RÉDACTION N° 142

COTE : NBR 045

TITRE : DEUXIÈME PARTIE
LIVRE I ALGÈBRE COMMUTATIVE
CHAPITRE III (ÉTAT 1)
ALGÈBRE LOCALE ÉLÉMENTAIRE

ASSOCIATION DES COLLABORATEURS DE NICOLAS BOURBAKI

NOMBRE DE PAGES : 34

NOMBRE DE FEUILLES : 34

DEUXIEME PARTIE

ANALYSE ALGÉBRIQUE.

LIVRE I

ALGÈBRE COMMUTATIVE

CHAPITRE III (Etat 1).

ALGÈBRE LOCALE ÉLÉMENTAIRE.

Commentaire sur les chapitres II et III.

Le chapitre II, relatif aux anneaux noethériens, présente les différences suivantes sur les rédactions précédentes. Comme il avait été annoncé en Congrès on a donné la décomposition primaire pour les modules noethériens stratifiés ; ceci est utile dans certains cas (à Snapper et au rédacteur dans le cas des modules, à tous ceux qui font de la géométrie projective dans le cas des anneaux gradués), çà ne coûte pas plus cher, et ça sépare bien les rôles. On a aussi montré que les anneaux de fractions d'Uzkov (qu'on a introduits au chap.I) sont les mêmes que ceux de Chevalley dans le cas où l'anneau est noethérien ; ce sera utile plus tard, en géométrie algébrique locale, et c'est un bon moyen d'introduire les puissances symboliques d'idéaux. Enfin on a montré qu'un anneau noethérien intégralement clos est normal.

Deux autres différences sont des innovations. La première est que l'on a ajouté un numéro sur les anneaux et modules ayant une suite de composition finie (qui sont dits "de longueur finie") ; ceux-ci jouent un certain rôle au chap.III ; en réalité ils ne sont autres (dans le cas commutatif et unitaire) que les anneaux et modules d'Artin, mais ceci n'est dit qu'au chap.III, où la démonstration arrive comme un fruit mûr. La seconde différence est qu'on a attendu le chap.III pour montrer qu'un anneau de séries formelles est noethérien (le résultat analogue pour les polynomes restant au chap.II) ; en effet la méthode de démonstration

adoptée se base sur le fait que l'anneau des séries formelles est le complété de celui des polynomes (ou, plus exactement, est complet et a pour anneau gradué associé l'anneau des polynomes), et s'étend à une situation plus générale qui est une situation typique d'algèbre locale.

Au chapitre III on a évité, autant que possible, de se borner aux anneaux noethériens. Le résultat en est une affreuse salade, où les théorèmes du cas noethérien se mêlent à ceux du cas général ; mais le rédacteur croit que ce serait encore pire si on séparait le cas noethérien en en faisant un § spécial. La raison de cette généralité est que, dans les fonctions holomorphes de plusieurs variables, on rencontre des anneaux dont on ne sait pas tout de suite qu'ils sont noethériens ; et ce sera peut être en leur appliquant les résultats donnés ici qu'on pourra démontrer qu'ils le sont.

Sauf mention expresse du contraire, tous les anneaux considérés dans ce chapitre sont supposés commutatifs et munis d'un élément unité noté 1 ; tous les homomorphismes et tous les modules sont supposés unitaires.

§ 1 - Anneau gradué associé à un idéal.

Soient A un anneau, M un idéal de A . Rappelons (Top.Génér., chap.III) que les puissances (M^n) de M forment un système fondamental de voisinages de 0 dans une topologie compatible avec la structure d'anneau de A . Pour que cette topologie soit séparée, il faut et il suffit que l'on ait $\bigcap_{n=0}^{\infty} M^n = (0)$; dans ce cas on dira que l'anneau A , muni de la topologie et de l'idéal M en question, est un anneau M-adique, et que cette topologie est la topologie M-adique de l'anneau A . D'après le th. de Krull (chap.II, § 3) il faut et il suffit, pour qu'un anneau noethérien A soit M-adique, qu'aucun élément de $1+M$ ne soit diviseur de zéro dans A .

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 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, on vérifie aussitôt que la forme initiale de xy dans M^{n+s}/M^{n+s+1} ne dépend que de $\bar{x}$ et $\bar{y}$, et non de leurs représentants x et 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 vérifie aisément qu'on obtient sur F(M) une structure d'anneau commutatif. Muni de cette structure F(M) est appelé l'anneau gradué associé à l'idéal M, ou l'anneau de formes de M.

Exemples - 1) Soient A l'anneau de polynomes $C[X_1,\dots,X_r]$, et M l'idéal engendré par les X_i. L'anneau F(M) est alors isomorphe à A ; la forme initiale d'un polynome p(X) est sa forme de plus bas degré. Si M' est l'idéal engendré par les X_i dans l'anneau de séries formelles $C[[X_1,\dots,X_r]]$, l'anneau F(M') est encore isomorphe à l'anneau de polynomes A.

2) Soit p un nombre premier ; l'annéau Z est un anneau (Zp)-adique. L'anneau de formes F(Zp) est isomorphe à l'anneau des polynomes à une indéterminée sur le corps fini F_p.

3) Soient F(M) un anneau de formes, et $\bar{M}$ l'idéal $\sum_{n=1}^{\infty} M^n/M^{n+1}$ de F(M) ; alors F(M) est un anneau $\bar{M}$-adique, et $F(\bar{M})$ est isomorphe à F(M).

2 - Anneau gradué associé à un anneau quotient.

Proposition 1 - Soient A un anneau M-adique, et I un idéal fermé de A ; alors A/I est un anneau (M+I)/I)-adique, dont l'anneau gradué associé F((M+I)/I) est isomorphe au quotient de F(M) par l'idéal engendré par les formes initiales des éléments de I.

Le fait que I est fermé s'exprime par $\bigcap_{n=0}^{\infty}(I+M^n) = I$, ce qui montre que A/I est un anneau $((M+I)/I)$-adique. L'application canonique de M^n sur $(M^n+I)/I$ applique M^{n+1} sur $(M^{n+1}+I)/I$, et définit donc, par passage aux quotients, une application de M^n/M^{n+1} sur $(M^n+I)/(M^{n+1}+I)$. On en déduit que $F(M+I)/I)$ s'identifie canoniquement à un anneau quotient $F(M)/\bar{I}$. Et l'idéal $\bar{I}$ est évidemment engendré par l'ensemble des formes initiales, dans $F(M)$, des éléments de I.

L'idéal $\bar{I}$ est appelé l'idéal directeur de I ; tout élément homogène de $\bar{I}$ est d'ailleurs forme initiale d'un élément de I.

3 - Passage des propriétés de l'anneau gradué associé à celles de l'anneau M-adique.

Proposition 2 - Soient A un anneau M-adique, et $F(M)$ son anneau gradué associé ; si $F(M)$ est un anneau d'intégrité, il en est de même de A.

En effet, si $\bar{x}$ et $\bar{y}$ sont les formes initiales des éléments non nuls x et y de A, $\overline{xy}$ est non nul et est la forme initiale de xy ; donc xy n'est pas nul.

Remarque - Pour tout élément non nul x de A, désignons par $v(x)$ le plus petit entier n tel que $x \notin M^{n+1}$, c'est-à-dire le degré de la forme initiale de x. Avec les hypothèses de la prop.2 on a $v(xy) = v(x)+v(y)$ (et non plus seulement $v(xy) \geqslant v(x)+v(y)$). Comme la relation $v(x+y) \geqslant \mathrm{Min}(v(x),v(y))$ est vraie dans tous les cas, le fait que $F(M)$ est un anneau d'intégrité implique que v est une valuation de A, dont le centre est M (chap.I, § 1).

Corollaire - Soient A un anneau M-adique, et I un idéal fermé de A ; si l'idéal directeur de I est premier, il en est de même de I.

Cela résulte aussitôt des prop.1 et 2.

Proposition 3 - *Soit A un anneau M-adique dont tout idéal principal soit fermé ; si son anneau gradué associé F(M) est un anneau d'intégrité qui soit intersection d'anneaux de valuations archimédiennes (chap.I, § 1) (par exemple un anneau normal (chap.I, § 4)), alors A est un anneau d'intégrité intégralement clos.*

Que A soit anneau d'intégrité résulte de la prop.2 . Considérons un élément y/x ($x \in A$, $y \in A$) entier sur A . On va montrer par récurrence sur n que $y \in Ax+M^n$. C'est vrai pour $n=0$. Si $y \in Ax+M^n$; il existe alors $z \in A$ tel que $y-zx \in M^n$ et que $u = (y-zx)/x$ soit entier sur A . On peut alors trouver un élément non nul d de A tel que $du^s \in A$ pour tout s . Ainsi $d(y-zx)^s$ est multiple de x^s , et, en passant aux formes initiales, $\overline{d}\,\overline{(y-zx)}^s$ est multiple de $\overline{x}^s$ pour tout s . Si w désigne une valuation archimédienne du corps des fractions de F(M) qui soit positive sur F(M) , on en déduit $w(\overline{d}) + s.w(\overline{y-zx}) \geqslant s.w(\overline{x})$ pour tout s , donc $w(\overline{y-zx}) \geqslant w(\overline{x})$ puisque w est archimédienne. L'hypothèse sur F(M) montre donc que $\overline{y-zx}$ est multiple de $\overline{x}$ dans F(M) . Par conséquent, il existe $t \in A$ tel que $\overline{y-zx} = \overline{tx}$; mais on a alors $y-zx-tx \in M^{n+1}$. On a donc bien $y \in Ax+M^j$ pour tout j , c'est-à-dire $y \in Ax$ puisque Ax est un idéal fermé.

