SÉMINAIRE HENRI CARTAN

R. GODEMENT

Topologies *m*-adiques

Séminaire Henri Cartan, tome 8 (1955-1956), exp. n° 18, p. 1-12
<http://www.numdam.org/item?id=SHC_1955-1956__8__A18_0>

© Séminaire Henri Cartan
(Secrétariat mathématique, Paris), 1955-1956, tous droits réservés.

L'accès aux archives de la collection « Séminaire Henri Cartan » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire E.N.S., 1955/56
(H. CARTAN et C. CHEVALLEY)

TOPOLOGIES m-adiques

(Exposé de R. GODEMENT, 30.4.1956)

1.- Topologies définies par des filtrations.

Soit E un groupe abélien filtré par des sous-groupes E_n :

$$E_n \supset E_{n+1} \quad , \qquad \bigcup_n E_n = E \quad .$$

On en déduit une topologie de groupe sur E, en prenant les E_n comme système fondamental de voisinages de 0 dans E. Pour que E soit séparé il faut et il suffit que $\bigcap E_n = 0$; plus généralement, un sous-groupe F de E est fermé si et seulement si l'on a

$$F = \bigcap_n (F + E_n) \quad .$$

Soit $\hat{E}$ le complété de E pour la topologie précédente. Le complété $\hat{F}$ d'une partie F de E (pour la structure uniforme induite) s'identifie évidemment à l'adhérence de F dans $\hat{E}$, et la topologie de $\hat{E}$ est définie par les sous-groupes $\hat{E}_n$. Si F est un sous-groupe fermé de E on a un isomorphisme canonique

$$E/F = \hat{E}/\hat{F}$$

(il n'y a aucune difficulté à cause du fait que la topologie de E est définie par une distance, ou tout au moins par un écart ; on peut aussi remarquer qu'une suite de Cauchy dans E/F est l'image d'une suite de Cauchy dans E) .

En particulier prenons $F = E_n$, qui est un sous-groupe ouvert et donc fermé ; E/E_n est discret, donc complet ; par suite il vient $E/E_n = \hat{E}/\hat{E}_n$, autrement dit

$$G(E) = G(\hat{E}) \quad . \tag{1}$$

Soit A un anneau (commutatif pour simplifier), filtré par une suite $(\mathfrak{m}_n)$ d'idéaux ; la topologie correspondante est une topologie d'anneau, et par suite le complété $\hat{A}$ est lui-même un anneau ; si E est un A-module, filtré par des sous-modules E_n tels que

$$\mathfrak{m}_p . E_q \subset E_{p+q} \quad ,$$

alors $\hat{E}$ est canoniquement un $\hat{A}$-module.

Le cas le plus important s'obtient en filtrant A par les puissances d'un idéal $\underline{m}$; si E est un A-module, la topologie définie par les sous-modules $\underline{m}^n.E$ est la topologie $\underline{m}$-adique sur E. Il ne faudrait pas croire que, dans ce cas, la topologie de $\hat{E}$ coïncide nécessairement avec la topologie $\hat{\underline{m}}$-adique (voir Théorème 2,(e), où l'on trouvera une condition suffisante pour qu'il en soit ainsi).

2.- Anneaux de Zariski.

Un anneau de Zariski est un couple $(A , \underline{m})$, où A est un anneau commutatif, avec unité, noethérien, et où $\underline{m}$ est un idéal contenu dans le radical de A (i.e. tel que tout élément de $1 + \underline{m}$ soit inversible). Dans ce numéro on munit tous les A-modules de la topologie $\underline{m}$-adique.

Théorème 1.- Soit $(A , \underline{m})$ un anneau de Zariski ; tout A-module E de type fini est séparé, tout sous-module F de E est fermé, et la topologie $\underline{m}$-adique de F est induite par la topologie $\underline{m}$-adique de E.

Ce théorème a été démontré dans l'Exposé 2, (cf. commentaires suivant le théorème 3), comme conséquence du Théorème de Krull-Artin.

