si* P *a une racine dans* $\hat{A}$, *alors l'idéal* $\tilde{P}$ *de* A_s *(resp. l'idéal* $\tilde{\tilde{P}}$ *de* A_R *) n'est pas de type fini.*

Preuve : Soit a une racine de P dans $\hat{A}$, alors $\tilde{P} \subset \eta_a$ (resp. $\tilde{\tilde{P}} \subset \mu_a$) [cf. VI. proposition 4.1. et VII. proposition 2.7.] ; ainsi $\tilde{P}_{\eta_a}$ (resp. $\tilde{\tilde{P}}_{\mu_a}$) est un idéal premier non maximal d'un anneau de valuation et n'est donc pas de type fini.

Corollaire 3.6. *Soit* A *un anneau de valuation discrète de corps résiduel fini ; alors aucun idéal premier de* A_R *n'est de type fini.*

[cf. §2]

Corollaire 3.7. *Soit* A *l'anneau des entiers d'un corps de nombres ; alors aucun idéal premier de* A_s *n'est de type fini.*

[cf. VI. §7] .

Par contre,

Proposition 3.7. *Soit* A *l'anneau d'une valuation discrète de corps résiduel fini et* P *un polynôme irréductible de* K[X]. *Si* P *n'a pas de racine dans* $\hat{A}$ *alors* $\tilde{P}$ *est un idéal premier de type fini de* A_s . *Si de plus on normalise* P *par la condition* $P \in A_s$, $P/\pi \notin A_s$, *alors* $\tilde{P}$ *est principal, engendré par* P , *si et seulement si* P(a) *est une unité de* A *pour tout élément* a *de* A .

Preuve : Si P n'a pas de racine dans $\hat{A}$, alors $\tilde{P}$ est maximal [cf. VI. corollaire 4.4.] . $\forall a \in \hat{A}$, $\exists f_a \in \tilde{P}$ et $f_a \notin \eta_a$; donc $f_a(a) \notin \hat{\mathfrak{m}}$. Comme $\hat{A}$ est compact et que les f_a sont continues, on peut en extraire un nombre fini $f_1,\ldots,f_s$ telles que $\forall x \in \hat{A}$, $\exists i \in \{1,\ldots,s\}$ et $f_i(x) \notin \hat{\mathfrak{m}}$. L'idéal $I = (f_1,\ldots,f_s,P)$ de A_s n'est donc inclus dans aucun idéal du type η_a de A_s ; et comme $P \in I$, il n'est pas non plus inclus dans aucun idéal du type $\tilde{Q}$, où Q est un polynôme irréductible distinct de P. En conclusion, $I_{\mathfrak{q}} = \tilde{P}_{\mathfrak{q}} = (A_s)_{\mathfrak{q}}$ pour tout idéal maximal $\mathfrak{q}$ de A_s , $\mathfrak{q} \neq \tilde{P}$; et comme $f_1,f_2,\ldots,f_s$ et P sont dans $\tilde{P}$, et que réciproquement $P \in I$, alors $I_{\tilde{P}} = \tilde{P}_{\tilde{P}} = (P)\ K[X]$. Les localisés de I et de $\tilde{P}$, étant les mêmes en tout idéal maixmal de A_s, $I = \tilde{P}$ et $\tilde{P}$ est de type fini. De plus, si $P(a) \notin \mathfrak{m}$, $\forall a \in A$, il est clair que $P(a) \notin \hat{\mathfrak{m}}$,

$\forall a \in \hat{A}$, et que déjà l'idéal $(P)A_S$ de A_S a mêmes localisés que $\tilde{P}$ en tout idéal maximal de A_S. Si par contre $\exists a \in A$ tel que $P(a) \in \mathfrak{M}$, et si $\tilde{P}$ était principal, engendré par Q, Q engendrerait aussi bien l'idéal (P) de $K[X]$, on aurait donc $Q = kP$, où $k \in K$ et même $k \in A$, puisque $Q \in A_S$ mais $P/\pi \notin A_S$ et donc $Q(a) \in \mathfrak{M}$, mais alors $Q \in \eta_a$, donc $\tilde{P} \subset \eta_a$ et $\tilde{P}$ ne serait pas maximal contrairement à l'hypothèse.