La prop.3 (due à Krull, comme d'ailleurs la plus grande partie de ce §) montre en particulier que l'anneau local d'un point simple est intégralement clos).

Proposition 4 - *Soit A un anneau M-adique complet ; si A/M est noethérien et si l'idéal M a un système fini de générateurs, alors A est noethérien.*

Soit en effet (m_j) un système de générateurs de M , et $\overline{m}_j$ leurs formes initiales. Les monômes de degré n en les m_j constituent un système de générateurs de M^n/M^{n+1} considéré comme (A/M)-module. Ainsi F(M) est égal à $(A/M)[(\overline{m}_j)]$; il est donc isomorphe à un quotient

(par un idéal homogène) d'un anneau de polynomes à un nombre fini d'indéterminées sur A/M, et c'est par conséquent un anneau noethérien. Notre assertion résulte alors du lemme suivant :

Lemme - Soient A un anneau M-adique complet, et (b_i) un système fini d'éléments d'un idéal B de A dont les formes initiales $(\overline{b}_i)$ forment un système de générateurs de l'idéal directeur $\overline{B}$ de B ; alors (b_i) est un système de générateurs de B .

Soit b un élément de B . Supposons, par récurrence, que nous ayons trouvé une famille (a_{ni}) d'éléments de A telle que $b \equiv \sum_i a_{ni} b_i \ (M^{n+1})$. Alors la forme initiale de $b - \sum_i a_{ni} b_i$, qui est au moins de degré n+1, est de la forme $\sum_i \overline{c}_{ni} \overline{b}_i$, où $\overline{c}_{ni}$ est au moins de degré $n+1 - d^0(\overline{b}_i)$ puisque F(M) est un anneau gradué. Posons $a_{n+1,i} = a_{ni} + c_{ni}$. On a par construction $b \equiv \sum_i a_{n+1,i} b_i \ (M^{n+2})$, et, pour tout i, la suite (a_{ni}) est une suite de Cauchy. Donc, si a_i désigne la limite de cette suite (qui existe puisque A est complet), on a $b = \sum_i a_i b_i$. CQFD .

Corollaire - Si C est un anneau noethérien, l'anneau de séries formelles à un nombre fini d'indéterminées $A = C[[X_1, \ldots, X_s]]$ est noethérien.

En effet, si M désigne l'idéal de A engendré par les X_i, A est un anneau M-adique complet, $A/M = C$ est noethérien, et M a un système fini (X_i) de générateurs.

Remarque - La conclusion de la prop.4 ne subsiste pas si on ne suppose pas A complet (contre exemple japonais dans le cas où A est un anneau local d'idéal maximal M)

Nous verrons d'autre part, au § 2, que tout idéal d'un anneau M-adique noethérien et complet est fermé. Donc, si B désigne le complété de l'anneau M-adique A , l'adhérence dans A de l'idéal I est l'idéal $BI \cap A$. Ainsi l'assertion que tout idéal I de A est fermé (qui, dans le cas d'un anneau A de Séries convergentes, veut dire que, si $a \in A$ est combinaison linéaire des $c_i \in A$ à coefficients séries formelles, il en est aussi combinaison linéaire à coefficients convergents), implique que A est noethérien puisqu'il y a correspondance biunivoque monotone entre les idéaux de A et ceux de son complété noethérien. Réciproquement, lorsque A est un anneau local, le fait que A est noethérien implique que tout idéal de A est fermé (cf. § 2) .

§ 2 - Complété et idéaux d'un anneau M-adique.

Soit A un anneau M-adique. Comme toute somme d'éléments de M^n appartient à M^n, une condition nécessaire et suffisante pour qu'une suite (a_n) d'éléments de A soit une suite de Cauchy est que l'on ait $a_{n+1}-a_n \in M^{s(n)}$ où $s(n)$ tend vers l'infini avec n. En particulier, lorsque A est complet, les séries convergentes sont celles dont le terme général tend vers 0. (On pourrait remonter ces remarques au début du § 1).

Notons aussi que, si A est un anneau M-adique, et si M' est un idéal de A et r et s deux entiers tels que $M \supset M'^r$ et $M' \supset M^s$, alors A est un anneau M'-adique, et les topologies M-adique et M'-adique de A sont identiques.

1 - Complété d'un anneau M-adique.

Proposition 1 - *Soient A un anneau M-adique, $\hat{A}$ son complété ; l'anneau topologique $\hat{A}$ est un anneau $(\hat{A}M)$-adique ; l'idéal $\overline{M} = \hat{A}M$ est l'adhérence dans $\hat{A}$ de M ; et on a $\overline{M}^n = \hat{A}.M^n$ et $M^n = \overline{M}^n \cap A$.*

Tout élément de $\hat{A}$ est somme d'une série $\sum_{n=0}^{\infty} a_n$ où $a_n \in M^n$; les éléments de l'idéal $\overline{M}^s$ engendré par M^s sont les sommes de séries de ce type où $a_0 = a_1 = \ldots = a_{s-1} = 0$. Ceci montre que $\overline{M}^s$ est l'adhérence de M^s dans $\hat{A}$. Comme les M^s forment un système fondamental de voisinages de 0 dans M, il résulte de la théorie des espaces uniformes (Top.Gén., chap.II) que les $\overline{M}^s$ forment un système fondamental de voisinages de 0 dans $\hat{A}$. Enfin (ibid.) $\overline{M}^s \cap A$ est l'adhérence dans A de M^s ; comme M^s est un idéal ouvert, il est fermé (Top.Gén., chap.III), et on a bien $M^s = \overline{M}^s \cap A$.

Proposition 2. *Si A est un anneau M-adique noethérien, son complété $\hat{A}$ est noethérien.*

Ceci résulte de la prop.4, §1 ; $\hat{A}$ est un anneau $\mathfrak{M}$-adique, $\mathfrak{M}$ est engendré par tout système fini de générateurs de M, et $\hat{A}/\mathfrak{M}$ est isomorphe à A/M et est donc noethérien.

2 - Idéaux fermés d'un anneau noethérien M-adique.

Proposition 3 - Soit A un anneau noethérien M-adique ; pour qu'un idéal I de 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.

Le fait que I est fermé s'exprime par $\bigcap_{n=0}^{\infty}(I+M^n)=I$. En appliquant le th. de Krull (chap.II, §3) à A/I, et comme l'ensemble des diviseurs de zéro de A/I est $\bigcup_i (P_i/I)$, ceci revient à dire que l'on a $P_i+M \neq A$ pour tout i.

Corollaire 1 - Soient I un idéal de l'anneau noethérien M-adique A, $I = \bigcap_i Q_i$ sa décomposition primaire, et P_i l'idéal premier associé à Q_i ; alors l'adhérence de I est l'idéal I' intersection de ceux des Q_i tels que $P_i + M \neq A$.

En effet l'idéal I' est fermé d'après la prop.3, et contient I. D'autre part, si Q_j est une composante primaire de I telle que $P_j+M = A$, on a, par élévation de cette égalité à une haute puissance, $Q_j+M^n = A$ pour tout n ; il existe alors dans Q_j un élément de la forme $1+u_j$ où $u_j \in M^n$; le produit de ces éléments relatifs aux divers Q_j est de la forme $1+m$ où $m \in M^n$. Soit alors x un élément de I' ; on a $x(1+m) \in I$. Ceci montre que I est dense dans I', donc que I' est l'adhérence de I.

Corollaire 2 - Soit A un anneau noethérien et M un idéal de A ; les conditions suivantes sont équivalentes :

a) Pour tout idéal I de A on a $\bigcap_n (I+M^n)=I$, c'est-à-dire que M détermine sur A une topologie M-adique pour laquelle tout idéal est fermé.

b) L'idéal M est contenu dans l'intersection des idéaux maximaux de A .

c) Tout élément de $1+M$ est inversible.

D'après la prop.3, a) équivaut à $P+M \neq A$ pour tout idéal premier P, c'est-à-dire à $V+M = V$ pour tout idéal maximal V puisque tout idéal premier de A est contenu dans un idéal maximal, c'est-à-dire encore à b). Soit V un idéal maximal de A ; les relations $M \subset V$ et $(1+M) \cap V = \emptyset$ sont équivalentes, puisque la première est la négation de $M+V = A$; comme les éléments inversibles de A sont ceux qui ne sont contenus dans aucun idéal maximal, ceci montre l'équivalence de b) et c).

Définition 1 - On dit qu'un anneau A est un anneau de Zariski, si c'est un anneau M-adique noethérien dont tout idéal est fermé.

(Le rédacteur ne tient nullement à donner un nom à ces anneaux).

Proposition 4 - Un anneau M-adique noethérien et complet est un anneau de Zariski.

En effet tout élément $1-m$ de $1+M$ admet pour inverse la somme de la série $1+m+m^2+\ldots+m^n+\ldots$, et on applique le cor.2 de la prop.3 .