On notera que la condition $\underline{m} \subset \underline{r}(A)$ est nécessaire pour assurer que tout module de type fini est séparé ; si en effet $1 + m$ $(m \in \underline{m})$ n'est pas inversible, i.e. est contenu dans un idéal $\underline{a} \neq A$, il existe dans le module $E = A/\underline{a}$ un $x \neq 0$ tel que $x + mx = 0$ en sorte que $x \in \bigcap \underline{m}^n.E$; E n'est donc pas séparé.

Théorème 2.- Soit $(A , \underline{m})$ un anneau de Zariski.

(a) - Si E et F sont des A-modules de type fini, tout homomorphisme algébrique $u : E \longrightarrow F$ est un homomorphisme topologique.

(b) - Pour tout A-module E de type fini on a un isomorphisme

$$\hat{E} = \hat{A} \underset{A}{\otimes} E \quad .$$

(c) - Le foncteur $E \longrightarrow \hat{A} \underset{A}{\otimes} E$ est exact sur la catégorie des A-modules.

(d) - Soit E un A-module de type fini. Pour tout sous-module F de E on a dans $\hat{E}$ les relations

$$\hat{F} = \hat{A}.F \quad ; \quad F = \hat{F} \cap E \quad .$$

Si F et G sont deux sous-modules de E, on a

$$\hat{F} \cap \hat{G} = \widehat{F \cap G} \quad ; \quad \hat{F} + \hat{G} = \widehat{F + G} \quad .$$

(e) - Si E est un A-module de type fini, la topologie de $\hat{E}$ est identique à la topologie $\hat{\mathfrak{m}}$-adique du $\hat{A}$-module $\hat{E}$.

(f) - Soit E un A-module de type fini ; si des éléments x_i de E sont linéairement indépendants sur A, ils le sont aussi sur $\hat{A}$.

(g) - Supposons A intègre, et soit E un A-module de type fini sans torsion ; alors les éléments de $\hat{A}$ qui sont diviseurs de zéro dans $\hat{E}$ le sont déjà dans $\hat{A}$.

(a) : on a $u(\mathfrak{m}^n.E) = \mathfrak{m}^n.u(E)$, donc la topologie $\mathfrak{m}$-adique de $u(E)$ est quotient de celle de E ; mais (Théorème 1) elle est induite par la topologie $\mathfrak{m}$-adique de F, d'où le résultat.

(b) : E étant de type fini et A noethérien, on a une suite exacte

$$L_1 \longrightarrow L_o \longrightarrow E \longrightarrow 0$$

où L_o et L_1 sont libres et de type fini. On en déduit un diagramme commutatif

$$\begin{array}{ccccccc} \hat{A}\otimes L_1 & \longrightarrow & \hat{A}\otimes L_o & \longrightarrow & \hat{A}\otimes E & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ \hat{L}_1 & \longrightarrow & \hat{L}_o & \longrightarrow & \hat{E} & \longrightarrow & 0 \end{array} \quad ;$$

la première ligne est exacte en vertu des propriétés générales des produits tensoriels ; la seconde ligne l'est aussi, en vertu de (a). Il suffit donc de démontrer que $\hat{L} \approx \hat{A}\otimes L$ lorsque L est de la forme A^n, ce qui est trivial.

(c) : d'après (a) et (b) on sait déjà que le foncteur $E \longrightarrow \hat{A}\otimes E$ est exact sur la catégorie des A-modules de type fini ; cela suffit, comme on sait, à entraîner (c), parce que tout A-module est limite inductive de modules de type fini, et que le produit tensoriel commute aux limites inductives. (Mais bien entendu $\hat{A}\otimes E$ n'est pas nécessairement le complété de E si E n'est pas de type fini).

