Séminaire Henri Cartan

H. Cartan

Théorie des algèbres analytiques

Séminaire Henri Cartan, tome 6 (1953-1954), exp. n° 7, p. 1-23
<http://www.numdam.org/item?id=SHC_1953-1954__6__A7_0>

Séminaire E.N.S., 1953-54

THÉORIE DES ALGÈBRES ANALYTIQUES

(Exposé de H. Cartan, 25-1-1954,
revisé ultérieurement)

§1. Anneaux noethériens.

Nous rappelons ici quelques propriétés fondamentales des anneaux noethériens. Il s'agit uniquement d'anneaux commutatifs, à élément unité $1 \neq 0$. Un anneau A est dit noethérien si tout idéal de A possède un système fini de générateurs; il est bien connu que tout sous-module d'un module de type fini sur un anneau noethérien A est lui-même de type fini. On suppose aussi connu le théorème de Hilbert: l'anneau $A[X]$ des polynômes à coefficients dans un anneau noethérien A est noethérien; d'où il résulte, par récurrence sur n, que l'anneau $A[X_1, \ldots, X_n]$ des polynômes à n variables est noethérien.

Proposition 1 ("Lemme d'Artin-Rees"). *Soient A un anneau noethérien, I un idéal de A, E un A-module de type fini, F un sous-module de E. Dès que l'entier $r \geq 0$ est assez grand, on a, pour tout entier $n \geq r$,*

$$(1) \qquad (I^n E) \cap F = I^{n-r}(I^r E \cap F) .$$

Démonstration: l'inclusion $I^{n-r}(I^r E \cap F) \subset (I^n E) \cap F$ est triviale. Plus généralement, si $r \leq r' \leq n$, on a trivialement

$$(2) \qquad I^{n-r}(I^r E \cap F) \subset I^{n-r'}(I^{r'} E \cap F) .$$

Il suffira de montrer que, pour r assez grand, et $n \geq r$, on a

$$(3) \qquad (I^n E) \cap F \subset I^{n-r}(I^r E \cap F) .$$

Soit (u_i) un système fini de générateurs de l'idéal I; et soit (e_j) un système fini de générateurs du A-module E. Le sous-module $I^n E$ se compose des éléments de la forme $\Sigma_j P_j(u_i) e_j$, où les P_j sont des poly-

nômes homogènes de degré n par rapport à des variables X_i (en correspondance biunivoque avec les éléments u_i), et à coefficients dans A. Considérons l'ensemble B_n des systèmes de polynômes P_j homogènes de degré n, tels que $\Sigma_j P_j(u_i)e_j \in F$; ils engendrent un module gradué B sur l'anneau des polynômes $A[X_i]$, que est noethérien. Donc B est engendré, comme module sur $A[X_i]$, par un nombre fini d'éléments, qu'on supposer homogènes; soient r_α leurs degrés. Soit r le plus grand des r_α, et soit n un entier $\geq r$; on a

$$(I^n E) \cap F \subset \sum_\alpha I^{n-r_\alpha}(I^{r_\alpha}E \cap F) .$$

D'après (2), le second membre est contenu dans $I^{n-r}(I^r E \cap F)$, et ceci établit (3). La proposition est démontrée.

Soit toujours I un idéal de l'anneau A. Pour tout A-module E, on considère la topologie dans laquelle les $I^n E$ constituent un système fondamental de voisinages de zéro; on l'appellera la I-topologie de E.

Proposition 2. Soient A un anneau noethérien, et E un A-module de type fini. Si un idéal I est contenu dans le radical $\mathfrak{r}(A)$, la I-topologie de E est séparée.

Démonstration: rappelons que le radical d'un anneau (non nécessairement noethérien) est l'intersection des idéaux maximaux; et que si $a \in \mathfrak{r}(A)$, $1 + a$ est inversible dans A. On veut montrer que l'intersection F des sous-modules $I^n E$ est réduite à zéro. Or la relation (1), où l'on fait $n = r + 1$, donne

$$F = IF.$$

Comme F est un A-module de type fini, et que I est contenu dans le radical de A, ceci entraîne $F = 0$, en vertu d'un lemme connu, dont nous allons rappeler maintenant la démonstration (et qui est valable sans supposer que A soit noethérien):

Supposons d'abord que F soit engendré par un élément x, et montrons que la relation $F = IF$ entraîne $x = 0$. En effet, on doit avoir

$x = ax$ pour un $a \in I$, et comme $1 - a$ est inversible dans A, ceci entraîne $x = 0$. Soit maintenant F un A-module engendré par n éléments; montrons, par récurrence sur n, que la relation $F = IF$ entraîne $F = 0$. C'est vrai pour $n = 1$; pour $n > 1$, on a une suite exacte de A-modules

$$0 \to F' \to F \to F'' \to 0,$$

où F' est engendré par $n - 1$ éléments, et F'' par un élément. Le module F''/IF'' est quotient de F/IF, donc est nul; par suite $F'' = 0$, et F est isomorphe à F', donc engendré par $n - 1$ éléments; d'après l'hypothèse de récurrence, on a $F = 0$.

Corollaire. Dans un anneau noethérien A, l'intersection des puissances I^n d'un idéal contenu dans le radical $\mathfrak{r}(A)$ est réduite à zéro.

Proposition 3. Soient A un anneau noethérien, E un A-module de type fini, F un sous-module de E. Si un idéal I est contenu dans le radical $\mathfrak{r}(A)$, la I-topologie de F est la topologie induite par la I-topologie de E, et F est fermé dans E.

Démonstration: l'entier r étant choisi comme dans la proposition 1, la relation (1) donne

$$I^n F \subset (I^n E) \cap F \subset I^{n-r} F \quad \text{pour} \quad n \geq r,$$

ce qui prouve bien que la I-topologie de F est la même que la topologie induite sur F par la I-topologie de E. D'autre part, la I-topologie de E/F est la topologie quotient de la I-topologie de E, et puisque E/F est séparé (Proposition 2), F est fermé dans E.

§2. Eléments entiers sur un anneau.

Nous rappelons ici quelques notions classiques. Soit A un anneau avec élément unité 1, et soit B un sous-anneau de A contenant 1. On dit qu'un élément $a \in A$ est entier sur B s'il existe un polynôme unitaire $P(X)$ à coefficients dans B, tel que $P(a) = 0$.

Cette condition équivaut à chacune des deux suivantes:

(i) le sous-anneau engendré par B et a est un B-module de type fini;

(ii) il existe un sous-anneau A' de A, contenant a et B, et qui soit un B-module de type fini.