Corollaire 1 - Soit I un idéal d'un anneau M-adique noethérien A , et soit $\hat{A}$ le complété de A ; l'adhérence de I dans A est $\hat{A}I \cap A$.

En effet tout élément de $\hat{A}I$ est adhérent à I . Comme $\hat{A}I$ est fermé, c'est l'adhérence de I dans $\hat{A}$. Le reste se déduit de la théorie des espaces uniformes.

Corollaire 2 - Soient A un anneau de Zariski, $\hat{A}$ son complété ; pour tout idéal I de A , on a $\hat{A}I \cap A = I$.

Voici maintenant un autre exemple d'anneaux de Zariski :

Définition 2 - On dit qu'un anneau topologique A est un anneau semi-local s'il n'a qu'un nombre fini d'idéaux maximaux, et s'il est muni de la topologie M-adique, M désignant l'intersection de ces idéaux maximaux.

Un anneau noethérien local d'idéal maximal M est semi local pour la topologie M-adique. Nous verrons que toute "extension finie" d'un anneau noethérien semi-local est un anneau noethérien semi-local (§ 3).

Proposition 5 - Pour qu'un anneau M-adique de Zariski A soit semi-local, il faut et il suffit que A/M soit de longueur finie.

Supposons d'abord que A soit un anneau semi-local, et notons M' l'intersection de ses idéaux maximaux. Il existe un exposant s tel que $M \supset M'^s$. Or A/M' est composé direct d'un nombre fini de corps ; c'est donc un anneau de longueur finie. Comme les M'^n ont chacun un nombre fini de générateurs les M'^n/M'^{n+1} sont des (A/M')-modules de type fini, donc des modules de longueur finie (chap.II, § 1). Par consóquent A/M'^s est un anneau de longueur finie d'après le th. de Jordan-Hölder, et à fortiori A/M .

Supposons réciproquement que A soit un anneau M-adique de Zariski, et que A/M soit de longueur finie. Comme A est un anneau de Zariski, les idéaux maximaux de A contiennent M , et sont en correspondance biunivoque avec ceux de A/M . Or tout idéal premier V/M de A/M est maximal, puisqu'un anneau d'intégrité de longueur finie est un corps (chap.II, § 1). D'autre part tout idéal premier contenant M contient au moins un idéal premier isolé de M (chap.II, § 2). Donc les idéaux premiers de A contenant M ne sont autres que les idéaux premiers isolés de M , et sont maximaux, et en nombre fini. Par consóquent M est contenu dans l'intersection R de ces idéaux, et contient une puissance R^s de R . Ceci montre que l'anneau M-adique A est semi-local.

Remarque sans grand intérêt - Dans un anneau M-adique A , l'ensemble $S = 1+M$ est un ensemble multiplicativement stable d'éléments qui ne sont pas diviseurs de zéro. L'anneau de fractions A_S est un anneau de Zariski pour la topologie (MA_S)-adique ; l'anneau A en est un sous-anneau et un sous-espace topologique ; les complétés de A et de A_S sont identiques ; les anneaux de Zariski sont caractérisés par $A=A_S$.

3 - Anneaux quotients d'un anneau M-adique.

Proposition 6 - Soit I un idéal fermé d'un anneau M-adique A ; le complété de A/I est canoniquement isomorphe à $\hat{A}/\hat{A}I$.

Comme $\hat{A}I \cap A = I$ (cor.1 de la prop.4), A/I s'identifie à un sous-anneau de $\hat{A}/\hat{A}I$. Un système fondamental de voisinages de zéro dans ce dernier anneau est formé par les $(\hat{A}M^n+\hat{A}I)/\hat{A}I = \hat{A}(M^n+I)/\hat{A}I$. Les traces de ces voisinages sur A/I sont les $(M^n+I)/I$, puisque les idéaux M^n+I de A sont ouverts, et donc fermés. Ainsi A/I est un sous-espace topologique de $\hat{A}/\hat{A}I$, évidemment partout dense. Enfin $\hat{A}/\hat{A}I$ est complet, en tant qu'anneau quotient de l'anneau métrisable et complet $\hat{A}$ (Top.Gén., chap.IX, § 3,prop.4). Ceci démontre la prop.6 .

Remarque - Lorsque I est un idéal ouvert de A , les anneaux A/I et $\hat{A}/\hat{A}I$ coïncident, puisque A/I est un anneau discret, et donc complet. En prenant $I = M$, ceci et la prop.5 montrent que le complété d'un anneau semi-local (resp.local) est semi-local (resp. local) (ceci pourrait être un corollaire ?) .

4 - Intersections d'idéaux.

Proposition 7 - Soient A un anneau de Zariski, c un élément de A , et I un idéal de A ; on a $(\hat{A}I:\hat{A}c) = \hat{A}(I:Ac)$ et $\hat{A}I \cap \hat{A}c = \hat{A}(I \cap Ac)$.

Comme $I \cap Ac = c(I:Ac)$ la seconde formule se déduit de la première. Pour la première il suffit de montrer que, si $x \in \hat{A}$ est tel que $xc \in \hat{A}I$, alors x est adhérent à $(I:Ac)$. Posons $x = x_n + m_n$ avec $x_n \in A$ et $m_n \in \hat{A}M^n$. On a $x_n c \in (\hat{A}I+\hat{A}M^n c) \cap A = I+M^n c$ (cor.2 de la prop.4). D'où $x_n c = d+m'_n c$, avec $d \in I$ et $m'_n \in M^n$. Alors x est limite de la suite $(x_n-m'_n)$ dont les éléments appartiennent à $(I:Ac)$.

Corollaire - Soient A un anneau de Zariski, et c un élément de A qui n'est pas diviseur de zéro dans A ; alors c n'est pas diviseur de zéro dans le complété $\hat{A}$ de A .

Il suffit de prendre $I = (0)$.

Proposition 8 - Soient A un anneau semi-local et complet, M l'intersection des idéaux maximaux de A, et (I_n) une suite décroissante d'idéaux de A telle que $\bigcap_{n=0}^{\infty} I_n = (0)$; on a alors $I_n \subset M^{s(n)}$ où $s(n)$ tend vers l'infini avec n.

(Ceci est une propriété de compacité, plus exactement de "linéaire compacité"). Remarquons d'abord que les A/M^s sont des anneaux de longueur finie (prop.5), et satisfont donc à la condition minimale pour leurs idéaux. Nous allons raisonner par l'absurde. Supposons qu'il existe un entier j tel que $I_n \not\subset M^j$ quel que soit n. Alors, pour tout $s \geqslant j$, on a $I_n \not\subset M^s$ quel que soit n. Comme les idéaux $I_n + M^j$ forment une suite décroissante et sont distincts de M^j, cette suite s'arrête, et il existe $x_j \notin M^j$ tel que $x_j \in I_n + M^j$ pour tout n. Supposons défini un élément $x_s \notin M^s$ tel que $x_s \in I_n + M^s$ pour tout n. Alors les ensembles $(x_s + M^s) \cap I_n$ sont non vides, et a fortiori aussi les $(x_s + M^s) \cap (I_n + M^{s+1})$. Ceux-ci forment une suite décroissante. Si celle-ci ne s'arrêtait pas, on pourrait, par translation, obtenir des suites décroissantes d'idéaux contenant M^{s+1} de longueur aussi grande que l'on veut. Comme ceci est impossible en vertu du th. de Jordan-Holder, il existe un élément x_{s+1} de $x_s + M^s$ tel que $x_{s+1} \in I_n + M^{s+1}$ quel que soit n. Nous avons ainsi défini par récurrence, pour tout $s \geqslant j$, des éléments x_s tels que $x_s \notin M^s$, $x_{s+1} - x_s \in M^s$, et $x_s \in I_n + M^s$ pour tout s. La suite (x_s) est une suite de Cauchy ; comme A est complet, elle admet une limite x ; on a $x \notin M^s$ pour tout $s \geqslant j$, et $x \in I_n + M^s$ quel que soit $s \geqslant j$; comme l'idéal I_n est fermé, on en déduit $x \in I_n$ pour tout n ; d'où $x = 0$ en vertu des hypothèses. Mais ceci est contraire à $x \notin M^j$. CQFD.

Corollaire 1 - Soient A un anneau semi-local, I un idéal de A et a un élément de A ; on a $(I+M^n:Aa) \subset (I:Aa)+M^{s(n)}$ où $s(n)$ tend vers l'infini avec n .

On applique en effet la prop.8 à la suite d'idéaux $\hat{A}((I+M^n):Aa)/\hat{A}(I:Aa)$, et on tient compte de la prop.7 .

Corollaire 2 - Si a n'est pas diviseur de zéro dans l'anneau semi-local A , on a $(M^n:Aa) \subset M^{s(n)}$ où $s(n)$ tend vers l'infini avec n .

Il suffit de prendre $I=(0)$ dans le cor.1 .

Corollaire 3 - Soit A un anneau semi-local complet, sous-anneau d'un anneau M-adique B tel que $M \cap A$ soit l'intersection R des idéaux maximaux de A ; alors A est un sous-espace topologique de B .

En effet $M^n \cap A$ contient évidemment R^n , et est contenu dans $R^{s(n)}$ en vertu de la prop.8 .

Remarques - 1) La conclusion de la prop.8 ne s'étend pas aux anneaux semi-locaux non complets (contre exemple à partir d'une courbe analytique plane qui n'est branche d'aucune courbe algébrique).

