Séminaire Dubreil.
Algèbre et théorie
des nombres

Pierre Samuel

Généralités sur l'algèbre locale

Séminaire Dubreil. Algèbre et théorie des nombres, tome 5-6 (1951-1953), exp. nº 1, p. 1-9
<http://www.numdam.org/item?id=SD_1951-1953__5-6__A1_0>

I. GÉNÉRALITÉS SUR L'ALGÈBRE LOCALE

par Pierre SAMUEL

INTRODUCTION. - L'algèbre locale s'occupe des problèmes du type suivant : "étude d'une courbe (ou d'une variété) au voisinage d'un point". Comme chacun sait, l'outil principal d'une telle étude est le développement de Taylor. Plus précisément, on considère les fonctions (rationnelles ou méromorphes) sur la courbe C qui ne sont pas infinies au point considéré P ; celles-ci forment un anneau A (par exemple l'anneau des fractions rationnelles $a(X)/b(X)$ telles que $b(0) \neq 0$, s'il s'agit de l'origine sur la droite OX) ; cet anneau A est un anneau <u>local</u>, c'est-à-dire que ses éléments non inversibles (ici les fonctions nulles en P) forment un <u>idéal</u> M , qui est alors le plus grand des idéaux non triviaux de A . D'autre part, on considère les développements de Taylor des éléments de A en fonction d'un certain nombre de paramètres (t_i) (indépendants ou non) ; ceux-ci appartiennent à l'anneau A' des séries entières en les (t_i) qui sont convergentes au voisinage de P ; or il se trouve que les (t_i) forment un système de générateurs de l'idéal maximal M de A ; donc, si l'on munit A de la topologie pour laquelle les idéaux M^n forment un système fondamental de voisinages de 0 , et A' de la topologie analogue définie par les idéaux $A'M^n$, l'anneau A est <u>partout dense</u> dans A' . L'avantage de A' sur A est que diverses opérations, qui feraient sortir de A , ne font pas sortir de A' .

D'autre part diverses particularités du voisinage de P sur C , qui n'étaient pas visibles dans l'anneau A , le deviennent dans l'anneau A' : par exemple, lorsque P est un point double ordinaire d'une courbe algébrique plane, l'anneau A est un anneau d'intégrité, mais l'anneau A' possède des diviseurs de zéro (les fonctions holomorphes nulles sur l'une des branches de C et non nulles sur l'autre).

Dans tout ceci la propriété que les séries entières, éléments de A', sont <u>convergentes</u> au voisinage de P est d'importance secondaire. Ce fait est singulièrement heureux, car il va nous permettre d'opérer sur un corps de base quelconque, où les notions de voisinage et de convergence n'auront plus de sens. Dans ce cas on pourra toujours définir l'anneau local d'un point P sur une courbe algébrique C , et, plus généralement, l'anneau local d'une sous-variété W sur une variété V . Soient A cet anneau, M son idéal maximal. A la place de l'anneau A' des séries convergentes en les (t_i) , on introduit le <u>complété</u> $\hat{A}$ de A pour la topologie définie par les idéaux M^n ; c'est un anneau de séries formelles (en des variables indépendantes ou non), et il contient A' lorsque A' existe. Par définition on dira que les propriétés de l'anneau $\hat{A}$ sont les propriétés <u>analytiques</u> de V au voisinage de W : par exemple, et pour suivre l'analogie avec le cas classique, on dira que V est <u>analytiquement réductible</u> (ou <u>irréductible</u>) au voisinage de W lorsque l'anneau $\hat{A}$ a (ou n'a pas) de diviseurs de zéro ; dans ce cas les idéaux premiers minimaux de $\hat{A}$ (qui décrivent la répartition des diviseurs de zéro dans $\hat{A}$) seront appelés les <u>nappes</u> (ou branches) analytiques de V au voisinage de W .