En effet, il est évident que si a est entier sur B, la condition (i) est satisfaite; et que (i) entraîne (ii). Il reste à prouver que (ii) entraîne que a est entier sur B; or soit (a_i) un système fini d'éléments de A' qui engendrent A' comme B-module; on suppose que 1 est l'un des a_i, et on écrit

$$aa_i = \sum_j u_{ij} a_j, \qquad u_{ij} \in B,$$

d'où $[\det(u_{ij} - \delta_{ij} a)]\cdot a_i = 0$ pour tout a_i; pour $a_i = 1$, cela donne $\det(u_{ij} - \delta_{ij} a) = 0$, ce qui prouve que a est entier sur B.

Si a_1 est entier sur B, et si a_2 est entier sur l'anneau (B, a_1) engendré par a_1 et B, alors le sous-anneau (B, a_1, a_2) engendré par a_1, a_2 et B est un B-module de type fini, donc a_2 est entier sur B. Si a_1 et a_2 sont entiers sur B, leur somme et leur produit sont dans (B, a_1, a_2), donc sont entiers sur B ; ainsi l'ensemble des éléments de A entiers sur B est un sous-anneau de A, qu'on appelle la fermeture intégrale de B dans A.

On dit qu'un anneau A est entier sur un sous-anneau B (ayant même élément unité) si tout élément de A est entier sur B.

Proposition 4. Si A est entier sur B, tout idéal maximal de A coupe B suivant un idéal maximal, et pour tout idéal maximal $\mathfrak{m}$ de B il existe un idéal maximal de A coupant B suivant $\mathfrak{m}$.

Cela résulte aussitôt du théorème de Krull-Cohen-Seidenberg,(1) qui affirme que tout idéal premier $\mathfrak{q}$ de B peut être "relevé" en un idéal premier $\mathfrak{p}$ de A (c'est-à-dire tel que $\mathfrak{p} \cap B = \mathfrak{q}$).

Corollaire. Le radical $\mathfrak{r}(B)$ est égal à l'intersection $B \cap \mathfrak{r}(A)$. Si A est un corps, B est un corps.

(1) Voir par ex. Bourbaki, Alg. commutative, Chap. V, §2, Théorème 1.

Soit A un anneau, et soit $F(A)$ l'anneau complet des fractions de A (c'est-à-dire l'ensemble des classes d'équivalence des quotients formels u/v, où $u \in A$, $v \in A$, v n'étant pas diviseur de zéro dans A; les opérations d'addition et de multiplication des quotients formels sont définies de la manière usuelle). L'anneau A s'identifie à un sous-anneau de $F(A)$; l'ensemble des éléments de $F(A)$ entiers sur A est un sous-anneau $\tilde{A}$ de $F(A)$, appelé la clôture intégrale de A. On dit qu'un anneau A est intégralement clos si $\tilde{A} = A$. Lorsque A est intègre, $F(A)$ est un corps, et la clôture intégrale $\tilde{A}$ est intègre.

Soit A un anneau noethérien sans élément nilpotent. Rappelons que les éléments minimaux dans l'ensemble des idéaux premiers de A sont en nombre fini [2]; ce sont des idéaux premiers $\mathfrak{p}_i$ dont l'intersection est réduite à 0. L'application naturelle

$$f: A \to \prod_i A/\mathfrak{p}_i ,$$

produit des applications

$$f_i: A \to A/\mathfrak{p}_i ,$$

est donc une injection; elle identifie l'anneau A à un sous-anneau du produit B des anneaux intègres $A/\mathfrak{p}_i = B_i$

Proposition 5. Sous les hypothèses précédents, l'application f induit un isomorphisme de la clôture intégrale $\tilde{A}$ sur le produit des clôtures intégrales $\tilde{B}_i$ des anneaux $B_i = A/\mathfrak{p}_i$.

Démonstration: les $a \in A$ qui sont non-diviseurs de zéro sont évidemment ceux qui n'appartiennent à aucun des $\mathfrak{p}_i$. Donc f_i se prolonge en un homomorphisme (noté encore f_i) de $F(A)$ sur $F(B_i)$, d'où un homomorphisme produit $F(A) \to \Pi_i F(B_i)$, qui prolonge f, et qu'on notera encore f. Il est clair que $\Pi_i F(B_i)$ s'identifie à l'anneau complet de fractions $F(B)$. D'autre part, f est une injection de $F(A)$ dans $F(B)$.

---

(2) Voir par ex. Bourbaki, Alg. commutative, Chap. II, §4, Coroll. 3 de la Proposition 14.

Comme $\mathfrak{p}_i$ n'est pas contenu dans l'intersection des $\mathfrak{p}_j$ pour $j \neq i$ (sinon $\mathfrak{p}_i$ serait contenu dans l'un de ces $\mathfrak{p}_j$, ce qui est absurde), il existe un $u_i \in A$ tel que $u_i \notin \mathfrak{p}_i$ et $u_i \in \mathfrak{p}_j$ pour tout $j \neq i$. L'élément $u = \Sigma_i u_i$ n'appartient à aucun des $\mathfrak{p}_i$, donc $u_i/u = e_i$ appartient à $F(A)$. On a

$$f_i(e_i) = 1, \quad f_j(e_i) = 0 \quad \text{pour} \quad j \neq i,$$

d'où $f((e_i)^2) = f(e_i)$, et par suite $(e_i)^2 = e_i$. Ainsi e_i est entier sur A, donc $e_i \in \tilde{A}$.

Montrons que f est un isomorphisme de $F(A)$ sur $F(B)$. Soit donné un système d'éléments $b_i \in F(B_i)$; choisissons $a_i \in F(A)$ tel que $f_i(a_i) = b_i$; prenons $a = \Sigma_i a_i e_i \in F(A)$. Alors $f_i(a) = b_i$ pour tout i, ce qui démontre l'assertion.

De plus, si chaque $b_i \in B_i$, on peut choisir $a_i \in A$, et alors $a = \Sigma_i a_i e_i$ est entier sur A. Donc si on identifie $F(A)$ à $F(B)$ au moyen de f, on voit que l'anneau B est entier sur A. Ces deux anneaux ont donc même fermeture intégrale dans $F(B)$, ce qui achève la démonstration.

Rappelons un autre résultat classique:

Proposition 6. Soit A un anneau noethérien, intègre et intégralement clos; soit F' un corps, extension algébrique séparable et de degré fini du corps $F(A)$. Alors la fermeture intégrale A' de A dans F' est un A-module de type fini (c'est donc un anneau noethérien).