2) Lorsque A est un anneau semi-local, la prop.7 peut se généraliser ainsi ; I et J étant des idéaux de A , on a $\hat{A}I \cap \hat{A}J = (I \cap J)\hat{A}$. La démonstration utilise le cor.1 de la prop.8, et est, en plus compliqué, une jonglerie sur les idéaux, du type de la prop.7 . Le rédacteur n'a jamais encore employé ce résultat qu'à des endroits où Zariski et Chevalley s'en passent fort bien. Mais il a peut être quelqu'intérêt pour algébriser certains trucs de Cartan sur les idéaux de fonctions holomorphes.

5 - Idéaux connexes - Structure des anneaux semi-locaux complets.

Un idéal I d'un anneau A est dit connexe s'il n'est pas intersection de deux idéaux V et V', distincts de A et I , et tels que $V+V' = A$;

autrement dit I est connexe lorsque A/I n'est pas composé direct de deux idéaux non triviaux.

Théorème 1 - Soient A un anneau M-adique complet tel que M soit non connexe, V et V' des idéaux non triviaux de A tels que $V+V' = A$ et $V \cap V' = M$. Alors A est composé direct des idéaux $N = \bigcap_{n=0}^{\infty} V^n$ et $N' = \bigcap_{n=0}^{\infty} V'^n$.

Ecrivons $1 = b+b'$ ($b \in V$, $b' \in V'$), et posons $b_n = 1-(1-b^n)^n$ et $b'_n = 1-(1-b'^n)^n$. On a $b_n \in V^n$, $b'_n \in V'^n$, $b_n \equiv 1$ (V'^n), $b'_n \equiv 1$ (V^n) et $b_n+b'_n \equiv 1$ $(V^n \cap V'^n)$. Or $V^n \cap V'^n = M^n$, car, de $x \in V^n$ et $x \in V'^n$, on déduit $x = xb_n+x(1-b_n) \in V^n V'^n$. On a donc $b_n+b'_n \equiv 1$ (M^n). D'autre part $b_{n+1}-b_n = -(1-b^n)^n+(1-b^{n+1})^{n+1}$ est multiple de b^n et de $(1-b)^n = b'^n$; d'où $b_{n+1}-b_n \in V^n \cap V'^n = M^n$; les suites (b_n) et (b'_n) sont donc des suites de Cauchy, et, comme A est complet, elles admettent des limites d et d'. Celles-ci ont les propriétés suivantes : $d \in N$, $d' \in N'$, $dd' \in \bigcap_{n=0}^{\infty} M^n = (0)$, $d+d' = 1$; d'où $d = d^2$, $d' = d'^2$; ainsi A est composé direct des idéaux Ad et Ad' (Alg., chap. I, § 8) ; et, comme $N \cap N' = (0)$, on a $N = Ad$ et $N' = Ad'$. CQFD.

Corollaire 1 - Soient A un anneau M-adique complet, $M = \bigcap_i V_i$ une décomposition de M comme intersection d'idéaux connexes V_i telle que A/M soit composé direct des idéaux U_i/M, où $U_i = \bigcap_{j \neq i} V_j$; alors A est composé direct des idéaux $N_i = \bigcap_{n=0}^{\infty} U_i^n$; et l'anneau N_i est canoniquement isomorphe à $A/(\bigcap_{n=0}^{\infty} V_i^n)$ qui est un anneau $(V_i/(\bigcap_{n=0}^{\infty} V_i^n))$-adique complet.

Ceci se déduit du th. 1 par récurrence.

Corollaire 2 - Un anneau semi-local complet A est isomorphe à un produit d'anneaux locaux complets.

En effet l'idéal M définissant la topologie de A est intersection finie d'idéaux maximaux, et on applique le cor. 1 .

Corollaire 3 - Un anneau A satisfaisant à la condition minimale est isomorphe à un produit fini d'anneau A_i de longueur finie, dont chacun possède un seul idéal premier, d'ailleurs nilpotent.

Soit M l'intersection des idéaux maximaux de A . Comme A/M satisfait à la condition minimale, M est déjà une intersection finie d'idéaux maximaux. On a vu (ou verra) au chapitre des anneaux primitifs que M est un idéal nilpotent (th. de Hopkins). Ainsi A est un anneau M-adique discret, et donc complet. Par conséquent le cor.1 montre qu'il est isomorphe à un produit fini d'anneaux A_i , dont chacun possède un idéal maximal nilpotent P_i . Tout idéal premier P de A_i contenant une puissance de P_i , doit contenir P_i et lui est donc identique. Enfin les groupes additifs P_i^{n-1}/P_i^n sont canoniquement munis de structures d'espaces vectoriels sur A_i/P_i ; comme A_i satisfait à la condition minimale, ceux ci sont de dimension finie ; et, comme P_i est nilpotent, le th. de Jordan-Holder montre que A_i est un anneau de longueur finie.

6 - Le lemme de Hensel.

Théorème 2 ("lemme de Hensel")- Soient A un anneau local complet, M son idéal maximal, f un polynome de degré n sur A , γ et γ' des polynomes sur A/M tels que γ soit de degré $r < n$, que $\gamma\gamma'$ soit le polynome $\overline{f}$ obtenu à partir de f par réduction mod.M de ses coefficients, et que γ et γ' soient étrangers. Il existe alors des polynomes g et g' sur A , de degrés r et n-r , tels que $f = gg'$, et que γ et γ' soient obtenus à partir de g et g' par réduction mod.M de leurs coefficients.

1) Une suggestion. Le lemme de Hensel est intimement lié au résultat du n° précédent. Considérons en effet l'anneau $B = A[X]/(f)$; c'est un A module de type fini (si l'on suppose f unitaire) ; nous verrons au § 3 que c'est un anneau (MB)-adique semi-local et complet. L'hypothèse du lemme de Hensel signifie que B/MB est composé direct des idéaux engendrés

par les classes de γ et γ' mod.$\overline{f}$. Le th.1 montre que cette décomposition se "prolonge" en une décomposition de B en somme directe de deux idéaux. On est donc tout près de la conclusion du th.2. Le seul ennui est qu'il faut passer de la décomposition (additive) dans $A[X]/(f)$ à une décomposition (multiplicative) du polynome f dans $A[X]$, point sur lequel le rédacteur s'est, jusqu'ici, escrimé en vain (il ne veut pas supposer A intègre, et passer à son corps des fractions). Il met la question au concours.

2) Démonstration classique. Etant donné deux polynomes h et h' sur A , nous écrirons $h \equiv h' \ (M^s)$ si les coefficients de h-h' appartiennent à M^s. Nous allons déterminer, par récurrence sur s , deux suites (g_s) et (g'_s) de polynomes de degrés r et n-r tels que $g_{s+1} \equiv g_s \ (M^s)$, $g'_{s+1} \equiv g'_s \ (M^s)$, $f \equiv g_s g'_s \ (M^s)$, et que γ et γ' soient obtenus à partir de g_s et g'_s par réduction mod.M de leurs coefficients. Les polynomes g_1 et g'_1 s'obtiennent en "relevant" arbitrairement γ et γ'. Supposons g_s et g'_s déterminés. Soit (m_i) un système fini de générateurs de M^s . Posons $g_{s+1}(X) = g_s(X) + \sum_i m_i v_i(X)$ et $g'_{s+1}(X) = g'_s(X) + \sum_i m_i v'_i(X)$. Il suffit de vérifier la condition $f \equiv g_{s+1} g'_{s+1} \ (M^{s+1})$ et la condition relative aux degrés, les autres étant automatiquement satisfaites. Or la première s'écrit, si l'on pose $f(X) - g_s(X) g'_s(X) = \sum_i m_i w_i(X)$, $\sum_i m_i (w_i - v_i g'_s - v'_i g_s) \equiv 0 \ (M^{s+1})$; en notant par une barre les polynomes obtenus par réduction mod.M des coefficients, ceci sera réalisé si l'on prend les polynomes v_i et v'_i tels que $\gamma' \overline{v}_i + \gamma \overline{v}'_i = \overline{w}_i$; or, comme γ et γ' sont étrangers, ceci est possible en vertu de l'identité de Bézout (Alg., chap.VII, § 1). Comme, par récurrence, les $\overline{w}_i$ sont au plus de degré n , on peut prendre les v_i de degré $\leqslant r$, et les v'_i de degré $\leqslant n-r$; la condition relative aux degrés reste ainsi satisfaite. Les suites des coefficients des polynomes (g_s) et (g'_s) sont alors des suites de Cauchy ;

comme A est complet, elles ont des limites, ce qui fournit les polynomes g et g' cherchés. CQFD .

Corollaire 1 - Soient A un anneau local complet d'idéal maximal M , et f un polynôme sur A tel que le polynôme $\overline{f}$ obtenu à partir de f par réduction mod.M des coefficients ait une racine simple $\alpha \in A/M$; il existe alors une racine simple $a \in A$ de f ayant α pour classe mod.M .

Exemples - Le polynome X^2+1 a une racine simple dans le corps à 5 éléments (la classe de 2 par exemple) ; il a donc une racine dans l'anneau des entiers 5-adiques.

Soit K un corps de caractéristique $\neq 2$; comme 1 a deux racines carrées dans K , la série formelle $1+Xs(X)$ a deux racines carrées dans $K[[X]]$.