Mais la situation que nous venons de décrire (un anneau local A et son complété $\hat{A}$) ne se rencontre pas seulement en géométrie algébrique. Considérons un nombre premier p , et l'anneau A des nombres rationnels de la forme a/b (a , b entiers, b non multiple de p) ; c'est un anneau local dont l'idéal maximal est Ap ; son complété n'est autre que l'anneau Z_p des entiers p-adiques. On peut ainsi dire que l'étude des entiers p-adiques est "l'étude analytique de l'ensemble des nombres premiers au voisinage du nombre premier p ".

D'autre part l'anneau local complété $\hat{A}$ peut quelquefois s'obtenir directement, soit à partir de l'anneau R des fonctions polynômes sur V , soit à partir de l'anneau Z des entiers, par complétion par rapport à la topologie définie par les idéaux I^n (I : idéal des fonctions de R nulles au point P , ou idéal engendré par p) ; par exemple l'anneau des séries formelles à n variables sur un corps K s'obtient par complétion de l'anneau des polynômes à n variables sur K . Ceci nous amène à la situation plus générale suivante ; on a un anneau A et un idéal M de A tel que $\bigcap_{n=1}^{\infty} M^n = (0)$. Les idéaux M^n définissent alors une topologie <u>séparée</u> sur A ; on dit que A , muni de l'idéal M et de cette topologie, est un <u>anneau M-adique</u> ; on peut alors former l'anneau complété $\hat{A}$ de l'anneau M-adique A . Les anneaux M-adiques ont été introduits par Zariski pour étudier les situtations suivantes : on a un nombre fini (P_i) de points d'une variété algébrique V , et l'on veut étudier V au voisinage de chacun des P_i (on prend alors pour A l'anneau des polynômes sur V et pour M l'idéal des polynômes nuls en l'un au moins des P_i) ;

on a une sous-variété W d'une variété algébrique V, et l'on veut étudier V au voisinage de chaque point de W (on prend pour A l'anneau des polynômes sur V, et pour M l'idéal des polynômes nuls sur W ; alors, lorsque W n'est pas un point (c'est-à-dire lorsque l'idéal premier M n'est pas maximal), l'anneau complété $\hat{A}$ de l'anneau M-adique A est distinct de l'anneau local complété de W sur V ; l'anneau $\hat{A}$ est l'anneau des fonctions sur V qui sont "holomorphes" (au sens de Zariski) en chaque point de W).

Dans le reste de cet exposé, nous allons passer rapidement en revue les divers points de vue qui se sont montrés féconds dans l'étude des anneaux locaux et M-adiques [1].

1. Les anneaux de formes.

Soit A un anneau M-adique. Pour tout élément non nul a de A, il existe un exposant s et un seul tel que $a \in M^s$, $a \notin M^{s+1}$; la classe $\bar{a}$ de a dans M^s/M^{s+1} est appelée la forme initiale de a. Etant donnés des éléments $\bar{x} \in M^n/M^{n+1}$ et $\bar{y} \in M^s/M^{s+1}$, et des éléments x et y de A ayant $\bar{x}$ et $\bar{y}$ pour formes initiales, la forme initiale de xy dans M^{n+s}/M^{n+s+1} ne dépend que de $\bar{x}$ et $\bar{y}$. Ceci définit le produit de $\bar{x}$ et $\bar{y}$; en étendant par linéarité cette multiplication aux éléments de la somme directe $F(M) = \sum_{n=0}^{\infty} M^n/M^{n+1}$, on obtient sur $F(M)$ une structure d'anneau commutatif ; on dit que $F(M)$ est l'anneau de formes de l'idéal M (La construction de $F(M)$ rentre dans le procédé général de formation d'un anneau gradué à partir d'un anneau filtré ; cf. LERAY, CARTAN).

Lorsque I est un idéal fermé de A, A/I est un anneau $((M + I)/I)$-adique, dont l'anneau de formes est le quotient de $F(M)$ par l'idéal "directeur" de I (idéal engendré par les formes initiales d'éléments de I).

Les propriétés suivantes font partie de la théorie élémentaire des anneaux de formes :

a. Si $F(M)$ est un anneau d'intégrité, il en est de même de A (réciproque fausse). En particulier, si I est un idéal fermé de A dont l'idéal directeur soit premier, I est premier.

