Séminaire Henri Cartan

P. Cartier

Dérivations dans les corps

Séminaire Henri Cartan, tome 8 (1955-1956), exp. n° 13, p. 1-13
<http://www.numdam.org/item?id=SHC_1955-1956__8__A13_0>

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

DÉRIVATIONS DANS LES CORPS
(Exposés de P. CARTIER, 13 et 20.2.1956)

1.- Dérivations et différentielles.

Soit A un anneau commutatif avec élément unité noté 1, et M un A-module ; on appelle dérivation de A à valeurs dans M une application $D : A \longrightarrow M$ qui vérifie :

(1) $\quad D(a + a') = D(a) + D(a') \qquad D(aa') = a.D(a') + a'.D(a)$

Si $M = A$, on dira que D est une dérivation de A.

Les formules (1) impliquent que l'on a $D(1) = D(1^2) = 2.D(1)$ donc $D(1) = 0$; puis par récurrence sur $k \geqslant 0$, $D(a^k) = ka^{k-1}.D(a)$, donc $D(a^p) = 0$ en caract. p ; enfin ces formules montrent que l'ensemble des éléments de A annulés par D est un sous-anneau de A.

Si B est un sous-anneau de A, une dérivation D nulle sur B s'appelle une B-dérivation : on a alors $D(ba) = b.D(a)$ puisque $D(b) = 0$ donc D est B-linéaire.

On définit sur $A \otimes_B A$ une structure de A-module par $a(a' \otimes a'') = aa' \otimes a''$, et on désigne par $D_B(A)$ (ou par $D(A)$ si $B = Z$) le quotient de $A \otimes_B A$ par le sous-module R sous-tendu par les éléments $1 \otimes aa' - a \otimes a' - a' \otimes a$; on note da la classe de $1 \otimes a$ mod R. On vérifie immédiatement que la correspondance $h \leftrightarrows h \circ d = D$ établit une correspondance biunivoque entre les homomorphismes h du A-module $D_B(A)$ dans le A-module M, et les dérivations $D = h \circ d$ de A dans M ; $D_B(A)$ s'appelle le module des B-différentielles de A, et da est la différentielle de $a \in A$. En particulier le dual de $D_B(A)$ est l'ensemble des dérivations de A, par $D(x) = \langle dx , D \rangle$.

A étant commutatif, l'application linéaire $P : a \otimes a' \longrightarrow aa'$ est un homomorphisme d'algèbres dont nous appellerons le noyau I ; la restriction de P à la sous-algèbre $A \otimes 1$ est bijective donc $A \otimes A$ est somme directe de I et de $A \otimes 1$, et I est sous-tendu par les éléments $aa' \otimes 1 - a \otimes a' = a(a' \otimes 1 - 1 \otimes a')$. De plus R est engendré par les éléments

$$1 \otimes aa' - a \otimes a' - a' \otimes a = aa' \otimes 1 + (a \otimes 1 - 1 \otimes a)(a' \otimes 1 - 1 \otimes a')$$

donc si $a = a' = 1$, on voit que $R \supset A \otimes 1$ et donc $R = A \otimes 1 + R \cap I$, tandis que $R \cap I$ est engendré comme A-module par les produits de deux éléments de la forme $a \otimes 1 - 1 \otimes a$, soit $R \cap I = I^2$. On a donc démontré que $D(A)$ s'identifie à I/I^2 , da étant la classe de $-a \otimes 1 + 1 \otimes a$ mod. I^2 .