Soient K un corps algèbriquement clos, et A l'anneau de séries formelles $K[[T]]$. Si $F(T,X)$ est un polynome sur A , et a une racine simple de $F(0,X)$, il existe une série formelle $x(T) \in A$ telle que $x(0)=a$ et que $F(T,x(T)) = 0$.

Corollaire 2 - Soient A un anneau local complet, M son idéal maximal ; supposons que A/M soit un corps de caractéristique 0 ; alors A contient un sous-corps K dont l'image canonique mod.M est A/M .

Comme A/M est de caractéristique 0 , tout élément de la forme n.1 de A (n entier non nul) est inversible ; donc A contient un corps isomorphe à Q . D'autre part l'ensemble des sous-corps de A , ordonné par inclusion est inductif. Soit donc K un sous-corps maximal de A . Notons p l'homomorphisme canonique de A sur A/M . Si A/M contenait un élément $\overline{x}$ transcendant sur $p(K)$, on aurait, x désignant un représentant de $\overline{x}$ dans A , $M \cap K[x] = (0)$, et A contiendrait $K(x)$. Ainsi A/M est algèbrique et séparable sur $p(K)$, et le cor.1 montre que l'on a $p(K) = A/M$.

Remarque - Lorsque A et A/M sont tout deux de caractéristique p , il existe encore un sous-corps K de A ayant la propriété énoncée au cor.2 . Ce corps K est unique lorsque A/M est parfait (démonstration astucieuse, mais raisonnablement courte, au moyen des "représentants multiplicatifs" de Hasse, etc.). Lorsque A/M est imparfait, la démonstration est effroyable. On sait aussi quelque chose lorsque A est de caract.0 et A/M de caract.p, mais c'est encore plus compliquée. En tous cas ce n'est pas ici le lieu.

---

§ 3 - Extensions finies d'anneaux M-adiques.

Définition 1 - On dit qu'un anneau B est une extension finie d'un anneau A si A est un sous-anneau de B , et si B est un A-module de type fini.

Lorsque B est extension finie de A , tout élément de B est entier sur A (chap.I, § 3).

1 - Propriétés des idéaux d'un anneau entier sur un autre.

On dit qu'un anneau B est entier sur un anneau A si A est un sous-anneau de B , et si tout élément de B est entier sur A .

Proposition 1 - Soit B un anneau entier sur l'anneau A ; pour tout idéal premier P de B , $P \cap A$ est premier ; pour que $P \cap A$ soit maximal, il faut et il suffit que P le soit.

Que $P \cap A$ soit premier est clair. Si $P \cap A$ est maximal, tout élément de l'anneau d'intégrité B/P est entier et donc algébrique le corps $A/(P \cap A)$; donc B/P est un corps (Alg.,chap.V), et P est maximal. Supposons maintenant P maximal ; tout élément a de $A/(P \cap A)$ a un inverse 1/a dans B/P ; écrivons que 1/a est entier sur $A/(P \cap A)$: $(1/a)^n + c_1(1/a)^{n-1} + \dots + c_n = 0$ avec $c_i \in A/(P \cap A)$; par multiplication par a^{n-1} on voit que 1/a est élément de $A/(P \cap A)$, ce qui montre que $A/(P \cap A)$ est un corps, et que $P \cap A$ est maximal .

Proposition 2 - Soient A un anneau, B un anneau entier sur A , et P' un idéal premier de A ; il existe un idéal premier P de B tel que $P' = P \cap A$. Si I est un idéal de B contenant P et distinct de P , on a $I \cap A \neq P'$.

Soit S le complément de P' dans A ; c'est un ensemble stable pour la multiplication ; formons les anneaux de fractions A_S et B_S (chap.I, § 1, n°1); l'anneau B_S est entier sur A_S (chap.I, § 3), et A_S est un anneau local d'idéal maximal $P'A_S$. Soit M un idéal maximal quelconque de B_S ; l'idéal $M \cap A_S$ est maximal (prop.1) ; on a donc $P'A_S = M \cap A_S$. Il suffit alors de prendre pour l'idéal noté $M \cap B$ (chap.I, § 1, n°1). Soit enfin I comme dans l'énoncé ; soit x un élément non nul de I/P ; considérons une équation de dépendance intégrale de plus petit degré de x sur A/P' :

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \quad (a_i \in A/P') \ .$$

Comme B/P est anneau d'intégrité, on a $a_n \neq 0$, sinon on obtiendrait par division par x une équation de dépendance intégrale de degré n-1 . Comme $a_n \in (A/P') \cap (I/P)$, ceci montre que $I \cap A \neq P'$.

Proposition 3 - Soient A un anneau, B un anneau entier sur A , et V un idéal de A ; l'idéal R de B composé des éléments dont une puissance appartient à BV , est identique à l'ensemble des éléments $x \in B$ satisfaisant à une équation de la forme $x^n + v_1 x^{n-1} + \ldots + v_n = 0$, où $v_i \in V$.

Si $x \in B$ satisfait à une équation de la forme ci-dessus, on a $x^n \in VB$, donc $x \in R$. Montrons réciproquement que tout élément x de R satisfait à une équation de dépendance intégrale à coefficients dans V . Si x^s satisfait à une telle équation, il en est de même de x ; nous pouvons donc nous borner au cas où $x \notin BV$. Lorsque x est de la forme $x = yv$ $(y \in B , v \in V)$, il suffit de multiplier par v^n une équation de dépendance intégrale de degré n de y sur A , pour obtenir une équation de dépendance intégrale de x à coefficients dans V . Il ne nous reste donc plus qu'à montrer que,

si y et z sont des éléments de B satisfaisant à des équations de dépendance intégrale à coefficients dans V, il en est de même de $y-z$. Par hypothèse il existe un entier r (resp.s) tel que tout monôme de degré $>r$ (resp.s) en y (resp.z) appartienne à $\sum_{i=0}^{r} Vy^i$ (resp. $\sum_{j=0}^{s} Vz^j$). Soient (t_k) $(1\leqslant k\leqslant (r+1)(s+1))$ les monômes $y^i z^j$ où $0\leqslant i\leqslant r$, $0\leqslant j\leqslant s$. Tout monôme $y^i z^j$ où $i>r$ et $j>s$ appartient alors à $\sum_k Vt_k$. On a par conséquent pour $1\leqslant k\leqslant (r+1)(s+1)$

$$(y-z)^{r+s+1}.t_n = \sum_k v_{nk}t_k \qquad \text{avec } v_{nk}\in V .$$

On en déduit $\det((y-z)^{r+s+1}\delta_{nk}-v_{nk})=0$, puisque l'un des t_k est égal à 1. Or ceci est une équation de dépendance intégrale à coefficients dans V satisfaite par $(y-z)^{r+s+1}$, et donc aussi par $y-z$.

2 - Généralités sur les extensions finies d'anneaux M-adiques.

Proposition 4 - Soient A un anneau M-adique noethérien, et B une extension finie de A.

a) Si M est intersection d'idéaux premiers, on a $MB\cap A = M$.

b) Pour que B soit un anneau (MB)-adique, il faut et il suffit qu'aucun élément de $1+M$ ne soit diviseur de zéro dans B.

c) Lorsque A est un anneau de Zariski, l'anneau (MB)-adique B est un anneau de Zariski.

d) Lorsque A est complet, il en est de même de l'anneau (MB) adique B.

e) Lorsque A est un anneau semi-local, il en est de même de B.

Soit $M=\bigcap_i P_i$ où les P_i sont des idéaux premiers de A ; soit P_i' un idéal premier de B tel que $P_i'\cap A = P_i$ (prop.2) ; on a alors $P_i'\supset MB$, $P_i\supset MB\cap A$ et $M\supset MB\cap A$; ceci démontre a). Comme $1+MB\supset 1+M$, la nécessité de b) résulte du th. de Krull (chap.II, § 3) ; réciproquement, de $(1-m')b=0$ $(m'\in MB$, $b\in B)$, on déduit par multiplication par b^n de l'équation de dépendance intégrale

$m'^n + a_1 m'^{n-1} + \ldots + a_n = 0$ que l'on a $b(1+a_1+\ldots+a_n)=0$; comme on peut supposer que $a_i \in M$ (prop.3) on en déduit l'existence d'un élément de $1+M$ qui est diviseur de zéro dans B ; comme B est noethérien, ceci et le th. de Krull montre la suffisance de b) . Lorsque A est un anneau de Zariski, tout élément de $1+M$ est inversible dans A (§ 2,cor.2 de la prop.3) et n'est donc pas diviseur de zéro dans B ; ainsi B est un anneau (MB)-adique ; d'autre part, pour tout idéal maximal P' de B , $P' \cap A$ est un idéal maximal de A (prop.1), et contient donc M ; donc MB est contenu dans l'intersection des idéaux maximaux de B , ce qui montre que B est un anneau de Zariski (§ 2,cor.2 de la prop.3) ; ceci démontre c). Supposons maintenant que A soit complet ; posons $B = \sum_i A b_i$; soit v_n une suite de Cauchy dans B ; on a $v_n - v_{n-1} \in M^{s(n)}B$ où $s(n)$ tend vers l'infini avec n ; on peut donc écrire $v_n - v_{n-1} = \sum_i a_{ni} b_i$ avec $a_{ni} \in M^{s(n)}$; comme A est complet, la série $\sum_{n=0}^{\infty} a_{ni}$ est convergente dans A ; désignons sa somme par a_i ; on voit alors aussitôt que $\sum_i a_i b_i$ est la limite de la suite (v_n) ; ainsi B est complet, et ceci démontre d). Supposons enfin A semi-local ; on peut alors prendre pour M l'intersection des idéaux maximaux de A ; on a alors, en vertu de a), $MB \cap A = M$; ainsi A/M s'identifie à un sous-anneau de B/BM , et B/BM est une extension finie de A/M ; comme A/M est un anneau de longueur finie (§ 2,prop.5), il en est de même de B/BM (chap.II, § 1) ; et, comme B est un anneau de Zariski (en vertu de c)), c'est un anneau semi-local (§ 2, prop.5) ; ceci démontre e) .