---

(1) Pour les démonstrations des résultats mentionnés, voir :

SAMUEL (Pierre). - Algèbre locale. - Paris, Gauthier-Villars 1953 (Mémorial des Sciences mathématiques n° 123).

b. Si tout idéal principal de A est fermé, et si $F(M)$ est un anneau d'intégrité intersection d'anneaux de valuations à groupes des ordres archimédiens, alors A est un anneau d'intégrité intégralement clos (si y/x est entier sur A on montre que $y \in Ax$ par approximations successives). Ceci montre que l'anneau local d'un point simple est intégralement clos.

c. Si A est un anneau M-adique complet, si A/M est noethérien, et si M a un système fini de générateurs, alors A est noethérien (on remarque que $F(M)$ est noethérien en tant que quotient d'un anneau de polynômes sur A/M ; puis on montre par approximations successives que, si des éléments (b_i) d'un idéal B de l'anneau complet A sont tels que l'idéal directeur de B soit engendré par les $(\bar{b}_i)$, alors les (b_i) engendrent B). Ceci montre en particulier qu'un anneau de séries formelles sur un anneau noethérien est noethérien ; il semble que ce soit là la démonstration la plus naturelle de ce théorème.

La théorie fine des anneaux de formes comprend essentiellement l'étude des polynômes caractéristiques. On suppose ici que A/M est un anneau de longueur finie (au sens Jordan-Hölder). Alors la longueur de A/M^n (c'est-à-dire aussi celle de M^{n-1}/M^n) est un polynôme en n pour n assez grand, soit $P_M(n)$. Si M et M' définissent la même topologie sur A, les polynômes P_M et $P_{M'}$ ont même degré d, appelé la <u>dimension</u> de A. Le terme de plus haut degré de $P_M(n)$ est de la forme $e(M).n^d/d'$, où $e(M)$ est un entier, appelé la multiplicité de l'idéal M'. On étudie les dimensions et multiplicités par passage des anneaux quotients de la forme A/Ax, x étant convenablement choisi ; et l'on montre que, lorsque A est un anneau local, sa dimension est égale au nombre minimum de générateurs d'un idéal primaire pour son idéal maximal (CHEVALLEY) et aussi à la longueur d'une chaîne maximum d'idéaux premiers emboités de A (KRULL) ; on obtient aussi une caractérisation de certaines multiplicités ; enfin l'on constate que, dans certains cas simples, la multiplicité de M est égale à la longueur de A/M. Tout ceci peut servir dans la théorie des multiplicités d'intersection des variétés algébriques et algébroïdes.

2. <u>Les idéaux fermés</u>.

On se borne ici au cas où A est un anneau <u>noethérien</u>, et l'on utilise le théorème suivant de Krull : soient A un anneau noethérien et M un idéal de A, pour que $\bigcap_{n=1}^{\infty} M^n = (0)$, il faut et il suffit qu'aucun élément de $1 + M$ ne soit diviseur de zéro dans A.

On en déduit que, pour qu'un idéal I de l'anneau M-adique A soit fermé, il faut et il suffit que l'on ait $P_i + M \neq A$ pour tout idéal premier P_i de I. Plus généralement l'adhérence de I est l'intersection de celles des composantes primaires Q_i de I dont l'idéal premier associé P_i satisfait à $P_i + M \neq A$.

En particulier, pour que tout idéal I de l'anneau M-adique A soit fermé, il faut et il suffit que M soit contenu dans l'intersection des idéaux maximaux de A (c'est-à-dire le radical de A), ou encore que tout élément de $1 + M$ soit inversible. On dit qu'un tel anneau M-adique est un <u>anneau de Zariski</u>. Un anneau M-adique noethérien et complet est un anneau de Zariski (car l'élément $1 - m$ de $1 + M$ admet $1 + m + m^2 + \dots$ pour inverse).