(d) : d'après (c) l'homomorphisme $\hat{A}\otimes F \longrightarrow \hat{A}\otimes E$ est injectif ; si donc l'on identifie $\hat{E}$ à $\hat{A}\otimes E$, $\hat{F}$ s'identifie à l'image de $\hat{A}\otimes F$ dans $\hat{E}$, c'est-à-dire à $\hat{A}.F$; $F = \hat{F}\cap E$ résulte du fait que F est fermé dans E. L'assertion concernant F et G se réduit de la suite exacte

$$0 \longrightarrow F\cap G \xrightarrow{u} F\times G \xrightarrow{v} F+G \longrightarrow 0$$

où $u(x) = (x , x)$ et où $v(x , y) = x - y$. En prenant son produit tensoriel par $\hat{A}$ on en déduit la suite exacte

$$0 \longrightarrow \hat{F}\cap\hat{G} \longrightarrow \hat{F}\times\hat{G} \longrightarrow \hat{F}+\hat{G} \longrightarrow 0 \quad ,$$

d'où les résultats cherchés.

(e) : soit $E_n = \underline{m}^n.E$; la topologie de $\hat{E}$ est définie par les sous-modules $\hat{E}_n$; or d'après (d) on a

$$\hat{E}_n = \hat{A}.E_n = \hat{A}.\underline{m}^n.E = (\hat{A}.\underline{m})^n.E = (\hat{\underline{m}})^n.E \quad ,$$

ce qu'il fallait démontrer.

(f) : on peut supposer les x_i en nombre fini n ; l'hypothèse qu'ils sont linéairement indépendants montre alors que l'homomorphisme $u : A^n \longrightarrow E$ donné par

$$u((a_i)) = \sum a_i x_i$$

est injectif ; en vertu de (b) et (c) il en est donc de même de $\hat{u} : \hat{A}^n \longrightarrow \hat{E}$, d'où le résultat.

(g) : soit K le corps des quotients de A ; comme E est sans torsion, il se plonge dans $K \underset{A}{\otimes} E$, vectoriel de dimension finie sur K, et comme E est de type fini on voit que l'on peut plonger E dans un A-module libre L, auquel cas $\hat{E} = \hat{A} \underset{A}{\otimes} E$ se plonge dans $\hat{A} \underset{A}{\otimes} L$, i.e. dans un $\hat{A}$-module libre, d'où évidemment le résultat.

3.- Anneaux semi-locaux.

On appelle anneau semi-local tout couple (A , q), où A est un anneau noethérien et $\underline{q}$ un idéal vérifiant les conditions suivantes :

(i) A n'a qu'un nombre fini d'idéaux maximaux ;
(ii) on a $\underline{r}(A) \supset \underline{q} \supset \underline{r}(A)^k$ pour un entier k.

Il est clair que $(A , \underline{q})$ est un anneau de Zariski, et que la topologie de A définie par $\underline{q}$ est la même que celle définie par $\underline{r}(A)$.

Pour qu'un couple $(A , \underline{q})$, où A est noethérien, soit semi-local, il faut et il suffit que les idéaux premiers de A contenant $\underline{q}$ soient exactement les idéaux maximaux de A. C'est nécessaire : si $(A , \underline{q})$ est semi-local, et si $\underline{p}$ premier contient $\underline{q}$, alors $\underline{p}$ contient une puissance de $\underline{r}(A)$, donc contient $\underline{r}(A)$, intersection d'un nombre fini d'idéaux maximaux ; donc $\underline{p}$ contient l'un d'eux, et par suite lui est identique ; d'autre part tout idéal maximal contient $\underline{r}(A)$, donc $\underline{q}$. C'est suffisant : en effet, s'il en est ainsi, tout idéal premier contenant $\underline{q}$ est minimal dans l'ensemble des idéaux premiers contenant $\underline{q}$, donc ces idéaux sont en nombre fini, ce qui prouve (i) ; la propriété (ii) résulte alors de l'Exposé 2 (corollaire au théorème 4).

Proposition 1.- Soit (A , q) un anneau semi-local ; soit A' un anneau contenant A, et tel que A' soit un A-module de type fini ; si q' désigne l'idéal $A'.q$, le couple (A' , q') est un anneau semi-local.