Remarque - La condition énoncée en b) n'est pas toujours satisfaite.

3 - Cas où le sous-anneau est un sous-espace topologique.

Soient A un anneau M-adique, B une extension finie de A, que nous supposons être un anneau (MB)-adique. Comme $M^n \subset (MB)^n \cap A$, la topologie M-adique de A est plus fine que la topologie induite sur A par la topologie (MB)-adique de B. On peut se demander si A est un sous-espace topologique de B. Ceci a lieu dans les cas suivants :

a) L'anneau B est somme directe de A et d'un sous A-module supplémentaire B'. En effet, pour tout idéal V de A, on a $VB = V+VB'$, et donc $VB \cap A = V$; en particulier $BM^n \cap A = M^n$. Ceci a lieu lorsque B est un A-module libre dont une base contient 1, et, plus particulièrement, si $B = A[b]$, où b est racine d'un polynome unitaire de degré n sur A mais d'aucun polynome de degré $< n$.

b) L'anneau A est un anneau semi-local complet (§2, cor.3 de la prop.8) ; plus généralement, A a la propriété décrite dans la prop.8 du §2 (par exemple A est l'anneau d'une valuation discrète).

c) L'anneau A est semi-local, et aucun élément non nul de A n'est diviseur de zéro dans B. Considérons en effet un système maximal et contenant 1, soit (y_j) d'éléments de B linéairement indépendants sur A ; comme B est extension finie de A, il existe un élément non nul c de A tel que $cB \subset \sum_j Ay_j$; on a alors $cBM^n \subset \sum M^n y_j$, et $c(BM^n \cap A) \subset M^n$ puisque les y_j sont linéairement indépendants et que l'un est égal à 1 ; alors le cor.2 de la prop.8 (§2) montre que l'on a $BM^n \cap A \subset M^{s(n)}$, où $s(n)$ tend vers l'infini avec n. Ceci montre que A est un sous-espace de B.

Proposition 5 - Soient A un anneau M-adique, B une extension finie de A ; supposons que B soit un anneau (MB)-adique, que A soit un sous-espace de B, et qu'aucun élément non nul de A ne soit diviseur de zéro dans le complété $\hat{B}$ de B. Alors :

a) L'adhérence de A dans $\hat{B}$ est le complété $\hat{A}$ de A , et $\hat{B}$ est extension finie de $\hat{A}$.

b) Les anneaux B et $\hat{A}$ sont linéairement disjoints sur A .

c) Tout élément $a \in \hat{A}$ qui est diviseur de zéro dans $\hat{B}$ est déjà diviseur de zéro dans $\hat{A}$.

Le fait que l'adhérence de A dans $\hat{B}$ est $\hat{A}$ se déduit aussitôt de ce que A est sous-espace de B ; d'autre part, si $D = \sum Ax_i$, $\sum \hat{A}x_i$ est un sous-anneau B' de $\hat{B}$, contenant B , et complet (prop°4,d)) ; donc $B' = \hat{B}$, et ceci démontre a). Pour démontrer b), considérons une famille finie (b_i) d'éléments de B linéairement indépendants sur A , et montrons que les b_i sont linéairement indépendants sur $\hat{A}$; nous pouvons supposer la famille (b_i) maximale. Il existe alors un élément non nul $c \in A$ tel que $cB \subset \sum Ab_i$. Supposons que l'on ait une relation $\sum a_i b_i = 0$ avec $a_i \in \hat{A}$. Pour tout n , soit a_{in} un élément de A tel que $a_i - a_{in} \in \hat{A}M^n$. On a alors $\sum a_{in} b_i \in \hat{B}M^n \cap B = BM^n$, et donc $\sum ca_{in} b_i \in \sum M^n b_i$; comme les b_i sont linéairement indépendants sur A , on en déduit $ca_{in} \in M^n$. Alors ca_i , qui est limite de la suite ca_{in} , est nul ; d'où $a_i = 0$ en vertu des hypothèses, et ceci démontre b) .

Démontrons enfin c). Soit a un élément de $\hat{A}$ tel qu'il existe un élément non nul b de $\hat{B}$ tel que $ab = 0$. Avec les notations précédentes on en déduit $0 = a.cb = \sum au_i b_i$ $(u_i \in \hat{A})$, d'où $au_i = 0$. Or les u_i ne sont pas tous nuls puisque c n'est pas diviseur de zéro dans $\hat{B}$. CQFD .

Remarque - Lorsque B est un anneau de Zariski, le cor. de la prop.7 (§ 2) montre que l'on peut remplacer la condition "aucun élément non nul de A n'est diviseur de zéro dans $\hat{B}$ " par "aucun élément non nul de A n'est diviseur de zéro dans B " .

4 - Le Vorbereitungssatz.

Proposition 6 - Soient A un anneau M-adique complet et B un anneau (MB)-adique quelconque contenant A tel que $MB \cap A = M$ et que B/MB soit 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.

Soit $(\bar{b}_i)$ un système fini de générateurs du (A/M)-module B/MB , et soient (b_i) des représentants des $\bar{b}_i$ dans B . Considérons un élément x de B , et supposons, par récurrence, que nous ayons déterminé des éléments y_{in} de A tels que $x \equiv \sum_i y_{in} b_i \pmod{M^n B}$. Soit (m_j) un système de générateurs de l'idéal M^n ; écrivons $x - \sum_i y_{in} b_i = \sum_j z_j m_j$ avec $z_j \in B$. Par définition il existe des $t_{ji} \in A$ tels que $z_j \equiv \sum_i t_{ji} b_i \pmod{MB}$. Alors, si l'on pose $y_{i,n+1} = y_{in} + \sum_j m_j t_{ji}$, on a $y_{i,n+1} - y_{in} \in M^n$, et $x - \sum y_{i,n+1} b_i \in BM^{n+1}$. Comme A est complet, les suites (y_{in}), qui sont des suites de Cauchy, ont des limites $y_i \in A$. Et on a $x - \sum_i y_i b_i \in \bigcap_{n=0}^{\infty} M^n B$, d'où $x = \sum_i y_i b_i$, puisque B est un anneau (MB)-adique. CQFD.

Théorème 1 ("Vorbereitungssatz formel") - Soient R un anneau local complet d'idéal maximal V , 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 $q = \sum_{i=0}^{s-1} a_i X^i$ $(a_i \in R)$.

La condition $f \notin VB$ veut dire que l'idéal Bf+BV est primaire pour l'idéal maximal BX+BV de B . Considérons le sous-anneau $A = R[[f]]$ de B . C'est un anneau local complet, dont l'idéal maximal M est Af+AV, et qui a même corps quotient A/M que R et B . L'anneau B est un anneau (MB)-adique. Comme les classes de $1, X, \ldots, X^{s-1}$ forment une base de

de $B/\mathfrak{M}B$ sur le corps $A/\mathfrak{M}$ d'après les hypothèses, la prop.6 montre que $(1, X, \ldots, X^{s-1})$ est un système de générateurs de B considéré comme A-module. On a donc $B = \sum_{0}^{s-1} AX^i = fB + \sum_{0}^{s-1} RX^i$, ce qui démontre l'existence de la décomposition $z = uf + q$.

Pour l'unicité, il suffit de montrer que 0 ne peut se représenter sous la forme $uf+q$ qu'avec $u=q=0$. Supposons donc que l'on ait $uf = \sum_{i=0}^{s-1} a_i X^i$ $(a_i \in R)$; en posant $u = \sum_{j=0}^{\infty} c_j X^j$ et $f = \sum_{j=0}^{\infty} b_j X^j$, ceci s'écrit

$$(1) \qquad \sum_{i+j=k} c_i b_j = 0 \quad \text{pour tout } k \geqslant s .$$

Nous allons montrer par récurrence sur n que l'on a $c_i \in \mathfrak{M}^n$ pour tout i. C'est clair qpour n=0. Supposons que l'on ait $c_i \in \mathfrak{M}^n$ pour tout i ; comme $b_j \in V$ pour $j \leqslant s-1$ et $b_s \notin V$, la relation

$$c_0 b_s + c_1 b_{s-1} + \ldots + c_s b_0 = 0$$

montre que $c_0 \in \mathfrak{M}^{n+1}$. Supposons alors, par récurrence sur t, que l'on ait $c_i \in \mathfrak{M}^{n+1}$ pour tout $i \leqslant t$; alors la relation

$$c_0 b_{s+t+1} + c_1 b_{s+t} + \ldots + c_{t+1} b_s + c_{t+2} b_{s-1} + \ldots + c_{t+s+1} b_0 = 0$$

montre que $c_{t+1} b_s \in \mathfrak{M}^{n+1}$ puisque $b_j \in V$ pour $j < s$; d'où $c_{t+1} \in \mathfrak{M}^{n+1}$. Ceci montre que l'on a $c_i \in \mathfrak{M}^{n+1}$ pour tout i. Comme $\bigcap_{n=0}^{\infty} \mathfrak{M}^n = (0)$, on en déduit que $c_i = 0$ pour tout i, c'est à dire $u=0$.