Un autre exemple d'anneau de Zariski est le suivant : A est un anneau noethérien ayant un nombre fini d'idéaux maximaux, et M est l'intersection de ceux-ci. On dit alors que A est un anneau semi-local, un anneau local est semi-local. Pour qu'un anneau M-adique de Zariski A soit semi-local, il faut et il suffit que A/M soit un anneau de longueur finie.

A la théorie des idéaux fermés se rattachent les propriétés relatives aux idéaux de A et de son complété $\hat{A}$. Si A est un anneau M-adique, $\hat{A}$ est un anneau M-adique, où $\hat{M}$ est l'idéal $\hat{A}M$ engendré par M dans $\hat{A}$, et aussi l'adhérence de M dans $\hat{A}$; on a $\hat{M}^n = \hat{A}.M^n$ et $M^n = \hat{M}^n \cap A$. Comme tout idéal de $\hat{A}$ est fermé, l'adhérence d'un idéal I de A (dans A) est $\hat{A}.I \cap A$; donc $\hat{A}.I \cap A = I$ lorsque A est anneau de Zariski. D'autre part, lorsque I est un idéal et c un élément d'un anneau de Zariski A, on a

$$(\hat{A}I : \hat{A}c) = \hat{A}.(I : Ac) \quad \text{et} \quad \hat{A}I \cap \hat{A}c = \hat{A}(I \cap Ac) \quad ,$$

en particulier si c n'est pas diviseur de zéro dans l'anneau de Zariski A, il n'est pas diviseur de zéro dans le complété $\hat{A}$. Lorsque I et J sont des idéaux de A, on a le résultat plus précis suivant :

$$\hat{A}I \cap \hat{A}J = \hat{A}.(I \cap J) \quad .$$

Pour démontrer ce dernier résultat on se sert du résultat suivant (qui exprime une propriété de compacité) : si A est un anneau semi-local et complet, si M est l'intersection des idéaux maximaux de A, et si (I_n) est une suite décroissante d'idéaux de A telle que $\bigcap_{n=1}^{\infty} I_n = (0)$, on a $I_n \subset M^{s(n)}$ où $s(n)$ tend vers l'infini avec n. Ce résultat est aussi utile pour montrer qu'un sous-anneau d'un anneau M-adique en est un sous-espace topologique.

3. Extension finie d'anneaux M-adiques.

Soient A un anneau M-adique, B un anneau contenant A et qui soit un A-module de type fini (tout élément de B est alors entier sur A) ; nous dirons alors que B est une extension finie de A. L'anneau B n'est pas nécessairement (MB)-adique, pour qu'il le soit il faut et il suffit qu'aucun élément de I + M ne soit diviseur de zéro dans B. Mais si A est un anneau de Zariski, ou un anneau complet, ou un anneau semi-local, il en est de même de B. On peut se demander quand A est un sous-espace topologique de B ((MB)-adique) ; il en est ainsi lorsque A est semi-local et complet. Un autre cas important est celui où A est semi-local et où aucun élément non nul de A n'est diviseur de zéro dans B ; dans ce cas l'adhérence de A dans $\hat{B}$ est le complété $\hat{A}$, $\hat{B}$ est extension finie de $\hat{A}$, B et $\hat{A}$ sont linéairement disjoints sur A, et tout élément de $\hat{A}$ qui est diviseur de zéro dans $\hat{B}$ est déjà diviseur de zéro dans A.

Lorsque A est un anneau M-adique complet, il est assez facile de montrer qu'une extension B de A est finie. En effet, si L est un anneau (MB)-adique quelconque contenant A, si $MB \cap A = M$, et si B/MB est extension finie de A/M, alors B est extension finie de A ; et l'on peut prendre pour système de générateurs du A-module B des représentants quelconques des éléments d'un système de générateurs du (A/M)-module B/MB (démonstration par approximation successives). Ce résultat donne aussitôt l'important théorème suivant ("Vorbereitungssatz formel") : soient R un anneau local complet, V son idéal maximal, B l'anneau de séries formelles R[[X]], f(X) un élément de B n'appartenant pas à VB, et $b_s X^s$ le terme de plus bas degré de f tel que $b_s \notin V$; alors tout élément z de B s'écrit, d'une manière et d'une seule, sous la forme $z = uf + q$, avec $u \in B$ et