§4. GROUPE DE PICARD.

Dans tout ce paragraphe, A désigne un anneau de valuation discrète de corps résiduel fini.

Proposition 4.1. *Le groupe de Picard de A_R est trivial. Celui de A_S est engendré par les classes des idéaux de type $\tilde{P}$ maximaux et non principaux ; c'est un groupe abélien, sans torsion, et il n'est pas de type fini.*

Preuve :

- *Si $\mathfrak{a}$ est un idéal fractionnaire de type fini de A_S (resp. de A_R), on peut trouver des polynômes $f_1, f_2, \ldots, f_s$ de $K[X]$ tels que $f_1, f_2, \ldots, f_s$ n'aient pas de diviseur commun dans $K[X]$, et l'idéal fractionnaire $\mathfrak{b} = (f_1, f_2, \ldots, f_s)$ de A_S (resp. de A_R) soit dans la même classe du groupe de Picard que $\mathfrak{a}$.*

En effet, $\mathfrak{a} = (g_1, g_2, \ldots, g_s)$. Comme $K[X]$ est principal, $\mathrm{Pic}(K[X])$ est trivial et $(g_1, g_2, \ldots, g_s)$ est principal en tant qu'idéal fractionnaire de $K[X]$. Ainsi, il existe $h \in K(X)$, tel que si on pose $f_n = hg_n$, alors $(f_1, f_2, \ldots, f_s)\, K[X] = K[X]$.

- *Il existe un polynôme* f *de* $K[X]$, *tel que* $\forall a \in \hat{A}$, *l'idéal* $\mathfrak{b}$ *de* A_s (*resp. de* A_R), *et l'idéal fractionnaire principal* (f) *aient même localisé* $\mathfrak{b}_{\eta_a} = (f)_{\eta_a}$ *dans* $(A_s)_{\eta_a}$ (*resp.* $\mathfrak{b}_{\mu_a} = (f)_{\mu_a}$ *dans* $(A_R)_{\mu_a}$).

On note n_a l'entier :

$$n_a = \mathrm{Inf}_{i=1}^{s} \left\{ \hat{v}[f_i(a)] \right\}.$$

Comme $f_1, f_2, \ldots, f_s$ sont des polynômes, n_a est bien défini, et $n_a < \infty$ puisque $f_1, \ldots, f_s$ n'ont pas de diviseur commun, en particulier les f_i ne s'annulent pas tous en a car le polynôme minimal P_a de a ne peut tous les diviser. La fonction g de $\hat{A}$ dans $\hat{K}$, telle que $g(a) = \pi^{n_a}$, $\forall a \in \hat{A}$ est bien sûr continue. Comme $\hat{A}$ est compact, $\exists N \in \mathbb{N}$ tel que $n_a < N$, $\forall a \in \hat{A}$, et comme $K[X]$ est dense dans $\mathcal{C}(\hat{A}, \hat{K})$, $\exists f \in K[X]$, tel que $\hat{v}[f(a) - g(a)] > N$, $\forall a \in \hat{A}$, soit donc $\hat{v}[f(a)] = n_a$. Par ailleurs $(A_s)_{\eta_a}$ (resp. $(A_R)_{\mu_a}$) est l'anneau d'une valuation discrète de rang 1 ou 2. Dans le cas de rang 1, notant v_a cette valuation, on a bien $v_a[(f)] = v_a[\mathfrak{b}] = n_a$. Dans le cas de rang 2, notant w_a cette valuation, puisque $f_1, \ldots, f_s$ n'admettent pas P_a comme diviseur commun, et que P_a ne divise pas davantage f (en effet

$f(a) \neq 0)$, on a aussi

$$w_a[(f)] = w_a[\mathfrak{b}] = (0, n_a) \qquad \text{[cf. VI. §5].}$$

Le groupe de Picard de A_s *est engendré par les classes des idéaux de type* $\tilde{P}$ *qui sont maximaux. Celui de* A_R *est trivial.*

Les seuls idéaux maximaux de A_R sont les idéaux du type μ_a. Comme $(f)_{\mu_a} = \mathfrak{b}_{\mu_a}$, $\forall a \in \hat{A}$, alors $\mathfrak{b} = (f)$ et ainsi tout idéal fractionnaire de type fini $\mathfrak{a}$ de A_R est dans la classe d'un idéal principal $\mathfrak{b} = (f)$.