De cette dernière forme, on déduit facilement la détermination des différentielles des polynomes ; soit $A = B[\dots , x_i , \dots]$; $A \otimes A$ est donc isomorphe à l'anneau des polynomes en deux séries de variables x_i et y_i . Posant $y_i = x_i + h_i$, on voit que les x_i et les h_i sont des variables indépendantes, et l'homomorphisme P de $A \otimes A$ dans A envoie x_i sur x_i et h_i sur 0 ; I est donc l'idéal engendré par les h_i , donc se compose des polynomes dont tout monôme $\neq 0$ est de degré $\geqslant 1$ en les h_i , tandis que les polynomes de I^2 sont les polynomes dont tout monôme $\neq 0$ est de degré $\geqslant 2$ en les h_i . Les polynomes homogènes de degré 1 en les h_i forment donc un système de représentants de I modulo I^2 ; or si $a = P(x) \in A$ on a $da = -a \otimes 1 + 1 \otimes a = P(\dots , x_i + h_i , \dots) - P(\dots , x_i , \dots)$, donc da se représente par la composante de degré 1 en les h_i de $P(\dots , x_i + h_i , \dots)$ et par suite $h_i = dx_i$. Ainsi $D(A)$ <u>est un</u> A-<u>module libre ayant pour base les</u> dx_i .

On peut donc poser $dP = \sum_i D_i P . dx_i$ où les $D_i P$ sont des éléments de A bien déterminés dépendant linéairement de dP , donc D_i est une dérivation de A , appelée dérivation partielle en x_i et caractérisée par $D_i x_j = \delta_{ij}$. On pose aussi $D_i P = \frac{\partial P}{\partial x_i} = P'_{x_i}$ et $DP = P'$ dans le cas d'une variable. On a alors $D_i x^\alpha = \alpha_i x^{\alpha - \varepsilon_i}$ ($\varepsilon_i = (0 , 0 , \dots , 1 , \dots)$, 1 à la i-ième place), donc si $dP = 0$ on a $P \in K[x_i^P]$ et réciproquement. De plus si D est une dérivation de B dans un A-module M , on la prolonge en une dérivation de $B[\dots , x_i , \dots]$ en posant

$$(2) \qquad P^D = \sum_\alpha (Da_\alpha)\, x^\alpha \qquad \text{si} \qquad P = \sum_\alpha a_\alpha x^\alpha \ .$$

Soit alors D une dérivation de <u>l'anneau</u> $B[\dots , x_i , \dots] = A$ dans le A-module M , D_o sa restriction à B qui est une dérivation de B dans M . La dérivation $P \longrightarrow D(P) - P^{D_o}$ annule B , donc se prolonge en une application A-linéaire de $D_B(A)$ dans M qui envoie dx_i sur Dx_i donc dP sur $\sum_i D_i P . Dx_i$; finalement, on a :

$$(3) \qquad D(P) = P^{D_o} + \sum_i D_i P . Dx_i \ .$$

Inversement, comme $D_B(A)$ admet les dx_i pour base, pour toute famille d'éléments $m_i \in M$, il existe une application linéaire de $D_B(A)$ dans M qui envoie dx_i sur m_i, et une seule ; en résumé :

Proposition 1.- Soit D_o une dérivation de B dans le A-module M, où $A = B[\ldots, x_i, \ldots]$, et soit $\{m_i\}$ une famille d'éléments de M ; il existe une dérivation D de A dans M est une seule qui envoie x_i sur m_i et prolonge D_o ; elle est donnée par la formule :

$$(4) \qquad D(P) = P^{D_o} + \sum_i D_i P . m_i \ .$$

2.- Prolongement des dérivations : critère de Weil.

Nous allons maintenant nous occuper du problème suivant : A étant une K-algèbre et B une sous-algèbre de A, à quelle conditions peut-on prolonger une dérivation de B dans un A-module M (M est donc aussi un B-module) en une dérivation de A dans M ?