$$q = \sum_{i=0}^{s-1} a_i X^i \quad (a_i \in R)$$

Cet énoncé reste encore valable lorsque R est l'anneau des séries convergentes en $X_1, \ldots, X_n$ sur un corps valué complet, et lorsque B est l'anneau des séries convergentes en $X_1, \ldots, X_n, X$; mais la méthode précédente ne marche pas, car il faut des expressions explicites des séries u et q pour pouvoir appliquer la méthode des majorantes. Une conséquence du Vorbereitungssatz est que l'anneau des séries formelles (resp. convergentes) sur un corps (resp. un corps valué complet) est un anneau à unique factorisation ; une autre est que l'anneau des séries convergentes sur un corps valué complet est noethérien.

4. Structure des anneaux complets.

On a des résultats assez complets sur la structure de certains anneaux M-adiques complets. On montre d'abord qu'un anneau semi-local et complet est composé direct d'anneaux locaux complets. Ceci se déduit du résultat plus général suivant : si A est un anneau M-adique complet, et si A/M se décompose en composé direct de deux idéaux, alors cette décomposition "se prolonge" en une décomposition de A (on obtient les idempotents de la décomposition de A à partir de représentants des idempotents de celle de A/M par approximations successives). Ce théorème de "prolongement des décompositions directes" est intimement lié à l'important lemme de Hensel : soient A un anneau local complet, M son idéal maximal, f un polynôme de degré n sur A, γ et γ' des polynômes de degrés r et $n-r$ sur A/M tels que $\gamma\gamma'$ soit le polynôme $\bar{f}$ obtenu à partir de f par réduction mod M de ses coefficients, et que γ et γ' soient premiers entre eux, il existe alors des polynômes g et g' de degrés r et $n-r$ sur A tels que $f = gg'$, et que $\bar{g} = \gamma$ et $\bar{g}' = \gamma'$. En particulier, si $\bar{f}$ a une racine simple dans A/M, il existe une racine simple a de f dans A ayant la racine donnée pour classe mod M. On trouve de nombreux exemples d'application du lemme de Hensel dans la théorie des nombres p-adiques, et dans celle des séries entières ; ainsi, comme 1 a deux racines carrées dans un corps K de caractéristique $\neq 2$, la série formelle $1 + Xs(X)$ a deux racines carrées dans $K[[X]]$.

Revenons à l'étude des anneaux complets. Nous venons de voir que celle des anneaux semi-locaux se ramène à celle des anneaux locaux. Pour un anneau local complet, on s'efforce de montrer que c'est un anneau quotient d'un anneau de séries formelles sur un anneau de nature simple. Pour simplifier l'exposé, nous nous bornerons au cas "d'égales caractéristiques", c'est-à-dire celui où l'anneau local A a même caractéristique que son corps quotient A/M, autrement dit, celui où A contient un corps (c'est le cas dans les applications géométriques). On montre, alors, que A contient un "corps complet de représentants des classes mod M" c'est-à-dire un sous-corps K, isomorphe à A/M, par l'homomorphisme canonique de A sur A/M. Dans ce cas, si (x_i) désigne une base de M, A est un quotient de l'anneau de séries formelles $K[[X_1, \ldots, X_n]]$, et on a un théorème de structure pour A. La démonstration d'existence du corps de représentants K est facile, lorsque A et A/M sont de caractéristique 0 : On "zornifie" sur les sous-corps de A, et on applique le lemme de H e n s e l. La d é m o n s t r a t i o n est encore assez simple, lorsque A et A/M sont de caractéristique

$p \neq 0$ et que A/M est parfait (on utilise les "représentants multiplicatifs" de Hasse). Mais c'est effroyablement compliqué lorsque A/M est imparfait (N.B. - Depuis 1952 la démonstration a été notablement simplifiée par NARITA et par GEDDES).