Dans le cas de A_s , maintenant, on décompose f en facteurs irréductibles de $K[X]$: $f = \prod_{i=1}^{s} P_i^{n_i} \prod_{j=1}^{r} P_j^{n_j}$ où les s premiers facteurs correspondent aux polynômes P_i sans racine dans $\hat{A}$, c'est à dire tels que $\tilde{P}_i$ soit maximal. L'idéal $\mathfrak{t} = (f) \prod_{i=1}^{s} \tilde{P}_i^{-n_i}$ de A_s est donc tel que pour tout idéal maximal du type $\tilde{P}$ de A_s, on a $(\mathfrak{t})_{\tilde{P}} = (A_s)_{\tilde{P}}$. Comme par ailleurs $\mathfrak{b}$ a précisément été choisi, dans la classe de $\mathfrak{a}$, pour satisfaire $(\mathfrak{b})_{\tilde{P}} = (A_s)_{\tilde{P}}$, on a $(\mathfrak{t})_{\tilde{P}} = (\mathfrak{b})_{\tilde{P}}$. Par ailleurs, on a encore, $\forall a \in \hat{A}$, $(\mathfrak{t})_{\eta_a} = (f)_{\eta_a} = (\mathfrak{b})_{\eta_a}$, car $(\tilde{P}_i)_{\eta_a} = (A_s)_{\eta_a}$, $\forall i \in \{1, \ldots, s\}$.

Ainsi $\mathfrak{t} = \mathfrak{b}$. La classe d'un idéal fractionnaire de type fini $\mathfrak{a}$ de A_s est donc aussi celle de $\mathfrak{t}$, et aussi celle de $\prod_{i=1}^{s} \tilde{P}_i^{-n_i}$.

Le groupe de Picard A_s *est en fait engendré par les*

classes des idéaux de type $\tilde{P}$ *maximaux, mais non principaux, c'est-à-dire correspondant à des polynômes irréductibles* P *de* $K[X]$, *tels que* $P \in A_s$, $P/\pi \notin A_s$, P *n'a pas de racine dans* $\hat{A}$ *et* $\exists a \in A$ *vérifiant* $P(a) \in \mathfrak{M}$.

C'est évident [cf. proposition 3.7.]

Bien sûr $Pic(A_s)$ est abélien ; de plus ,

$Pic(A_s)$ *est sans torsion.*

Tout idéal fractionnaire de type fini, on l'a vu, est dans la même classe que $\mathfrak{b} = \tilde{P}_1^{k_1} \ldots \tilde{P}_s^{k_s}$. Où $k_i \in \mathbb{N}$, $k_i \leq 0$, $\forall i \in \{1,\ldots,s\}$. Si $\mathfrak{a}^n$ est principal, il en est de même de $\mathfrak{b}^n$ et un générateur de $\mathfrak{b}^n$ est de la forme $g = kP_1^{nk_1} \ldots P_s^{nk_s}$, où $k \in K$ et nécessairement $\hat{v}[g(a)] = 0$, $\forall a \in \hat{A}$. Si donc on pose $f = P_1^{k_1} \ldots P_s^{k_s}$, on a $0 = \hat{v}[g(a)] = \hat{v}(k) + n\,\hat{v}[f(a)]$, $\forall a \in \hat{A}$, ainsi $\hat{v}(k)$ est divisible par n, et si on pose aussi $f' = \pi^{\hat{v}(k)/n} f$, alors $\hat{v}[f'(a)] = 0$, $\forall a \in \hat{A}$, on en conclut facilement que (f') $A_s = \tilde{P}_1^{k_1} \ldots \tilde{P}_s^{k_s} = \mathfrak{b}$. Donc $\mathfrak{b}$ lui-même est principal, et $\mathfrak{a}$ est principal.