Démonstration: on peut supposer que l'extension F' est engendrée sur $F(A)$ par un élément u (théorème de l'"élément primitif"), et il est loisible de choisir u entier sur A. Soit $P(X)$ le polynôme minimal de u par rapport au corps $F(A)$; ses coefficients sont entiers sur A, donc appartiennent à A puisque A est intégralement clos. On a $P'(u) \neq 0$, puisque les racines de $P(X)$ sont simples (P' désigne le polynôme dérivé de P). On va utiliser le lemme suivant:

Lemme 1. Soit A un anneau intègre et intégralement clos. Soit $P(X)$ un polynôme unitaire irréductible à coefficients dans A, dont toutes

les racines sont simples (dans une clôture intégrale du corps des fractions F(A)). Soit B l'anneau quotient A[X]/(P), et soit u la classe de X dans B. Alors, pour tout élément a de la clôture intégrale de B, le produit aP'(u) appartient à B.

Admettons ce lemme pour un instant, et achevons la démonstration de la Proposition 6. L'application A-linéaire injective $x \to xP'(u)$ de la fermeture intégrale A' dans l'anneau B identifie A' à un sous-A-module de B; comme B est un A-module de type fini et que A est noethérien par hypothèse, A' est un A-module de type fini, ce qui démontre la Proposition 6.

On va maintenant démontrer le Lemme 1. Si un y du corps des fractions F(B) est entier sur B, la trace Tr(y) (somme des conjugués de y par rapport à F(A) dans une clôture algébrique Ω de F(B)) est un élément de F(A) entier sur A, donc c'est un élément de A puisque A a été supposé intégralement clos. Ecrivons l'identité polynomiale

$$P(X) - P(Y) = (X-Y)(X^{n-1} + c_1(Y)X^{n-2} + \cdots + c_{n-1}(Y)) , \tag{4}$$

où n désigne le degré du polynôme unitaire P, et où les $c_i(Y)$ sont des polynômes de degré $< n$, à coefficients dans A. Dans (4), remplaçons Y par u, et X par l'un quelconque des n-1 conjugués u_i de u, distincts de u:

$$0 = u_i^{n-1} + c_1(u)u_i^{n-2} + \cdots + c_{n-1}(u) . \tag{5}$$

D'autre part, dérivons les deux membres de (4) par rapport à X, puis remplaçons X et Y par u:

$$P'(u) = u^{n-1} + c_1(u)u^{n-2} + \cdots + c_{n-1}(u) . \tag{6}$$

Soit alors a entier sur B; soit a_i le transformé de a par l'automorphisme de Ω qui transforme u en u_i. Multiplions les deux membres de (5) par a_i, sommons sur i, puis ajoutons (6) multiplié par a; il vient

$$aP'(u) = \mathrm{Tr}(au^{n-1}) + c_1(u)\ \mathrm{Tr}(au^{n-2}) + \cdots + c_{n-1}(u) ,$$

et le second membre appartient bien à l'anneau B, ce qui prouve le lemme.

Il sera utile d'expliciter le

Corollaire au Lemme 1. Soit A un anneau factoriel. Soit P(X) un polynôme unitaire de l'anneau A[X], dont les facteurs irréductibles soient tous distincts. Et soit B l'anneau A[X]/(P), quotient de A[X] par l'idéal engendré par P. Alors si $a \in \tilde{B}$ (clôture intégrale de B), on a

$$P'(u)\cdot a \in B,$$

u désignant la classe de X dans l'anneau quotient B.

Démonstration: puisque A est factoriel, il est intègre et intégralement clos; de plus, A[X] est factoriel, donc tout polynôme unitaire à coefficients dans A s'écrit d'une seule manière comme produit de polynômes unitaires P_i irréductibles. Soit $B_i = A[X]/(P_i)$; puisque les P_i sont distincts, B se plonge dans l'anneau produit $\Pi_i B_i$, et d'après la Proposition 5, la clôture intégrale $\tilde{B}$ s'identifie au produit $\Pi_i \tilde{B}_i$ des clôtures intégrales des anneaux intègres B_i. Il suffit donc de montrer que si $a_i \in \tilde{B}_i$, on a

$$P'(u)\cdot a_i \in B_i;$$

or $P'(u)\cdot a_i = Q_i(u)P_i'(u)\cdot a_i$ (avec $Q_i = P/P_i$), compte tenu du fait que $P_i(u)\cdot a_i = 0$. D'après le Lemme 1, $P_i'(u)\cdot a_i$ est dans B_i, d'où le résultat.

§3. Algèbres locales.

On sait qu'un anneau local est un anneau A (que nous supposons toujours commutatif, avec élément unité $1 \neq 0$) qui possède un seul idéal maximal, noté $\mathfrak{m}(A)$. Cet idéal est évidemment le radical de A. L'anneau quotient $A/\mathfrak{m}(A)$ est un corps, appelé corps des restes de A; l'application $\varepsilon: A \to A/\mathfrak{m}(A)$ s'appelle l'augmentation de l'anneau local A. Pour qu'un anneau A soit un anneau local, il faut et il suffit que $A/\mathfrak{r}(A)$ soit un corps.

Proposition 7. Soit A un anneau local, et soit B un sous-anneau de A, tel que A soit entier sur B. Alors B est un anneau

local dont l'idéal maximal est $B \cap \mathfrak{m}(A)$. Si de plus B est un anneau noethérien et A un B-module de type fini, l'anneau A est noethérien, la $\mathfrak{m}(A)$-topologie de A induit sur B la $\mathfrak{m}(B)$-topologie, et B est fermé dans A.

Démonstration: la première partie de l'énoncé résulte aussitôt de la Proposition 4. Supposons maintenant que B soit un anneau noethérien et A un B-module de type fini; alors tout idéal de A est un B-module de type fini, et a fortiori un A-module de type fini; donc A est noethérien. Appliquons la Proposition 3 en y remplaçant A par B, E par A, F par B, et I par $\mathfrak{m}(B)$. On voit que la $\mathfrak{m}(B)$-topologie de A induit sur B la $\mathfrak{m}(B)$-topologie de B, et que B est fermé dans A; il reste donc simplement à montrer que la $\mathfrak{m}(B)$-topologie de A coïncide avec sa $\mathfrak{m}(A)$-topologie.

Or la $\mathfrak{m}(B)$-topologie de A n'est autre que sa I-topologie, I désignant l'idéal de A engendré par $\mathfrak{m}(B)$; on a $I \subset \mathfrak{m}(A)$. On va prouver que I contient une puissance de $\mathfrak{m}(A)$. Or $B/\mathfrak{m}(B)$, qui est un corps K, se plonge dans A/I, et A/I est un K-module de type fini, autrement dit est un espace vectoriel de dimension finie sur K. La suite des images de $(\mathfrak{m}(A))^n$ dans A/I est une suite décroissante d'espaces vectoriels dont l'intersection est nulle, puisque la $\mathfrak{m}(A)$-topologie de A/I est séparée (Proposition 2). Il existe donc un entier n tel que l'image de $(\mathfrak{m}(A))^n$ dans A/I soit nulle; ceci achève la démonstration.