La réponse est fournie par le critère suivant, dû à Weil :

Proposition 2.- Supposons que A soit engendrée sur B par une partie S donc $A = B[S]$; soit $\{f_\lambda\}$ une base de l'idéal des relations algébriques entre les $s \in S$, $D : B \to M$ une dérivation et $(m_s)_{s \in S}$ des éléments de M. Pour que D se prolonge en une dérivation $\bar{D}$ de A dans M telle que $\bar{D}_s = m_s$, il faut et il suffit que l'on ait :

$$(5) \qquad f_\lambda^D(\ldots, s, \ldots) + \sum_s (D_s f_\lambda)(\ldots, s, \ldots)\, m_s = 0 \quad \text{pour tout } \lambda \ .$$

Soit A' l'anneau des polynomes à coefficients dans B en des variables X_s ($s \in S$) ; le noyau de l'homomorphisme φ de A' sur A qui envoie X_s sur s donc f sur $f(\ldots, s, \ldots)$ est l'idéal I engendré par les f_λ. Si M est un A-module, c'est aussi un A'-module par $a'.m = \varphi(a').m$; d'après le paragraphe 1.- , la dérivation D de B dans M se prolonge d'une seule manière en une dérivation D' de A' dans M qui envoie X_s sur m_s. La formule (5) signifie que $D'(f_\lambda) = 0$ d'après la formule (4) ; soit alors $a' = \sum_\lambda a'_\lambda f_\lambda \in I$, on aura :

$$(6) \qquad D'(a') = \sum_\lambda \varphi(a'_\lambda).D'(f_\lambda) + \sum_\lambda \varphi(f_\lambda).D'(a'_\lambda) = 0 \ .$$

D' s'annulant sur I, passe au quotient et définit une dérivation $\bar{D}$ de A dans M, comme on le vérifie sur la formule (1).

Inversement, si $\bar{D} : A \to M$ prolonge D et envoie $s \to m_s$, alors $D' = \bar{D} \circ \varphi$ est une dérivation de A' dans M qui s'annule sur les f_λ, d'où la formule (5).

Corollaire : Si A est un anneau d'intégrité, toute dérivation définie sur A se prolonge de manière unique à son corps des fractions K (si elle prend ses valeurs dans un espace vectoriel sur K)

Soit f l'homomorphisme de $A' = A[\ldots, X_b, \ldots]_{b \in A^*}$ dans K qui envoie X_b sur b^{-1} ; soit I le noyau de f ; f contient les polynomes $bX_b - 1$ qui engendrent un idéal $I_1 \subset I$; or b est inversible modulo I_1, donc A'/I_1 est engendré par les classes des éléments de $A \subset A'$ et les inverses de ces éléments qui sont $\neq 0$, d'où résulte immédiatement que A'/I_1 est un corps, donc que I_1 est maximal et $I = I_1$. Par suite, pour trouver une dérivation $\bar{D}$ prolongeant D et appliquant b^{-1} sur m_b, il est nécessaire et suffisant de résoudre les équations :

$$D(b)b^{-1} + b.m_b = 0 \quad , \tag{7}$$

d'où $m_b = - b^{-2}.D(b)$.

3.- Prolongement des dérivations définies dans un corps.

Soit K un corps, D une dérivation définie dans K, et L un surcorps de K. Considérons l'ensemble Φ formé des couples (K', D'), où K' est un corps intermédiaire entre K et L, et D' une dérivation définie sur K' et induisant D sur K. On ordonne Φ "par prolongement" ; comme les identités des dérivations ne font intervenir qu'un nombre fini d'éléments, Φ est inductif, d'où résulte dans tous les cas, par le lemme de Zorn, l'existence d'un prolongement maximal de D. Il nous reste donc à nous occuper des extensions monogènes.