En effet, il est clair que A' est noethérien, et entier sur A. Montrons que les idéaux premiers de A' contenant q' sont exactement les idéaux maximaux. Si p' est maximal, $p' \cap A$ est un idéal maximal de A (Exposé 1, corollaire 1 du théorème 3), donc contient q, et par suite p' contient q'. Réciproquement, soit p' un idéal premier contenant q' ; alors $p' \cap A$ contient q, donc est un idéal maximal de A, et par suite p' est maximal (même référence).

L'étude des anneaux semi-locaux, au moins lorsqu'ils sont complets, se ramène immédiatement à celle des anneaux locaux :

Théorème 3.- Soient A un anneau semi-local, m_i $(1 \leq i \leq k)$ ses divers idéaux maximaux ; on a un isomorphisme canonique

$$\hat{A} = \prod_{i=1}^{i=k} \hat{A}_{m_i} .$$

(On munit évidemment A de la topologie $r(A)$-adique, et chaque A_m de la topologie $r(A_m)$-adique).

Considérons les homomorphismes canoniques

$$\varepsilon_i : A \longrightarrow A_{m_i} = A_i$$

et l'homomorphisme

$$\varepsilon : A \longrightarrow \prod A_i = B$$

qui s'en déduit. L'homomorphisme ε est injectif ; en effet, si $\varepsilon(x) = 0$, il existe pour tout i un $s_i \in A - m_i$ tel que $s_i x = 0$; l'idéal a des s tels que $sx = 0$ n'est donc contenu dans aucun idéal maximal de A, donc contient 1, ce qui prouve que $x = 0$ (on notera que ce raisonnement ne suppose pas les idéaux maximaux en nombre fini). D'autre part, comme les idéaux maximaux m_i sont deux à deux distincts, et en nombre fini, on voit facilement (généralisation du théorème chinois) que pour tout entier n l'application

$$A \longrightarrow \prod A_i/r(A_i)^n$$

est surjective, ce qui prouve que $\varepsilon(A)$ est partout dense dans B. Il reste

donc à prouver que la topologie de A est induite par celle de B (en convenant d'identifier A à son image dans B) . Or il est évident que $\underline{r}(B) = B.\underline{r}(A)$, donc que $\underline{r}(B)^n = B.\underline{r}(A)^n$ pour tout n ; reste donc à prouver que

$$B.\underline{r}(A)^n \cap A = \underline{r}(A)^n \quad ;$$

or on sait que le passage à un anneau de fractions définit sur la catégorie des A-modules un foncteur exact ; si donc $\underline{a}$ est un idéal quelconque de A , $B \underset{A}{\otimes} \underline{a}$ s'identifie à son image dans $B \underset{A}{\otimes} A = B$, i.e. à $B.\underline{a}$; et pour la même raison les relations

$$\underline{a}' \subset \underline{a}'' \quad , \ \underline{a}' \neq \underline{a}'' \quad \text{impliquent} \quad B.\underline{a}' \neq B.\underline{a}'' \quad ;$$

prenant $\underline{a}'' = B.\underline{a}' \cap A$ on déduit de là que

$$B.\underline{a} \cap A = \underline{a}$$

pour tout idéal $\underline{a}$ de A , ce qui achève la démonstration.

4.- Anneaux complets noethériens.

Soient A un anneau filtré par des idéaux $\underline{m}_p$, et E un A-module filtré par des sous-modules E_q ; on suppose que

$$\underline{m}_p.E_q \subset E_{p+q} \quad ,$$

de sorte que

$$G(E) = \sum E_q/E_{q+1}$$

est un module gradué sur l'anneau gradué

$$G(A) = \sum \underline{m}_p/\underline{m}_{p+1} \quad .$$

Pour tout $x \in E$ non nul, il existe un entier n tel que

$$x \in E_n \quad , \quad x \notin E_{n+1} \quad ;$$

l'image $g(x)$ de x dans E_n/E_{n+1} s'appelle la forme initiale de x .

Lemme : Supposons A complet et E séparé ; si des $x_i \in E$ $(1 \leq i \leq n)$ sont tels que leurs formes initiales engendrent le $G(A)$-module $G(E)$, alors les x_i engendrent le A-module E .