Définition: soit K un corps. On appelle K-algèbre locale une algèbre (commutative) A sur K, qui est un anneau local, et qui est somme directe de K et de son idéal maximal (cette dernière condition revient à dire que l'augmentation de A identifie K au corps des restes de A).

Sur une K-algèbre locale A, on considérera toujours la topologie définie par les puissances de l'idéal maximal $\mathfrak{m}(A)$; on dira que A est séparée si cette topologie est séparée (c'est-à-dire si l'intersection des

puissances de $\mathfrak{m}(A)$ est réduite à 0). Toute K-algèbre locale noethérienne est séparée.

Proposition 8. Soient A et A' des K-algèbres locales; tout homomorphisme de K-algèbres $f: A \to A'$ envoie $\mathfrak{m}(A)$ dans $\mathfrak{m}(A')$, donc est continu. Si B est une sous-algèbre d'une K-algèbre locale A, et si A est entière sur B, B est une K-algèbre locale; si de plus B est noethérienne et si A est un B-module de type fini, la topologie de A induit celle de B, et B est fermée dans A.

Démonstration: l'application composée de $f: A \to A'$ et de l'augmentation $\varepsilon': A' \to A'/\mathfrak{m}(A') \approx K$ applique A sur K, donc son noyau est un idéal maximal, c'est-à-dire $\mathfrak{m}(A)$; f applique donc $\mathfrak{m}(A)$ dans $\mathfrak{m}(A')$. Les autres assertions de l'énoncé résultent immédiatement de la proposition 7.

§4. Algèbres analytiques

A partir de maintenant, le corps K est un corps valué complet, non discret, fixé une fois pour toutes. Toutes les algèbres considérées sont des K-algèbres; "algèbre locale" signifiera K-algèbre locale.

On notera $H_n(X_1, \ldots, X_n)$, ou simplement H_n, l'algèbre des séries convergentes à n lettres $X_1, \ldots, X_n$ et à coefficients dans K. C'est un anneau noethérien et intégralement clos (cf. Séminaire 1951-52, Exposés 10 et 11). Et c'est une algèbre locale, dont l'idéal maximal se compose des séries dont le "terme constant" est nul. Plus généralement, étant donnée une famille quelconque de lettres X_i ($i \in I$), on notera $H_I(X_i)$ (ou simplement H_I) l'algèbre des séries convergentes en les lettres X_i, chaque série ne comportant qu'un nombre fini des X_i; cette algèbre s'identifie à une limite inductive d'algèbres de la forme H_n. Il est presque immédiat que H_I est une anneau factoriel (comme les H_n), donc intégralement clos; et que la topologie de H_I est séparée.

Définition: on appelle K-algèbre analytique (ou simplement: algèbre analytique) une K-algèbre locale séparée A qui possède la propriété suivante:

(AN) pour tout système fini de p éléments $a_i \in \mathfrak{m}(A)$ (p entier quelconque), il existe un homomorphisme de K-algèbres

$$\varphi: H_p(X_1, \ldots, X_p) \to A$$

tel que $\varphi(X_i) = a_i$.

Il est clair qu'un tel homomorphisme est unique: en effet, φ est bien déterminé sur la sous-algèbre des polynômes $K[X_1, \ldots, X_p]$, qui est dense dans H_p. Or φ est continu (Prop. 8).

Notation: pour tout $f(X_1, \ldots, X_p) \in H_p$, on notera $f(a_1, \ldots, a_p)$ l'image de f par l'unique homomorphisme φ de l'axiome (AN). Cette notation se justifie par les considérations suivantes:

L'algèbre H_n est une algèbre analytique: car c'est une algèbre locale séparée, qui vérifie (AN) (substitution de séries convergentes sans terme constant, aux variables d'une série convergente). Si les g_i ($1 \leq i \leq p$) sont des séries convergentes sans terme constant en $Y_1, \ldots, Y_n$, la fonction composée $f(g_1, \ldots, g_p)$ est bien l'élément de $H_n(Y_1, \ldots, Y_n)$, image de f par l'unique homomorphisme $\varphi: H_p \to H_n$ qui envoie X_i en $g_i(Y_1, \ldots, Y_n)$. Plus généralement, toute algèbre H_I est une algèbre analytique. Remarquons aussi que toute algèbre de séries formelles est un algèbre analytique.

Proposition 9. Soient A et B deux algèbres analytiques, et soit $\psi: A \to B$ un homomorphisme d'algèbres. Pour tout système de p éléments $a_i \in \mathfrak{m}(A)$ et pour tout $f \in H_p$, on a

$$\psi(f(a_1, \ldots, a_p)) = f(\psi(a_1), \ldots, \psi(a_p)) .$$

C'est une conséquence immédiate de l'unicité de l'homomorphisme $H_p \to B$ qui envoie les X_i dans les $\psi(a_i)$.

Quotients d'algèbres analytiques. Soit J un idéal fermé d'une algèbre analytique A, avec $J \neq A$. Alors A/J est une algèbre analytique. En effet, c'est une algèbre locale séparée, et la condition (AN) est satisfaite: car si on se donne des $b_i \in \mathfrak{m}(A/J)$, il suffit de les relever dans des $a_i \in \mathfrak{m}(A)$.

Proposition 10. Pour qu'une sous-algèbre B d'une algèbre analytique A soit une algèbre analytique, il faut et il suffit que, pour tout système fini p éléments $b_i \in B \cap \mathfrak{m}(A)$, et tout $f \in H_p$, l'élément $f(b_1, \ldots, b_p)$ soit dans B. (On exprime cette condition en disant que B est analytiquement stable.)

Démonstration: la condition est nécessaire; en effet, les éléments b_i sont non-inversibles dans B, puisqu'ils ne sont pas inversibles dans A; donc il existe un homomorphisme $H_p \to B$ qui envoie chaque X_i en b_i, et en composant cet homomorphisme avec l'injection $B \to A$, on obtient nécessairement l'unique homomorphisme $H_p \to A$ qui envoie X_i en b_i. Réciproquement, soit B une sous-algèbre analytiquement stable de A; B est somme directe de K et $B \cap \mathfrak{m}(A)$; les éléments non-inversibles de B sont exactement ceux de $B \cap \mathfrak{m}(A)$, car tout élément $k + b$ (avec $k \in K$, $k \neq 0$, $b \in B \cap \mathfrak{m}(A)$) possède un inverse dans B. En effet, soit $f(X)$ la fonction analytique $f(X) = 1/(k+X)$; il est clair que $f(b) \in B$ est inverse de $k+b$. Ainsi B est une algèbre locale, d'idéal maximal $B \cap \mathfrak{m}(A)$; elle est évidemment séparée, puisque A l'est, et la condition (AN) est satisfaite par B puisque B est une sous-algèbre analytiquement stable de A.