$Pic(A_s)$ *n'est pas de type fini.*

Si $Pic(A_s)$ était de type fini, il pourrait être engendré par les classes de $\tilde{P}_1, \tilde{P}_2, \ldots, \tilde{P}_s$, un système fini de générateurs. Comme les idéaux $\tilde{P}_i$ sont maximaux, les polynômes correspondant P_i n'ont pas de racine dans $\hat{A}$, et on trouve un nombre $n \in \mathbb{N}$, tel que

$$\forall m \geq n \ , \quad \hat{v}[P_i(\pi^m)] = \hat{v}[P_i(0)] = a_i < \infty \quad , \forall i \in 1,\ldots,s \ .$$

Si maintenant p et q sont deux nombres premiers tels que $q > (n+1)p$, on pose $P = X^p + \pi^q$. Il est clair que P est irréductible dans $K[X]$, car $[K[X] / (P) : K]$ doit être égal à p (en effet si v' est un prolongement de v à $L = K[X] / (P)$, et x la classe de X dans L, $v'(x) = q/p$, donc l'indice de ramification de v' par rapport à v est p) ; $P \in A[X]$, donc $P \in A_s$, et $P/\pi \notin A_s$ car $P/\pi\,(1) = \dfrac{1 + \pi^q}{\pi} \notin A$; P n'a pas de racine dans $\hat{A}$, car pour une telle racine a on aurait $\hat{v}(a) = q/p$ et donc $\hat{v}$ ne pourrait pas être une extension immédiate de v. Ainsi $\tilde{P}$ est maximal, et non principal car $P(\pi) = \pi^p + \pi^q \in \mathfrak{M}$. De plus, pour tout choix d'entiers relatifs $z_1, z_2, \ldots, z_s$, alors $\mathfrak{A} = \tilde{P}_1^{z_1}\ \tilde{P}_2^{z_2} \ldots \tilde{P}_s^{z_s}\ \tilde{P}$ n'est pas un idéal fractionnaire principal. S'il l'était, un générateur serait de la forme $f = k\, P_1^{z_1}\ P_2^{z_2} \ldots P_s^{z_s}\ P$, $f \in K(X)$ et $\hat{v}[f(a)] = 0$, $\forall a \in \hat{A}$. En particulier, on aurait

$$\hat{v}[f(\pi^n)] = \hat{v}(k) + \sum_{i=1}^{s} \hat{v}[P_i(\pi^n)^{z_i}] + \hat{v}[(\pi^{np} + \pi^q)]$$

et comme $\hat{v}[P_i(\pi^n)] = a_i$ et $np < q$, alors :

$$0 = \hat{v}[f(\pi^n)] = \hat{v}(k) + \sum_{i=1}^{s} a_i z_i + np$$

De même

$$0 = \hat{v}[f(\pi^{n+1})] = \hat{v}(k) + \sum_{i=1}^{s} a_i z_i + (n+1)p$$

car

$$\hat{v}[P_i(\pi^{n+1})] = a_i \quad \text{et} \quad (n+1)p < q. \quad \text{Ainsi,}$$

$$0 = \hat{v}[f(\pi^{n+1})] - \hat{v}[f(\pi^n)] = p,$$

mais $p \neq 0$. Contradiction. La classe de $\tilde{P}$ n'est pas dans le sous-

groupe engendré par les classes de $\tilde{P}_1, \tilde{P}_2, \ldots, \tilde{P}_s$.

Remarque : $\widetilde{(X^2 - \pi)}$ et $\widetilde{(X^3 - \pi)}$, qui sont maximaux et non principaux, sont dans la même classe de $\mathrm{Pic}(A_s)$. En effet, $f = X^2 - \pi / X^3 - \pi$ est tel que $\hat{v}[f(a)] = 0$, $\forall a \in \hat{A}$; il en résulte facilement que $(f)A_s = \widetilde{(X^2 - \pi)} / \widetilde{(X^3 - \pi)}$.