Le théorème de structure se simplifie lorsque A est un anneau local <u>régulier</u>, c'est-à-dire lorsque M est engendré par d éléments, d étant la dimension de A ; alors ces éléments sont analytiquement indépendants sur K, et A est un anneau de séries formelles sur K. L'anneau local d'une sous-variété simple d'une variété algébrique est régulier par définition des sous-variétés simples, donc son complété est un anneau de séries formelles.

5. <u>Anneaux à noyau et anneaux locaux géométriques</u>.

La structure des anneaux locaux non complets est beaucoup moins bien connue que celle des anneaux locaux complets. Jusqu'ici beaucoup de propriétés d'anneaux locaux qui sont utiles pour les applications géométriques n'ont pû être démontrées que pour certaines classes d'anneaux (contenant d'ailleurs tous les anneaux rencontrés en Géométrie) dont la définition est constructive et assez artificielle. Les anneaux considérés sont ceux qui contiennent des sous-anneaux de type très spécial (les "noyaux") et qui, en un certain sens, sont assez proches de ces noyaux ; on les appelle les <u>anneaux à noyau</u>. Le noyau d'un anneau à noyau n'est nullement déterminé de façon unique. D'autre part, dans les théorèmes utiles démontrés pour les anneaux à noyau, le noyau qui a servi à la démonstration n'apparaît, ni dans les hypothèses, ni dans la conclusion. Tout ceci montre que cette partie de la théorie est encore dans un état fort peu satisfaisant. Aussi serons-nous assez brefs.

Soit K un corps d'exposants caractéristique p tel que $[K : K^p]$ soit fini. On appelle <u>noyaux</u> les anneaux suivants : l'anneau des fractions de l'idéal premier $(x_1, \dots, x_n)$ de l'anneau de polynômes $K[x_1, \dots, x_n]$ (c'est-à-dire l'anneau des fractions rationnelles $a(x)/b(x)$ telles que $b(0) \neq 0$) ; l'anneau de séries formelles $K(x_1, \dots, x_m)[[x_{m+1}, \dots, x_n]]$. Ce sont des anneaux locaux réguliers. On dit qu'un anneau local A est un <u>anneau à noyau</u>, s'il existe un noyau B et un anneau intermédiaire $C (B \subset C \subset A)$ tels que C soit extension finie de B, que A soit l'anneau des fractions d'un idéal maximal de C, et qu'aucun élément non nul de B ne soit diviseur de zéro dans A. Alors A a même dimension que le noyau B.

Les opérations suivantes ne font pas sortir de la classe des anneaux à noyau : complétion, formation de l'anneau des fractions d'un idéal premier, passage à l'anneau quotient par un idéal équidimensionnel. Les anneaux obtenus à partir des noyaux par application répétée des opérations de complétion, formation de l'anneau des fractions d'un idéal premier, passage au quotient par un idéal premier, forment une sous-classe de celle des anneaux à noyau, et sont appelés les anneaux locaux géométriques.

Les principales propriétés des anneaux à noyau et des anneaux locaux géométriques sont des relations entre les multiplicités de certains idéaux de certains anneaux. Citons parmi elles le théorème de transition (qui permet le passage des variétés algébriques aux variétés algébroïdes), et la formule d'associativité (source de l'associativité des intersections en géométrie). Un cas particulier de théorème de transition montre qu'un anneau local géométrique n'a pas d'éléments nilpotents, en termes géométriques ceci signifie que la décomposition locale d'une variété algébrique en variétés algébroïdes n'est pas plus compliquée au sens de la théorie des idéaux qu'elle ne l'est au sens ensembliste.

6. Diverses propriétés d'anneaux intégralement clos et à unique factorisation (ou "factoriels").

Le complété d'un anneau d'intégrité à noyau et intégralement clos est un anneau d'intégrité intégralement clos (ZARISKI). Géométriquement : une variété localement normale est analytiquement irréductible et localement normale en tant que variété algébroïde.

Un anneau local régulier et complet est factoriel (au moins dans le cas d'égales caractéristiques).

Un anneau local régulier à noyau est factoriel.

Il existe des anneaux locaux géométriques factoriels qui ne sont pas réguliers.