Soit A une algèbre analytique. Pour toute partie $B \subset A$, l'intersection des sous-algèbres analytiquement stables de A contenant B est une sous-algèbre analytiquement stable. Il existe donc une plus petite sous-algèbre analytique contenant B; on dit que c'est la sous-algèbre analytiquement engendrée par B. On dit qu'une algèbre analytique A est de génération finie s'il existe une partie finie B telle que A soit analytiquement engendrée par B.

Il est évident que les algèbres analytiques de génération finie sont celles qui sont isomorphes à une algèbre de la forme H_n/J (n entier quelconque, J idéal de H_n). Toutes ces algèbres sont noethériennes.

Soit donnée une algèbre analytique **A** de génération finie. Cherchons à quelle condition des éléments $a_1, \ldots, a_p$ de l'idéal maximal $\mathfrak{m}(A)$ engendrent analytiquement A.

Proposition 11. Pour que $a_1, \ldots, a_p \in \mathfrak{m}(A) = \mathfrak{m}$ engendrent analytiquement A, il faut et il suffit que leurs images dans le K-espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$ engendrent cet espace vectoriel.

Démonstration: si $a_1, \ldots, a_p$ engendrent analytiquement A, tout $x \in \mathfrak{m}$ s'écrit $\varphi(a_1, \ldots, a_p)$, où $\varphi(x_1, \ldots, x_p)$ est une fonction holomorphe (au voisinage de l'origine) dont le développement de Taylor commence par une fonction linéaire $f_1(x_1, \ldots, x_p)$. Donc x est congru à $f_1(a_1, \ldots, a_p)$ modulo $\mathfrak{m}^2$, et par suite les images de $a_1, \ldots, a_p$ dans $\mathfrak{m}/\mathfrak{m}^2$ engendrent l'espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$.

Réciproquement, supposons que les images des a_i dans $\mathfrak{m}/\mathfrak{m}^2$ l'engendrent comme K-espace vectoriel. Quitte à ne garder qu'une partie des a_i, on peut supposer que les images des a_i forment une base de l'espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$. Soient $b_1, \ldots, b_n$ des éléments de $\mathfrak{m}$ qui engendrent analytiquement l'algèbre **A**. Chaque a_i est congru, modulo $\mathfrak{m}^2$, à une fonction linéaire homogène $L_i(b_1, \ldots, b_n)$. Donc les $L_i(b_1, \ldots, b_n)$ engendrent $\mathfrak{m}/\mathfrak{m}^2$ comme espace vectoriel. On peut alors faire sur $b_1, \ldots, b_n$ une substitution linéaire de facon que $a_i - b_i$ soit congru à 0 mod $\mathfrak{m}^2$ pour $1 \leq i \leq p$, et que $b_{p+1}, \ldots, b_n$ soient dans $\mathfrak{m}^2$. On a donc des fonctions holomorphes $\varphi_i(x_1, \ldots, x_n)$ au voisinage de l'origine, d'ordre ≥ 2 à l'origine, telles que

$$\begin{cases} a_i = b_i + \varphi_i(b_1, \ldots, b_n) & \text{pour } i \leq p, \\ 0 = b_i + \varphi_i(b_1, \ldots, b_n) & \text{pour } i > p. \end{cases}$$

D'après le théorème des fonctions implicites, le système d'équations

$$x_i = y_i + \varphi_i(y_1, \ldots, y_n) \quad (1 \leq i \leq n)$$

équivaut, au voisinage de l'origine, à

$$y_i = x_i + \psi_i(x_1, \ldots, x_n) \quad (1 \leq i \leq n)$$

où les ψ_i sont holomorphes, d'ordre ≥ 2 à l'origine. On a donc, dans l'algèbre A, les relations

$$\begin{cases} b_i = a_i + \psi_i(a_1, \ldots, a_p, 0, \ldots, 0) & \text{pour } i \leq p. \\ b_i = \psi_i(a_1, \ldots, a_p, 0, \ldots, 0) & \text{pour } i > p. \end{cases}$$

Ainsi $b_1, \ldots, b_n$ s'expriment comme fonctions analytiques de $a_1, \ldots, a_p$, et par suite $a_1, \ldots, a_p$ engendrent analytiquement l'algèbre A.

C.Q.F.D.

Corollaire. Pour que l'algèbre analytique A (supposée de génération finie) puisse s'écrire comme quotient de H_n, il faut et il suffit que l'entier n soit au moins égal à la dimension du K-espace vectoriel $\mathfrak{m}(A)/\mathfrak{m}(A)^2$.

§5. Utilisation du "théorème de préparation" de Weierstrass (cf. Séminaire 1951-52, Exposé 10)

Considérons l'anneau H_{n+1} des séries convergentes à n+1 variables X, $X_1, \ldots, X_n$, et notons H_n l'anneau des séries convergentes en $X_1, \ldots, X_n$. Si $f \in H_{n+1}$, f définit une série entière en X à coefficients dans H_n; l'augmentation $\varepsilon: H_n \to K$, appliquée à chaque coefficient de cette série, donne une série entière (convergente) $\overline{f}(X) = f(X, 0, \ldots, 0)$. En particulier, à tout polynôme P(X) à coefficients dans H_n, l'augmentation associe un polynôme $\overline{P}(X)$ à coefficients dans le corps K. Un polynôme P(X) est distingué de degré p s'il est unitaire de degré p, et si $\overline{P}(X) = X^p$. Le théorème de préparation dit que si $f \in H_{n+1}$ est telle que la série $\overline{f}(X)$ soit d'ordre exactement égal à p (c'est-à-dire si X^p est en facteur dans $\overline{f}(X)$, mais non X^{p+1}), alors f s'écrit d'une seule manière comme un produit uP, où u est inversible dans H_{n+1}, et P est un

polynôme distingué de degré p. De plus, si P est un polynôme distingué de degré p, alors toute $g \in H_{n+1}$ s'écrit d'une manière et d'une seule

$$g = hP + R,$$

où $h \in H_{n+1}$ et R est un polynôme en X, de degré $< p$, à coefficients dans H_n. Dans le cas particulier où g est un polynôme en X à coefficients dans H_n, l'identité précédente n'est autre que l'identité de la division des polynômes à coefficients dans l'anneau H_n (le diviseur P étant un polynôme unitaire).