Soit p_i le degré de $g(x_i)$, et considérons le A-module $F = A^n$, filtré par les

$$F_p = \underline{m}_{p-p_1} \times \ldots \times \underline{m}_{p-p_n} \quad ;$$

comme A est complet il est immédiat que F lui-même est complet.

Considérons l'homomorphisme $f : F \longrightarrow E$ donné par

$$f((a_i)) = \sum a_i x_i \quad ;$$

l'homomorphisme correspondant

$$\bar{f} : G(F) \longrightarrow G(E)$$

est surjectif d'après l'hypothèse faite ; on va en déduire que f est lui-même surjectif, ce qui démontrera le lemme.

Soit en effet $x \in E_p$; puisque $\bar{f}$ est surjectif il existe $y_p \in F_p$ tel que

$$x \equiv f(y_p) \mod. E_{p+1} \quad ;$$

plus généralement il est clair par récurrence que pour tout $q \geq p$ on a une relation

$$x \equiv f(y_p + \ldots + y_q) \mod. E_{q+1}$$

avec des $y_r \in F_r$. Puisque F est complet, la série $\sum y_r$ converge vers un $y \in F$ et l'on a évidemment $x \equiv f(y) \mod. E_{q+1}$ pour tout $q \geq p$ ce qui prouve que $x = f(y)$ puisque E est séparé ; d'où le lemme.

Théorème 4.- Soit A un anneau filtré par des idéaux $\mathfrak{m}_p$; supposons A séparé et complet, et l'anneau G(A) noethérien ; alors A est noethérien.

Soit en effet $\mathfrak{a}$ un idéal de A, et filtrons-le par les $\mathfrak{a} \cap \mathfrak{m}_n$; on obtient un A-module séparé ; d'autre part, $G(\mathfrak{a})$ est un idéal (homogène) de G(A), et comme G(A) est noethérien on voit que $G(\mathfrak{a})$ admet un système fini de générateurs ; le Théorème 4 résulte donc du Lemme précédent.

Corollaire 1 : Soit A un anneau noethérien ; l'anneau de séries formelles A [[X]] est noethérien.

Il suffit de le filtrer par les puissances de l'idéal formé des séries sans terme constant.

Corollaire 2 : Soit (A , m) un anneau de Zariski ; alors $(\hat{A}, \hat{\mathfrak{m}})$ est un anneau de Zariski.

En effet, $\hat{A}$ est séparé et complet (noter que la topologie $\hat{\mathfrak{m}}$-adique se déduit par complétion de la topologie $\mathfrak{m}$-adique de A), et $G(\hat{A}) = G(A)$ est noethérien puisque quotient d'un anneau de polynomes sur l'anneau noethérien

$A/\underline{m}$; il s'ensuit que $\hat{A}$ est noethérien ; de plus, pour $m \in \underline{m}$, on a

$$(1-m)^{-1} = \sum m^k$$

(série convergente puisque $\hat{A}$ est complet), ce qui prouve que $\hat{\underline{m}}$ est contenu dans le radical de $\hat{A}$.

5.- Le théorème de Cohen.

Soit M un anneau local ; supposons le corps

$$L = M/\underline{r}(M)$$

de caractéristique p ; on dira qu'on est dans le cas d'égales caractéristiques si l'on a $px = 0$ pour tout $x \in M$. Par ailleurs on appelle corps de Cohen de M tout sous-corps R de M tel que l'homomorphisme canonique $R \longrightarrow L$ soit bijectif ; un tel corps ne peut exister que dans le cas d'égales caractéristiques. Pour vérifier qu'un sous-anneau R de M est un corps de Cohen, il suffit évidemment de vérifier que R s'applique sur L et que $R \cap \underline{r}(M) = 0$.

Théorème 5.- Soit M un anneau local séparé et complet pour la topologie $\underline{r}(M)$-adique, ayant même caractéristique que son corps de restes $L = M/\underline{r}(M)$; alors M possède au moins un corps de Cohen. De plus soit K un sous-corps de M , tel que L soit extension séparable de K ; alors M possède un corps de Cohen contenant K .