Soit donc x un élément de L qui n'appartient pas à K.

a) x est transcendant sur K : $K[x]$ est alors isomorphe à l'algèbre des polynomes à une variable à coefficients dans K, et $K(x)$ est le corps des quotients de $K[x]$; l'existence du prolongement de D à $K(x)$ résulte alors de la proposition 1 et du corollaire de la proposition 2. De plus on peut choisir $\bar{D}(x)$ arbitrairement.

b) x est algébrique sur K : supposons d'abord que x soit "séparable", i.e. racine simple d'un polynome $F(X)$, donc a fortiori racine simple de son polynome minimal $H(X)$: on a donc $F(X) = (X-x)G(X)$ avec $G(x) \neq 0$. Or en

dérivant, on trouve $F'(x) = G(x)$, et de même $H'(x) \neq 0$. Comme H engendre l'idéal des relations satisfaites par x , on peut appliquer la proposition 2 qui montre que le prolongement de D à $K[x] = K(x)$ existe et est unique, et que l'on a $H^D(x) + H'(x).\bar{D}(x) = 0$.

c) x <u>est algébrique inséparable sur</u> K : on a donc $G'(x) = 0$, et comme $\deg G' < \deg G$, ceci implique $G'(X) = 0$; or, cela n'est pas possible en caractéristique 0 , et en caract. $p \neq 0$, cela implique que $G(X) = G_1(X^p)$. La proposition 2 montre que le prolongement n'est possible que si $G^D(x) = 0$ et que dans ce cas $\bar{D}(x)$ peut être choisi arbitrairement. Supposons par exemple que $x \notin K$, mais $x^p = u \in K$; le lemme qui suit montre que le polynome minimal de x est $X^p - u$, donc D ne se prolonge à $K(x)$ que si $D(u) = 0$ et alors on peut choisir $\bar{D}(x) \neq 0$.

<u>Lemme</u> : <u>Si</u> $F(X)$ <u>est un polynome unitaire irréductible sur le corps</u> K <u>de caract.</u> $p \neq 0$, <u>alors</u> $F(X^p)$ <u>est irréductible ou une puissance d'exposant</u> p^e <u>d'un polynome irréductible</u>.

Soit G irréductible, et $F(X^p) = G(X)^e H(X)$, où G ne divise pas H ; dérivant et divisant par $G(X)^{e-1}$, on trouve $eG'H + GH' = 0$, donc G divise $eG'H$ et par suite il divise eG' puisqu'il ne divise pas H ; pour raison de degré on a donc $eG' = 0$; donc e est divisible par p , ou $G' = 0$; d'où $G(X) = G_1(X^p)$. La décomposition de $F(X^p)$ en facteurs irréductibles est donc $\prod_i G_i(X^p) \prod_j H_j(X)^{pf_j}$; mais comme H_j^p est un polynome en X^p et que $F(X)$ est irréductible, on voit que $F(X^p)$ est irréductible, ou que $F(X^p) = H(X)^p$, avec H irréductible.

Ainsi $X^p - u$ est irréductible, ou $X^p - u = (X - a)^p$ donc $x^p = a^p = u$ soit $x \in K$, ce qui est contradictoire.

Voici maintenant la réponse au problème de prolongement dans le cas des corps.

<u>Théorème 1.- Soit</u> K <u>un corps</u>, D <u>une dérivation définie dans</u> K <u>à valeurs dans un espace vectoriel</u> V <u>sur un surcorps</u> L <u>de</u> K .

1) <u>Si</u> K <u>est de caractéristique</u> 0 , D <u>se prolonge à</u> L , <u>et ceci de manière que si</u> $x \in L$ <u>transcendant sur</u> K <u>est fixé, on ait</u> $\bar{D}(x) \neq 0$.

2) <u>Si</u> K <u>est de caractéristique</u> $p \neq 0$, <u>et si</u> $K \subset L^p$, D <u>se prolonge à</u> L ; <u>si</u> $x \notin K$ <u>est donné, on peut choisir</u> D <u>de sorte que</u> $\bar{D}(x) \neq 0$.

L'étude précédente montre que dans les deux cas précédents, on peut prolonger D à $K(x)$, puisque dans le deuxième qui est seul douteux, on a $D(x^p) = 0$. Puis on choisit un prolongement (K', D') maximal de D. Si on avait $K' \neq L$ et $y \notin K'$, on pourrait prolonger D' à $K'(y) \neq K'$ puisque $D(y^p) = 0$ dans le deuxième cas, ce qui donnerait une contradiction.