Remarque: La notion de polynôme distingué de degré p s'étend évidemment au cas plus général des polynômes en X à coefficients dans un anneau local quelconque.

Lemme 2. Soit B une K-algèbre analytique. Tout polynôme unitaire $P(X)$ à coefficients dans B peut se mettre sous la forme d'un produit $Q(X)R(X)$, où Q et R sont unitaires, Q étant distingué, et $R(0)$ étant inversible dans B.

Démonstration: soit p l'ordre du polynôme $\overline{P}(X)$ (à coefficients dans le corps K). Le polynôme $P(X)$ est somme de $\overline{P}(X)$ et d'un polynôme à coefficients $b_i \in \mathfrak{m}(B)$. Considérons des variables X_i; substituons-les aux coefficients b_i dans le polynôme $P(X)$; on obtient un polynôme $\pi(X)$ à coefficients dans H_n (n désigne le nombre des X_i), et $\overline{\pi}(X) = \overline{P}(X)$ est d'ordre p. D'après le théorème de préparation, $\pi(X)$ est de la forme uv, où u et v appartiennent à H_{n+1}, u étant un polynôme distingué en X (à coefficients dans H_n). L'identité $\pi = uv$ est alors nécessairement celle de la division des polynômes à coefficients dans H_n; autrement dit, v est un polynôme en X, à coefficients dans H_n. Par l'homomorphisme $H_n \to B$ qui envoie chaque X_i en b_i, $v(X)$ définit un polynôme $R(X)$ à coefficients dans B, et définit un polynôme distingué $Q(X)$, de degré p. On a ainsi

$$P(X) = Q(X)R(X), \quad \overline{P}(X) = \overline{Q}(X)\overline{R}(X),$$

et ceci montre que $\overline{R}(0)$ est égal au coefficient de X^p dans $\overline{P}(X)$, donc n'est pas nul. Donc $R(0)$ est inversible dans B.

Remarque: le Lemme 2 est en relation avec le "lemme de Hensel" (voir Appendice).

Lemme 3. Soient B une algèbre analytique, A une algèbre contenant B, et a $\in$ A un élément entier sur B. Pour que a soit racine d'un polynôme distingué à coefficients dans B, il suffit que soit remplie l'une des deux conditions suivantes:

1) a appartient au radical $\mathbf{r}(A)$;

2) A est intègre, et a n'est pas inversible dans A.

Démonstration: puisque a est entier sur B, il existe un polynôme unitaire $P(X)$, à coefficients dans B, tel que $P(a) = 0$. Soit une décomposition $P(X) = Q(X)R(X)$ comme dans le Lemme 2. On a donc $Q(a)R(a) = 0$, et de cela on veut conclure que $Q(a) = 0$ dans chacun des cas 1) et 2). Or $R(0)$ est inversible dans B; dans le cas 1), $R(a)$ est de la forme $R(0)(1+a')$, où $a' \in \mathbf{r}(A)$, donc $R(a)$ est inversible dans A, et on a donc bien $Q(a) = 0$. Dans le cas 2), on a $R(a) \neq 0$, sinon l'on aurait $R(a) = a^k + b_1 a^{k-1} + \cdots + b_k = 0$, où les $b_i \in B$, avec b_k inversible dans B; le produit de a par $(b_k)^{-1}(a^{k-1} + b_1 a^{k-2} + \cdots)$ serait donc égal à 1, et a serait inversible, contrairement à l'hypothèse. Ainsi on a $Q(a)R(a) = 0$ et $R(a) \neq 0$, et puisque A est intègre, on conclut que $Q(a) = 0$. Le lemme est donc démontré.

Ce lemme admet une réciproque partielle:

Lemme 4. Si un anneau A est entier sur un sous-anneau B, et si B est un anneau local, tout a $\in$ A qui est racine d'un polynôme distingué à coefficients dans B appartient au radical $\mathbf{r}(A)$.

En effet, on a $\mathbf{r}(A) \cap B = \mathbf{m}(B)$ (Coroll. de la Prop. 4). Si $Q(a) = 0$ (Q polynôme distingué), et si on réduit cette relation modulo $\mathbf{r}(A)$, on trouve que la classe a' de a modulo $\mathbf{r}(A)$ satisfait à $a'^p = 0$ (p entier), d'où $a' = 0$ puisque $\mathbf{r}(A)$ est intersection d'idéaux premiers (maximaux).

Théorème 1. Soient **A** une algèbre locale, et B une sous-algèbre de A, qui soit une algèbre analytique. Toute sous-algèbre A' de A qui contient B et est entière sur B est une algèbre analytique.

Démonstration: montrons d'abord que A' est une algèbre locale. Soit $a \in A' \cap \mathfrak{m}(A)$; a est racine d'un polynôme distingué à coefficients dans B (Lemme 3), donc appartient au radical $\mathfrak{r}(A')$ (Lemme 4). Réciproquement, tout élément $a \in \mathfrak{r}(A')$ est contenu dans $\mathfrak{m}(A)$, sinon il serait de la forme $k + r$ (avec $k \in K$, $k \neq 0$, $r \in \mathfrak{r}(A')$), donc il serait inversible dans A'. Ainsi $\mathfrak{r}(A') = A' \cap \mathfrak{m}(A)$, et A' est somme directe de K et de $\mathfrak{r}(A')$; A' est donc une algèbre locale, d'idéal maximal $A' \cap \mathfrak{m}(A)$.

Il reste à montrer que l'algèbre A' satisfait à la condition (AN). Soient donnés des $a_i \in \mathfrak{m}(A')$, en nombre égal à n; pour chaque i, il existe un polynôme distingué $Q_i(X)$, à coefficients dans B, tel que $Q_i(a_i) = 0$ (Lemme 3). Soit

$$Q_i(X) = X^{p_i} + \sum_{0 \leq j < p_i} b_{ij} X^j, \quad \text{avec} \quad b_{ij} \in \mathfrak{m}(B).$$

Introduisons des lettres X_i et Y_{ij}, et soit $P_i(X_i; Y_{ij})$ le polynôme

$$(X_i)^{p_i} + \sum_{0 \leq j < p_i} Y_{ij} (X_i)^j \quad .$$

Considérons-le comme polynôme en X_i à coefficients dans l'anneau $H(Y_{ij})$ des séries convergentes en les lettres Y_{ij}. Par application répétée du "théorème de préparation," on voit que, dans l'anneau $H(X_1, \ldots, X_n; Y_{ij})$, toute série convergente $f(X_1, \ldots, X_n)$ est congrue, modulo les $P_i(X_i; Y_{ij})$, à un polynôme $R(X_1, \ldots, X_n)$ à coefficients dans l'anneau $H(Y_{ij})$, polynôme dont le degré en X_i est $< p_i$. Par l'unique homomorphisme de l'algèbre $H(Y_{ij})$ dans B qui envoie Y_{ij} en b_{ij}, $R(X_1, \ldots, X_n)$ devient un polynôme $S(X_1, \ldots, X_n)$ à coefficients dans B, de degré $< p_i$ en X_i.