Démontrons d'abord le théorème en caractéristique $p \neq 0$ (la démonstration qui suit, beaucoup plus simple que celle de Cohen, est due à M. Narita).

Soit $(\xi_i)_{i \in I}$ une p-base de L (Exposé 13, Proposition 4) : les différentielles $d\xi_i$ forment une base de D(L) , ou, ce qui revient au même, les monômes

$$\xi^{\alpha} = \prod \xi_i^{\alpha_i} \qquad (0 \leqslant \alpha_i < p)$$

forment une base de L sur L^p . Il est clair que pour tout k , les $\xi_i^{p^k}$ forment une p-base de L^{p^k} ; on en déduit que pour tout k les monômes $\prod \xi_i^{\alpha_i}$, où $0 \leqslant \alpha_i < p^k$, forment une base de L sur L^{p^k} .

Choisissons dans M des représentants x_i des ξ_i , et considérons les sous-anneaux

$$R_k = M^{p^k}[(x_i)_{i \in I}] \quad ;$$

on note bien entendu M^{p^k} l'image de M par l'homomorphisme $x \longrightarrow x^{p^k}$.

L'homomorphisme $R_k \longrightarrow L$ est <u>surjectif</u>, car l'image de R_k contient L^{p^k} et les ξ_i. D'autre part, on a

$$R_k \cap \underline{r}(M) \subset \underline{r}(M)^{p^k} \quad ;$$

en effet tout $x \in R_k$ est de la forme

$$x = \sum c_\alpha^{p^k} . x^\alpha$$

avec des $c_\alpha \in M$, et où les monômes x^α sont a priori arbitraires, mais peuvent, comme il est immédiat de le vérifier, être soumis à la condition $0 \leqslant \alpha_i < p^k$ pour tout i ; comme les ξ^α correspondants sont linéairement indépendants sur L^{p^k}, on voit que $x \in \underline{r}(M)$ implique $c_\alpha \in \underline{r}(M)$, d'où le résultat. Enfin, il est clair que les R_k vont en décroissant.

Cela dit, nous allons montrer que le sous-anneau

$$R = \bigcap (R_k + \underline{r}(M)^{p^k})$$

est un corps de Cohen de M. On a en effet tout d'abord

$$R \cap \underline{r}(M) = \bigcap (R_k \cap \underline{r}(M) + \underline{r}(M)^{p^k}) = \bigcap \underline{r}(M)^{p^k} = 0 \quad ,$$

puisque M est supposé <u>séparé</u>. D'autre part, pour tout $x \in M$ il existe des $x_k \in R_k$ tels que l'on ait $x \equiv x_k$ mod. $\underline{r}(M)$; pour $h > k$ on a $x_k - x_h \in R_k \cap \underline{r}(M) \subset \underline{r}(M)^{p^k}$; comme M est <u>complet</u> la suite (x_k) converge vers un $y \in M$, et l'on a $y \equiv x_k$ mod. $\underline{r}(M)^{p^k}$ pour tout k ; cela prouve d'une part que $y \in R$, d'autre part que $x \equiv y$ mod. $\underline{r}(M)$; donc $R \longrightarrow L$ est surjectif, ce qui démontre notre assertion.

Si de plus on a déjà "relevé" à M un sous-corps K de L, et si L est séparable sur K, on peut supposer que parmi les ξ_i figure une p-base de K, et choisir les x_i correspondants dans K ; alors on a $R \supset K$. En effet supposons que des $x_i \in K$ $(i \in J)$ forment une p-base de K ; pour tout k, les monômes $\prod x_i^{\alpha_i}$ $(0 \leqslant \alpha_i < p^k)$ forment une base de K sur K^{p^k} ; on a donc

$$K = K^{p^k}[(x_i)_{i \in J}]$$

et a fortiori $K \subset R_k$, d'où évidemment le résultat.