BIBLIOGRAPHIE

1. ACZEL, J. Uber die Gleichheit der Polynomfunctionen auf Ringen. Act. Sci. Math., 21, (1960), p. 105-107.

2. AMICE, Y. Interpolation p-adique. Bull. Soc. Math. France. 92, (1964), p. 117-180.

3. BOURBAKI, N. [Bbki] . Algèbre commutative. Paris, Hermann.

4. BOURBAKI, N. Topologie générale. Paris, Hermann.

5. CAHEN, P.J. [P.J.C. (1)] . Torsion theory and associated primes. A paraître, Proc. Amer. Math. Soc.

6. CAHEN, P.J. [P.J.C. (2)] . Commutative torsion theory. A paraître. Aussi Queen's Math. Preprints, no 7, 9, 17 (1972).

7. CAHEN, P.J. et CHABERT J.L. [Cah & Cha] . Coefficients et valeurs d'un polynôme. Bull. Sci. Math. 95, (1971), p. 295-304.

8. CHABERT, J.L. [CHABERT] . Anneaux de polynômes à valeurs entières et anneaux de Fatou. Bull. Soc. Math. France 99, (1971), p. 273-283.

9. CHABERT, J.L. Anneaux de polynômes à valeurs entières. Colloque d'Algègre de Rennes (1972), exposé no 8.

10. EAKIN, P. A note on finite dimensional subrings of Polynomial rings. Proc. Amer. Math. Soc. 31, (1972), p. 75-79.

11. GUNJI, H. and McQUILLAN, D.L. On polynomials with Integer Coefficients. Journal of Number theory 1, (1969), p. 486-493.

12. GUNJI, H. and McQUILLAN, D.L. On a class of Ideals in an Algebraic Number Field. Journal of Number theory 2, (1970), p. 207-221.

13. GABRIEL, P. Des catégories abéliennes.
Bull. Soc. Math. France 90, (1962), p. 323-448.

14. HARTSHORNE, R. Residues and Duality.
Springer Verlag Lecture Notes, no 41.

15. HILBERT, D. Die theorie der algebraischen Zahlkörpern.
Jahresbreit der Deutschen Math. Vereignung.
4, (1897), p. 175-546.

16. HILY, J. Polynômes à valeurs entières.
Séminaire Delange Pisot 4, (1962-63), no 1.

17. LAMBEK, J. Torsion theories, additive semantics and rings of quotients.
Springer Verlag Lecture Notes, no 177.

18. LAZARD, D. Autour de la platitude.
Bull. Soc. Math. France 97, (1969), p. 81-128.

19. LIND, D.A. Which polynomials over an algebraic number field map the algebraic integers into themselves ?
Amer. Math. Monthly 78, (1971).

20. MacCLUER, C.R. Common divisors of values of polynomials.
Journal of Number Theory 3, (1971), p. 33-34.

21. MATSUMARA, H. Commutative Algebra.
New-York, Benjamin.

22. MAHLER, K. An interpolation series for a continous function of a p-adic variable.
J. fur Reine und angew. math. 199, (1958), p. 23-34.

23. NORTHCOT, D.G. An Introduction to Homological Algebra.
Cambridge University Press.

24. OHM, J. Noetherian Intersection of integral domains.
Trans. Amer. math. soc. 167, (1972), p. 291-307.

25. OSTROWSKI, A. Über ganzwertige Polynome in algebraishen Zahlkörpern.
J. Reine Angew. Math., 149, (1919), p. 117-124.

26. POLYA, P. Über ganwwertige Polynome in algebraishen Zahlkörpern.
J. Reine Angew. Math. 149, (1919), p. 97-115.

27. SAMUEL, P. Théorie algébrique des Nombres.
Paris, Hermann.

28. SERRE, J.P. Algèbre locale.multiplicités.
Springer Verlag Lecture Notes no 11.

29. STORRER, H.H. Torsion theories and dominant dimension.
Springer Verlag Lecture Notes no 177. Appendix.

30. TACHIKAWA, H. On dominant dimension of QF.3 Algebras.
Trans. Amer. Math. Soc. 112, (1964), p. 249-266.

31. ZARISKI, O. et SAMUEL, P. Commutative Algebra.
Princeton, D. Van Nostrand.

TABLE DES MATIERES