Cela dit, associons à chaque $f(X_1, \ldots, X_n)$ l'élément $S(a_1, \ldots, a_n) \in A'$, S désignant le polynôme défini par f. On définit ainsi une

application φ: $H(X_1, \ldots, X_n) \to A'$, et on vérifie facilement que c'est un homomorphisme d'algèbres, en utilisant les relations $P_i(a_i; b_{ij}) = 0$. Il est clair que $\varphi(X_i) = a_i$, et la propriété (AN) est ainsi établie pour l'algèbre A', ce qui achève la démonstration.

Corollaire. Soient A une algèbre analytique, et B une sous-algèbre analytique. Si A est analytiquement engendrée par des éléments $a_i \in \mathbf{m}(A)$ entiers sur B, alors A est entière sur B, et A est algébriquement engendrée par les a_i et B.

En effet, soit A' la sous-algèbre engendrée (algébriquement) par les a_i et B; A' est entière sur B. D'après le Théorème 1, A'est une algèbre analytique; puisque A est analytiquement engendrée par les a_i, on a nécessairement $\mathbf{A} = A'$.

Remarque. Dans la situation du corollaire précédent, supposons de plus que les a_i soient en nombre fini; alors B est une algèbre analytique de génération finie. (En effet, les a_i sont entiers sur une sous-algèbre analytique B' de B, de génération finie; d'après le corollaire, A est algébriquement engendrée par les a_i et B', donc A est un B'-module de type fini. Comme B' est neothérien, le sous-B'-module B de **A** est de type fini sur B', donc B est engendrée par B' et un nombre fini d'éléments.)

Théorème 2. Soient A une algèbre intègre, et B une sous-algèbre de A, qui soit une algèbre analytique. Si A est entière sur B, et si le corps de base K est algébriquement clos, alors A est une K-algèbre analytique.

Démonstration: montrons d'abord que A est une K-algèbre locale. Soit a un élément non inversible de A; d'après le Lemme 3, a est racine d'un polynôme distingué à coefficients dans B; donc (Lemme 4) a est dans le radical $\mathbf{r}(\mathbf{A})$. Ainsi $\mathbf{r}(\mathbf{A})$ contient tous les éléments non inversibles de A, et par suite A est un anneau local. Soit $K' = A/\mathbf{m}(\mathbf{A})$ son

corps des restes; puisque A est entier sur B, K' est une extension algébrique de $B/\mathfrak{m}(B) = K$, donc $K' = K$ puisque K est supposé algébriquement clos. Il s'ensuit que A est somme directe de K et de $\mathfrak{m}(A)$; autrement dit, A est une K-algèbre locale. Il suffit alors d'appliquer le Théorème 1, et le Théorème 2 est ainsi démontré.

Corollaire: la clôture intégrale d'une K-algèbre analytique et intègre est une K-algèbre analytique, lorsque K est algébriquement clos.

§6. Etude plus particulière des algèbres analytiques de génération finie.

Théorème 3. Soit A une algèbre analytique, analytiquement engendrée par des éléments $a_i \in \mathfrak{m}(A)$ en nombre fini égal à n. Dans l'espace vectoriel V engendré par les a_i, on peut trouver k éléments b_j jouissant des propriétés suivantes:

(a) si $f(X_1, \ldots, X_k)$ est telle que $f(b_1, \ldots, b_k) = 0$, alors f est identiquement nulle (on exprime cette propriété en disant que les b_j sont analytiquement indépendants);

(b) A est un B-module de type fini, B désignant la sous-algèbre analytiquement engendrée par les b_i.

Démonstration: l'énoncé est trivial si $n = 0$. Supposons-le démontré pour n-1, et prouvons-le pour n ($n \geq 1$). Si les a_i sont analytiquement indépendants, le théorème est démontré. Sinon, soit $f \in H_n$, avec $f(a_1, \ldots, a_n) = 0$, $f \neq 0$. On peut effectuer sur les variables $X_1, \ldots, X_n$ une substitution linéaire homogène (de déterminant $\neq 0$) telle que, après cette substitution, $f(0, \ldots, 0, X_n) \neq 0$. Le "théorème de préparation" dit alors que $f = uP$, $u \in H(X_1, \ldots, X_n)$ étant inversible, et P étant un polynôme distingué en X_n, à coefficients dans $H(X_1, \ldots, X_{n-1})$. L'élément $u(a_1, \ldots, a_n) \in A$ est inversible dans A, donc $P(a_n; a_1, \ldots, a_{n-1}) = 0$. Ainsi a_n est entier sur la sous-algèbre analytique A' engendrée par $a_1, \ldots, a_{n-1}$; d'après le corollaire au Théorème 1, A est un A'-module de type fini. En appliquant à A' l'hypothèse de récurrence, on obtient le théorème pour n. C.Q.F.D.

Corollaire. Toute algèbre analytique de génération finie est un module de type fini sur une sous-algèbre analytique isomorphe à une algèbre H_k, donc intégralement close.

(En effet, l'algèbre B du Théorème 3 est isomorphe à H_k, puisque les b_j sont analytiquement indépendants.)

Théorème 4. Soit K un corps algébriquement clos, de caractéristique nulle. La clôture intégrale $\tilde{A}$ d'une K-algèbre analytique A de génération finie est isomorphe au produit direct d'un nombre fini de K-algèbres analytiques, chacune d'elles étant de génération finie.

Démonstration: examinons d'abord le cas où A est intègre. Soit B une sous-algèbre analytique de A, de génération finie, intégralement close, et telle que A soit un B-module de type fini (Coroll. au Théorème 3). Appliquons la Proposition 6, en y remplaçant A par B, F(A) par F(B), et F' par F(A) (corps des fractions de A). On trouve que la clôture intégrale $\tilde{A}$ est un A-module de type fini; on sait d'autre part (Coroll. au Théorème 2) que c'est une algèbre analytique. C'est donc une algèbre analytique de génération finie.

Le cas général se ramène à ce cas particulier, grâce à la Proposition 5. En effet, avec les notations de cette proposition, les B_i sont des algèbres analytiques intègres, de génération finie.