Remarque - La démonstration montre qu'on a $u \in R[[f]]$.

Pour démontrer le Vorbereitungssatz pour les séries convergentes la mirificque méthode ci-dessus ne marche pas, et il faut une formule explicite. Les algébristes s'arrachent les cheveux.

Démonstration explicite et katalogiesierbar.

Réduisons d'abord un peu le problème. Ecrivons

$$f(X) = b_0 + \ldots + X^s(b_s + g(X)) \quad \text{où } g(X) \in B .$$

Comme $b_s \notin V$, $b_s + g(X)$ est inversible dans D . En multipliant $u(X)$ par $b_s + g(X)$, nous sommes ramenés à trouver une série formelle $v(X)$ et un polynome $q(X)$ de degré $< s$ tels que

$$z(X) = v(X)(h(X)+X^s) + q(X)$$

où tous les coefficients de $h(X)$ sont dans V . D'autre part, en faisant rentrer dans $q(X)$ les termes de degré $< s$ de $z(X)$, on peut supposer $z(X)$ multiple de X^s . Donc, en changeant un peu les notations et les signes, on est ramené, étant donnés une série formelle $w(X)$ quelconque et une série formelle $p(X)$ dont tous les coefficients sont dans V , à trouver une série formelle $v(X)$ telle que

(2) $v(X)X^s - w(X)X^s - v(X)p(X)$ soit un polynome de degré $< s$.

Pour toute série formelle $f(X)$, notons $R(f)X^s$ la somme de ses termes de degrés $\geqslant s$. Définissons par récurrence une suite (w_n) de séries formelles au moyen de

(3) $\qquad w_1 = w \quad , \qquad w_{n+1} = R(pw_n)$.

D'après (2) les coefficients de $h_1 = v - w_1$ doivent tous appartenir à V ; et la condition (2) équivaut à

(2.1) $\quad h_1X^s - w_2X^s - h_1p$ est un polynôme de degré $< s$

puisque $w_2 = R(pw_1)$. Supposons par récurrence sur n que $h_n = v - (w_1 + w_2 + \ldots + w_n)$ ait tous ses coefficients dans V^n , et que la condition (2) soit équivalente à

(2.n) $\quad h_nX^s - w_{n+1}X^s - h_np$ est un polynome de degré $< s$.

Alors, en posant conformément à la récurrence, $h_n = w_{n+1} + h_{n+1}$, on voit que (2.n) équivaut à

(2.n') $\quad h_{n+1}X^s - w_{n+1}p - h_{n+1}p$ est un polynome de degré $< s$.

Comme $h_{n+1} + w_{n+1} = h_n$ a tous ses coefficients dans V^n , et p tous les siens dans V , ceci montre que h_{n+1} a tous ses coefficients dans V^{n+1} . D'autre part la définition de R et le fait que $w_{n+2} = R(pw_{n+1})$ montrent que (2.n') est équivalent à

(2.n+1) $h_{n+1}X^s - w_{n+2}X^s - h_{n+1}p$ est un polynome de degré $< s$. Ceci montre que, pour tout n , h_n a tous ses coefficients dans V^n et que pour tout n la condition (2.n) équivaut à la condition (2).

D'autre part on déduit aussitôt de (3) par récurrence sur n que w_n a tous ses coefficients dans V^n . Comme l'anneau de base R est un anneau local complet, ceci montre que la série $\sum_{n=1}^{\infty} w_n$ est convergente dans l'anneau local $B = R[[X]]$; soit v' sa somme. Le fait que h_n a tous ses coefficients dans V^n montre aussitôt que, s'il existe une série formelle v satisfaisant à (2), ce ne peut être que v'.

Montrons enfin que $v(X) = v'(X)$ satisfait à (2). En effet, par construction, la différence

$$(h_nX^s - w_{n+1}X^s - h_np) - (h_{n+1}X^s - w_{n+2}X^s - h_{n+1}p)$$

est un polynôme $a_n(X)$, de degré $< s$, et dont tous les coefficients appartiennent à V^{n+2} ; c'est en effet $w_{n+2}X^s - w_{n+1}p$, c'est à dire l'opposé de la somme des termes de degré $< s$ de $w_{n+1}p$. Comme R est complet la série $\sum_{n=1}^{\infty} a_n(X)$ converge dans B , et sa somme est un polynome de degré $< s$, soit $a(X)$. Comme tous les termes de (2.n) tendent vers 0 lorsque n tend vers l'infini, ceci montre que l'on a

$$h_1(X)X^s - w_2X^s - h_1(X)p(X) = a(X) ,$$

c'est-à-dire que $v(X)X^s - v(X)X^s - v(X)p(X)$ est un polynome de degré $< s$. CQFD.

En résumé il y a une série formelle $v(X)$ et une seule qui satisfasse à (2), et cette série est donnée par la formule

(4) $v = w + R(pw) + R(pR(pw)) + R(pR(pR(pw))) + \ldots$

Considérons maintenant un corps valué complet K . Nous dirons qu'une série entière à n variables et à coefficients dans K est convergente s'il existe un voisinage de 0 dans K^n où cette série converge.

Rappelons (chap. des séries entières) que ces séries convergentes forment un sous-anneau de l'anneau des séries formelles.

Théorème 2 ("Vorbereitungssatz") - Soient K un corps valué complet, R l'anneau des séries convergentes en $Z_1,\dots,Z_n$ à coefficients dans K, V son unique idéal maximal, et B l'anneau des séries convergentes en $Z_1,\dots,Z_n,X$ à coefficients dans K. Soit f(X) un élément de B n'appartenant pas à VB, et soit $b_s X^s$ $(b_s \in R)$ le terme de plus bas degré de f tel que $b_s \notin V$. Alors tout élément z(X) de B s'écrit, d'une façon et d'une seule sous la forme $z(X) = u(X)f(X) + q(X)$, avec $u \in B$ et $q = \sum_{i=0}^{s} a_i X^i$ $(a_i \in R)$.

Nous avons à montrer que les séries formelles u et q fournies par le th.1 sont convergentes. Or les opérations faites pour réduire le problème à la condition (2) (multiplication et division par la série convergente $b_s+g(X)$ dont le terme constant est $\neq 0$, suppression de termes, mise de X^s en facteurs) ne sont pas sortie de l'anneau des séries convergentes. Par conséquent les séries w et p de la condition (2) sont convergentes, et il s'agit de montrer que la série v donnée par la formule (4) est convergente. Alors les séries z, et donc q, seront convergentes.

Or la formule (4) montre que les coefficients de v s'expriment sous forme de polynomes à coefficients entiers positifs en les coefficients de w et p. Donc, si l'on remplace w et p par des séries majorantes w' et p', l'unique série formelle v' qui satisfait à (2) sera une majorante de v, puisqu'elle est donnée par la formule (4).

Par hypothèse p est de la forme $\sum_{i=1}^{n} Z_i p_i$. En choisissant convenablement les nombres réels >0 M et S, la fonction

$$M(1-S(Z_1+\dots+Z_n+X))^{-1}$$

est une majorante de w et des p_i . En posant $Z = Z_1+\ldots+Z_n$, on peut donc prendre pour majorantes de w et de p les fonctions

$$w' = M(1-S(Z+X))^{-1} \quad \text{et} \quad p' = MZ(1-S(Z+X))^{-1} .$$

Posons alors $v' = \sum_{k=0}^{\infty} c_k(Z)X^k$, et soit $\sum_{k=0}^{s-1} d_k(Z)X^k$ le polynome $v'X^s-w'X^s-v'p'$ (cf. condition (2)). On a alors l'égalité

$$(5) \quad \Big(\sum_{k=0}^{\infty} c_k(Z)X^k\Big)(X^s(1-S(Z+X))-MZ) = MX^s+(1-S(Z+X))\Big(\sum_{j=0}^{s-1} d_j(Z)X^j\Big) .$$

En égalant les coefficients des diverses puissances de X , on obtient à partir de (5) un <u>système linéaire</u> en les $c_k(Z)$ et $d_j(Z)$, dont les coefficients sont éléments du corps K(Z) des fractions fationnelles en Z . Comme ce système admet une solution unique (th.1), celle-ci se trouve dans K(Z) (Alg., chap.II, § 5). Donc $\sum_{j=0}^{s-1} d_j(Z)X^j$ est une fraction rationnelle en X et Z , et par conséquent aussi v' d'après l'égalité (5). Comme v' est développable en série entière, cette série est convergente. (Soit en effet A l'anneau local $(A[Z,X])_{(Z,X)}$; on a $v' = \alpha/\beta$ $(\alpha,\beta \in A)$ et $v' \in \hat{A}$; comme $\hat{A}\beta \cap A = A\beta$ (§ 2, cor.2 de la prop.4), on a $\alpha \in A\beta$ et $v' \in A$; donc v' s'écrit comme quotient de deux polynomes, le dénominateur étant $\neq 0$ à l'origine). Ceci démontre le th.2 (N-B : ceci est la première revanche des algébristes).