Faisons maintenant la démonstration <u>en caractéristique</u> 0 ; nous allons voir que <u>tout sous-corps maximal</u> R <u>de</u> M <u>est alors un corps de Cohen de</u> M ;

il suffit évidemment de démontrer que R s'applique sur L . Or, L est algébrique sur R (car dans le cas contraire on pourrait adjoindre un élément transcendant à R). Soient alors $\xi \in L$, et considérons un polynome unitaire $f(X)$, à coefficients dans R , tel que le polynome $\bar{f}$ obtenu par réduction mod. $\underline{r}(M)$ des coefficients de f soit le polynome minimal de ξ sur R . Comme on est en caractéristique 0 , ξ est racine simple de $\bar{f}$ et bien évidemment tout revient à montrer que f admet une racine dans M . Or cela résulte du classique

Lemme de Hensel : Soient M un anneau local séparé et complet, f un polynome unitaire à coefficients dans M , et

$$\bar{f}(X) = \varphi(X)\ \psi(X)$$

une décomposition de $\bar{f}$ en deux polynomes étrangers à coefficients dans $L = M/\underline{r}(M)$, de degrés p et q . Il existe alors des polynomes unitaires g et h , à coefficients dans M , de degrés p et q , tels que l'on ait

$$f(X) = g(X)h(X) \quad , \quad \bar{g}(X) = \varphi(X) \quad , \quad \bar{h}(X) = \psi(X) \quad .$$

Pour démontrer le lemme, choisissons des polynomes g_1 et h_1 à coefficients dans M , de degrés p et q , et tels que l'on ait

$$\bar{g}_1 = \varphi \quad , \quad \bar{h}_1 = \psi \quad .$$

On va construire par récurrence sur k des polynomes g_k et h_k à coefficients dans M , de degrés p et q au plus, et tels que l'on ait

$$g_k \equiv g_{k-1} \quad \text{mod. } \underline{r}(M)^{k-1}$$
$$h_k \equiv h_{k-1} \quad \text{mod. } \underline{r}(M)^{k-1}$$
$$f \equiv g_k h_k \quad \text{mod. } \underline{r}(M)^{k} \quad ;$$

pour $k = 1$ la construction est déjà faite ; supposons-la effectuée jusqu'à k ; on aura alors une relation

$$f = g_k h_k + \sum m_j p_j \quad ,$$

où les p_j sont des polynomes à coefficients dans M , de degré $\leqslant p+q$, et où les m_j sont dans $\underline{r}(M)^k$. Or comme φ et ψ sont premiers entre eux il existe (Bezout) des polynomes u_j , v_j à coefficients dans M tels que l'on ait

$$\bar{p}_j = \bar{v}_j \varphi + \bar{u}_j \psi \quad ;$$

on peut même évidemment supposer les u_j de degré $\leqslant p$ et les v_j de degré $\leqslant q$; cela dit, il est clair qu'en posant

$$g_{k+1} = g_k + \sum m_j u_j \quad , \quad h_{k+1} = h_k + \sum m_j v_j$$

on parvient à résoudre les conditions posées pour $k+1$.

Cela dit, M étant complet, les suites g_k et h_k convergent vers des polynomes g et h de degrés $\leq p$ et q , qui évidemment vérifient $\bar{g} = \varphi$, $\bar{h} = \psi$; de plus la relation $f \equiv g_k h_k$ mod. $\underline{r}(M)^k$ donne à la limite $f = gh$ puisque M est séparé. Comme enfin f , φ et ψ sont unitaires, les coefficients dominants de g et h sont inversibles et peuvent être remplacés par 1 , d'où le résultat.