APPENDICE

Le "lemme de Hensel" pour l'anneau des séries convergentes.

K désigne un corps valué complet, non discret. A désigne l'anneau des séries convergentes à n variables, à coefficients dans K. Soit ε: $A \to K$ l'augmentation qui, à chaque série convergente, associe son "terme constant."

A chaque polynôme P(X) à une variable X, et à coefficients dans A, on associe le polynôme $\overline{P}(X)$, à coefficients dans K, qu'on obtient en effectuant ε sur les coefficients de P(X).

LEMME DE HENSEL. Soit $P(X)$ un polynôme unitaire à coefficients dans A. Soit donnée une décomposition

$$\bar{P}(X) = Q_1(X)Q_2(X)$$

dans l'anneau $K[X]$, Q_1 et Q_2 étant des polynômes unitaires, premiers entre eux. Alors il existe un système unique de deux polynômes unitaires $P_1(X)$, $P_2(X)$ à coefficients dans A, tels que

(1) $\bar{P}_i(X) = Q_i(X)$ pour $i = 1, 2$;

(2) $P(X) = P_1(X)P_2(X)$.

Démonstration: on va d'abord prouver l'unicité, en procédant par identification. Le développement de chaque coefficient de $P(X)$ en série de polynômes homogènes dans l'anneau A permet d'écrire

$$P(X) = \bar{P}(X) + \sum_{k \geq 1} P^k(X) ,$$

les coefficients de P^k étant des éléments homogènes de degré k de A. Puisque $P(X)$ est unitaire, chaque $P^k(X)$ est un polynôme en X de degré $< p$, en notant p le degré de $P(X)$, qui est aussi celui de $\bar{P}(X)$. De même, les polynômes inconnus $P_i(X)$ $(i = 1,2)$ s'écrivent

$$P_i(X) = Q_i(X) + \sum_{k \geq 1} P_i^k(X),$$

$P_i^k(X)$ étant de degré $< q_i$, en notant q_i le degré de $P_i(X)$, qui est aussi celui de $Q_i(X)$; on a $p = q_1 + q_2$.

Le calcul formel des $P_i^k(X)$ s'effectue comme suit. La relation (2) équivaut à l'ensemble des relations $(k = 1,2,\ldots)$

$$(3) \quad P_2^k(X)Q_1(X) + P_1^k(X)Q_2(X) = P^k(X) - \sum_{0 < h < k} P_1^h(X)P_2^{k-h}(X) .$$

Si les P_i^h sont connus pour $h < k$, cette relation détermine P_1^k et P_2^k, à cause des restrictions imposées à leurs degrés; en effet, on a vu que

$$\deg P_i^k < \deg Q_i .$$

La solution explicite de (3) est la suivante: *si* $U_1(X)$ *et* $U_2(X)$ *désignent les polynômes, à coefficients dans* K, *de degrés respectivement* $< q_1$ *et* $< q_2$, *tels que l'on ait l'identité de Bezout*

$$(4) \quad U_2Q_1 + U_1Q_2 = 1 ,$$

alors P_i^k *est le reste de la division, par le polynôme unitaire* Q_i, *du polynôme produit* $U_i(P^k - \Sigma_{0<h<k} P_1^h P_2^{k-h})$. D'où le calcul des P_i^k par récurrence sur k. Et ceci prouve l'unicité.

Pour démontrer l'existence, nous prenons les polynômes $P_i^k(X)$ tels qu'ils viennent d'être définis. Alors les polynômes

$$P_i(X) = Q_i(X) + \sum_{k \geq 1} P_i^k(X) \qquad (i = 1, 2)$$

sont définis comme polynômes à coefficients dans l'anneau des séries formelles (par rapport aux n variables de l'anneau A), et ils satisfont formellement à (2). Il reste à prouver que leurs coefficients sont, en fait, des séries convergentes. On va utiliser dans ce but une méthode de majorantes.

Introduisons une variable $r > 0$, qui majore toutes les variables de l'anneau A. Pour chaque polynôme en X, à coefficients homogènes de degré k par rapport aux variables de A, on appellera "majoration" de ce polynôme un nombre de la forme ar^k qui majore la somme des valeurs absolues des coefficients de ce polynôme (lorsque les variables de A sont majorées par r); a désigne un nombre réel > 0. Tous les polynômes considérés sont de degré borné (strictement inférieur à 2p). Donc si ar^k majore un polynôme R, le reste de la division de R par l'un des Q_i est majoré par bar^k (b désignant un nombre fixe > 0).

Puisque le polynôme donné P a ses coefficients dans l'anneau des séries convergentes, il existe $M > 0$ tel que chacun des P^k soit majoré par Mr^k. Soit c une majoration des deux polynômes U_1 et U_2; on obtient une majoration $N_k r^k$ de chacun des polynômes P_1^k et P_2^k en prenant

$$N_1 = bcM, \quad N_k = bc\Big(M + \sum_{0<h<k} N_h N_{k-h}\Big) \quad \text{pour} \quad k \geq 2.$$

Tout revient à montrer que les N_k ainsi calculés sont les coefficients d'une série entière $\Sigma_{k\geq 1} N_k z^k$ dont le rayon de convergence est $\neq 0$.

La relation qui définit les N_k par récurrence est

$$N_k/N_1 = 1 + (bcN_1)\Big[\sum_{0<h<k} (N_h/N_1)(N_{k-h}/N_1)\Big], \quad k \geq 2 .$$

On peut supposer $bcN_1 \geq 1$ (puisqu'on peut toujours remplacer M par un nombre plus grand). Définissons des nombres a_k par récurrence en posant:

$$(5) \qquad a_1 = 1, \quad a_k = 1 + \sum_{0<h<k} a_h a_{k-h} \quad \text{pour} \quad k \geq 2 .$$

On vérifie immédiatement que l'on a

$$N_k/N_1 \leq a_k (bcN_1)^{k-1} ,$$

et par suite tout revient à prouver que la série $\Sigma_{k\geq 1} a_k z^k$ a un rayon de convergence $\neq 0$. Or cette série est le développement de la fonction holomorphe $f(z)$ définie par la relation

$$(f(z))^2 - f(z) + \frac{z}{1-z} = 0 \quad (f(0) = 0),$$

car la méthode des coefficients indéterminés, appliquée à cette équation, donne les relations (5); la solution est bien holomorphe, puisque c'est

$$\frac{1}{2}\left(1 - \sqrt{1 - \frac{4z}{1-z}}\right)$$

(la détermination du radical étant celle qui est égale à 1 pour $z = 0$).

Ceci achève la démonstration.