5 - <u>Conséquences du Vorbereitungssatz</u>.

<u>Définition 1</u> - <u>Soit</u> A <u>un anneau</u> ; <u>une série formelle</u> $f(Z_1,\ldots,Z_n,X)$ <u>sur</u> A <u>est dite régulière en</u> X <u>s'il existe un entier</u> s <u>tel que le terme en</u> X^s <u>de</u> f <u>soit</u> $\neq 0$; <u>autrement dit si on a</u> $f(0,\ldots,0,X) \neq 0$.

Dans les hypothèses des th.1 et 2 on a supposé la série f régulière.

<u>Proposition 7</u> - <u>Soit</u> K <u>un corps</u> (resp. <u>un corps valué complet</u>), B <u>l'anneau des séries formelles</u> (resp. <u>convergentes</u>) <u>en</u> $Z_1,\ldots,Z_n,X$ <u>sur</u> K , <u>et</u> f <u>un élément normal de</u> B ; <u>il existe un automorphisme</u> σ <u>de</u> B <u>laissant</u> X <u>invariant et tel que</u> $\sigma(f)$ <u>soit régulière en</u> X .

Nous allons montrer qu'il existe des entiers $u_1,\dots,u_n \geqslant 2$ tels que $f(X^{u_1},\dots,X^{u_n},X)\neq 0$. Alors les formules $\sigma(Z_i)=Z_i+X^{u_i}$, $\sigma(X)=X$ définiront un automorphisme de B (Alg., chap.IV, §6, et chap. des séries entières) répondant à la question.

Pour montrer l'existence des u_i nous procéderons par récurrence sur n. Il nous suffira alors de montrer que, si $g(Z,X)$ est une série formelle non nulle sur un anneau d'intégrité A, on ne peut avoir $g(X^u,X)=0$ pour tout entier $u \geqslant 2$. En effet montrons par récurrence sur n qu'alors $g(Z,X)$ est divisible par $\prod_{i=2}^{n}(Z-X^i)$; c'est clair pour $n=1$; de $g(Z,X) = g_n(Z,X)\prod_{i=2}^{n}(Z-X^i)$ et de $g(X^{n+1},X)=0$, on déduit $g_n(X^{n+1},X)\prod_{i=2}^{n}(X^{n+1}-X^i)=0$, d'où $g(X^{n+1},X)=0$ puisqu'un anneau de séries formelles sur un anneau d'intégrité est un anneau d'intégrité ; alors $g_n(Z,X) = g_n(Z,X)-g_n(X^{n+1},X)$ admet $Z-X^{n+1}$ pour facteur de chacun de ses termes, et est multiple de $Z-X^{n+1}$. Mais le fait que $g(Z,X)$ est divisible par $\prod_{i=2}^{n}(Z-X^i)$ pour tout n, montre que son ordre est $\geqslant n-2$ quel que soit n, contrairement à $g(X,Z)\neq 0$.

<u>Théorème 3</u> - <u>Soit</u> K <u>un corps valué complet</u> ; <u>l'anneau</u> B <u>des séries convergentes à</u> n <u>variables sur</u> K <u>est noethérien</u>.

Soit I un idéal de B ; nous allons montrer qu'il admet une base finie. Pour cela nous pouvons supposer $I \neq (0)$. Procédons par récurrence sur n, le cas n=0 étant trivial. Soit X l'une des variables, $Z_1,\dots,Z_{n-1}$ les autres. Prenons un élément non nul f de I. Il existe un automorphisme σ de B qui transforme f en une série $g = \sigma(f)$ régulière en X (prop.7). Il va nous suffire de montrer que $\sigma(I)$ a une base finie.

Pour cela, considérons un élément quelconque h de $\sigma(I)$, et appliquons lui le Vorbereitungssatz (th.2) : h est congru mod.g à une série convergente h' de la forme $\sum_{i=0}^{s-1} a_i(Z)X^i$, où les $a_i(Z)$ sont des éléments de l'anneau A des séries convergentes en $Z_1,\dots,Z_{n-1}$. Or h' parcourt

le sous-module $M \cap \sigma(I)$ du A-module M engendré par $(1, X, \ldots, X^{s-1})$. Comme A est un anneau noethérien d'après l'hypothèse de récurrence, ce sous-module admet une base finie $(b_1, \ldots, b_q)$ sur A (chap.II, § 1, cor.2 de la prop.2). Par conséquent $(g, b_1, \ldots, b_q)$ est une base finie de l'idéal $\sigma(I)$.

Proposition 8 - Soient K un corps (resp. un corps valué complet), B l'anneau des séries formelles (resp. convergentes) en $Z_1, \ldots, Z_n, X$ sur K ; toute série $f \in B$ qui est régulière en X est associée (Alg., chap.VI) dans B à un élément de la forme

$$X^s + a_{s-1}(Z)X^{s-1} + \ldots + a_0(Z) = p(X,Z) \cdot$$

où les a_i sont des séries formelles (resp. convergentes) en $Z_1, \ldots, Z_n$.

Soit en effet s l'ordre de la série $f(0, \ldots, 0, X)$. Prenons dans le th.1 (resp. th.2) $z(X) = X^s$. On a alors $X^s = u(Z,X)f(Z,X) + q(Z,X)$. Substituons $0, \ldots, 0$ à $Z_1, \ldots, Z_n$. Comme $f(0,X)$ est d'ordre s, la comparaison des termes en X^s des deux membres montre que $u(0,0) \neq 0$, c'est-à-dire que u est inversible dans B. Ainsi f est associé dans B à $X^s - q(Z,X)$, qui est de la forme annoncée.

Remarque - Le polynome unitaire en X, $p(Z,X)$, associé à f est appelé un polynome distingué.

Théorème 4 - Soient K un corps (resp. un corps valué complet), B l'anneau des séries formelles (resp. convergentes) en $Z_1, \ldots, Z_n, X$ sur K ; l'anneau B est un anneau factoriel (chap.I, § 5).

Nous procéderons par récurrence sur le nombre n+1 de variables, le cas $n+1 = 0$ étant trivial. Soit f un élément extrémal (= irréductible; cf.Alg., chap.VI) de B. Il nous suffira de montrer que l'idéal Bf est premier ; en effet :

Lemme - Soit B un anneau d'intégrité noethérien ; pour que B soit factoriel, il faut et il suffit que tout élément extrémal de B engendre un idéal premier. (ce lemme pourrait remonter au chap.II).

La nécessité a été démontrée au chap.I, § 5 (et même pour un anneau non noethérien). Réciproquement l'axiome (N') des suites croissantes d'idéaux montre que tout élément de B est produit d'une famille finie d'éléments extrémaux. Montrons l'unicité de cette décomposition (à des éléments inversibles près) : de $p_1 \dots p_n = p'_1 \dots p'_m$, les p_i et p'_j étant extrémaux, on déduit que l'un des p_i , soit p_1 , appartient à l'idéal Bp'_1 puisque celui-ci est premier ; comme p_1 est extrémal, il est nécessairement associé à p'_1 ; l'on divise alors par p_1 , et l'on continue par récurrence sur m .

Revenons à la démonstration du th.4 . En soumettant éventuellement B à un automorphisme, on peut supposer que f est régulière en x (prop.7). Notons A l'anneau des séries formelles (resp. convergentes) en $Z_1, \dots, Z_n$ sur K . D'après le th.1 (resp. th.2) on a $B = Bf + A[X]$; donc les anneaux B/Bf et $A[X]/(Bf \cap A[X])$ sont canoniquement isomorphes ; par conséquent, pour montrer que Bf est premier, il nous suffira de montrer que $Bf \cap A[X]$ est premier. Or (prop.8) f est associée dans B à un polynome unitaire g de $A[X]$; comme f est extrémal, il en est de même de g ; mais A est factoriel par récurrence, donc aussi l'anneau de polynomes $A[X]$ (chap.I, § 7, th.1) ; par conséquent l'idéal $gA[X]$ est premier. Ainsi il ne nous reste plus à montrer que l'égalité $Bf \cap A[X] = gA[X]$.

Soit B' l'anneau de séries formelles $A[[X]]$; c'est le complété de $A[X]$ pour la topologie $(XA[X])$-adique. Comme il contient B , on a $B'f = B'g$. Il nous suffira donc de montrer que l'on a $B'g \cap A[X] = gA[X]$.

c'est-à-dire puisque $A[X]$ est noethérien (th.3 (resp. § 1, cor.1 de la prop.4), et chap.II, § 1, th.1), que l'idéal $gA[X]$ est fermé pour la topologie $(XA[X])$-adique. Or c'est un idéal premier, et l'idéal (g,X) de $A[X]$ est distinct de $A[X]$ sinon g serait inversible dans B ; il suffit alors d'appliquer la prop.3 du § 2.

(N-B : les analystes (Behnke-Thüllen, Bochner-Martin) donnent, à la place du dernier alinéa, une démonstration plus élémentaire, mais bien plus longue ; les algébristes ont voulu prendre leur revanche).