Remarque : En caractéristique 0 il y a en général une infinité de corps de Cohen (on peut "relever" arbitrairement des éléments de L , pourvu qu'ils soient algébriquement indépendants sur le corps des rationnels). Par contre en caractéristique $p \neq 0$ il peut arriver qu'il n'existe qu'un seul corps de Cohen, par exemple si L est parfait $(L = L^p)$; dans ce cas en effet la démonstration prouve que

$$R = \bigcap (M^{p^k} + \underline{r}(M)^{p^k})$$

est un corps de Cohen (on aura soin de distinguer les deux significations de l'exposant p^k dans la relation précédente ...) ; mais tout corps de Cohen R vérifie nécessairement $R = R^{p^k}$, donc est contenu dans $\bigcap M^{p^k}$; comme deux corps de Cohen emboîtés sont identiques, on voit que dans ce cas le seul corps de Cohen de M est

$$R = \bigcap M^{p^k} \quad ,$$

i.e. l'ensemble des $x \in M$ qui, quel que soit k , admettent dans M une racine p^k-ième.

APPENDICE

ayant pour but de mettre en rapport le critère de Zariski, le théorème de Cohen, et le prolongement des dérivations dans les corps.

Soit M un anneau local, de corps des restes $L = M/\underline{r}(M)$; on a établi (Exposé 17, Théorème 5) l'existence d'une suite exacte

$$(1) \qquad 0 \longrightarrow G_1(M) \longrightarrow L \otimes D(M) \longrightarrow D(L) \longrightarrow 0 \quad ;$$

la démonstration, comme on le remarquera, consiste purement et simplement à remplacer M par $M' = M/\underline{r}(M)^2$ et à démontrer le théorème de Cohen pour M' (qui est complet et séparé, et pour cause ...).

Lorsque M est une localité pure sur un corps K le résultat précédent permet, comme on va le voir, de donner une nouvelle démonstration d'un théorème

sur le prolongement des dérivations dans les corps, à savoir : soit r le degré de transcendance de L sur K, et formons la suite exacte

$$0 \longrightarrow N_{K,L} \longrightarrow L \underset{K}{\otimes} D(K) \longrightarrow D(L) \longrightarrow D_K(L) \longrightarrow 0$$

(Exposé 13, page 06) ; alors on a

$$(3) \qquad [D_K(L) : L] - [N_{K,L} : L] = r \quad .$$

Pour établir ce résultat, on écrit $L = M/\underline{r}(M)$ où M est une localité pure sur K (ce qui est toujours possible), et on va appliquer la suite exacte (1), en tenant compte du fait que, M étant simple, on a

$$[G_1(M) : L] = h(M) \quad .$$

Considérons en effet le diagramme commutatif suivant :

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & N_{K,L} & \longrightarrow & L \underset{K}{\otimes} D(K) & \longrightarrow & D(L) & \longrightarrow & D_K(L) & \longrightarrow & 0 \\
 & & & & \uparrow \text{id.} & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & L \underset{K}{\otimes} D(K) & \longrightarrow & L \underset{M}{\otimes} D(M) & \longrightarrow & L \underset{M}{\otimes} D_K(M) & \longrightarrow & 0 \\
 & & & & \uparrow & & & & \\
 & & & & G_1(M) & & & & \\
 & & & & \uparrow & & & & \\
 & & & & 0 & & & &
\end{array}$$

les homomorphismes figurant sur la seconde ligne horizontale sont évidents, et cette ligne est exacte parce que M est une localité <u>pure</u> sur K (de sorte que toute dérivation de K se prolonge à M). De ce diagramme résulte immédiatement une suite exacte

$$(2) \qquad 0 \longrightarrow N_{K,L} \longrightarrow G_1(M) \longrightarrow L \underset{M}{\otimes} D_K(M) \longrightarrow D_K(L) \longrightarrow 0 \quad ;$$

or, supposons que M soit un anneau de fractions d'une algèbre de polynomes à n variables sur K ; évidemment $D_K(M)$ est isomorphe à M^n, donc le troisième terme de (2) est de dimension n ; si le degré de transcendance de L sur K est r, on sait par ailleurs que M est de hauteur $n-r$, en sorte que $G_1(M)$ est de dimension $n-r$; tenant compte de l'exactitude de (2) on trouve bien la relation (3) cherchée.

Bien entendu (3) pourrait inversement servir à établir le critère jacobien pour les localités (mais le théorème de Cohen le donne dans des anneaux locaux beaucoup plus généraux).