Corollaire : l'ensemble des éléments de L annulés par toute K-dérivation de L, est la fermeture algébrique de K dans L si $p = 0$, et $K(L^p)$ si $p \neq 0$.

Nous allons de ce théorème tirer un certain nombre de renseignements sur les différentielles dans un corps. Si K est contenu dans L, on définit un homomorphisme canonique de $D(K)$ dans $D(L)$ en faisant correspondre à $\sum a_i db_i$ (où les a_i et b_i sont considérés comme éléments de K) cette même forme où les éléments sont considérés comme appartenant à L ; comme $D(L)$ est un espace L-vectoriel, on peut prolonger ceci en application L-linéaire $\varphi_{K,L}$ de $L \otimes_K D(K)$ dans $D(L)$ dont nous noterons le noyau $N_{K,L}$. Soit $D_{K,L}$ le conoyau de $\varphi_{K,L}$. On a la suite exacte :

$$(S) \qquad (0) \longrightarrow N_{K,L} \longrightarrow L \otimes_K D(K) \xrightarrow{\varphi_{K,L}} D(L) \longrightarrow D_{K,L} \longrightarrow (0) .$$

Il est clair que $D_{K,L}$ s'identifie au module $D_K(L)$ des K-différentielles de L.

Proposition 3.- Si L/K est une extension de type fini, $N_{K,L}$ et $D_K(L)$ sont de rang fini sur L, et on a :

$$(8) \qquad d_{K,L} = [D_K(L) : L] - [N_{K,L} : L] = \deg.\mathrm{tr}._K L$$

Soient V et W deux espaces vectoriels sur un corps K, et f une application linéaire de V dans W ; le noyau de f est l'espace $N = f^{-1}(0) \subset V$ et le conoyau de f est l'espace $C = W/f(V)$. Si N et C sont de rang fini sur K et dans ce cas seulement, on définira le "défaut" de f comme le nombre $\delta(f) = [C : K] - [N : K]$ qui a les propriétés suivantes :

a) $\delta(f)$ est invariant par extension des scalaires.

b) si $\delta(f)$ et $\delta(g)$ sont définis, il en est de même de $\delta(g \circ f)$ qui est égal à $\delta(f) + \delta(g)$.

Soient $f : V \longrightarrow W$, $g : W \longrightarrow T$ deux applications linéaires, $h : V \longrightarrow T$ leur composée ; nous appellerons respectivement N, N', N'' les noyaux de f, g, h et C, C', C'' les conoyaux des mêmes ; comme $f(x) = 0$ implique $h(x) = 0$, on voit que $N \subset N''$; comme $h(x) = g(f(x))$, on voit de

même que $f(N'') = f(V) \cap N'$; l'application canonique π de W sur $C = W/f(V)$ induit une application π' de N' dans C dont le noyau est $f(V) \cap N'$; g définit par passage au quotient une application $\bar{g}$ de $C = W/f(V)$ dans $C'' = T/h(V)$ dont le noyau est évidemment $N'/f(V) = \pi'(N')$; enfin l'application canonique ρ de $C'' = T/h(V)$ sur $C' = T/g(W)$ a pour noyau $g(W)/h(V) = \bar{g}(C)$. En résumé, on a démontré que la suite suivante est exacte :

$$(S') \qquad (0) \longrightarrow N \longrightarrow N'' \xrightarrow{f} N' \xrightarrow{\pi'} C \xrightarrow{\bar{g}} C'' \xrightarrow{\rho} C' \longrightarrow (0)$$

Si N et N' sont de dimension finie, il en est donc de même de N'' , et une raison analogue vaut pour C'' , ce qui montre que $\delta(h)$ est défini si $\delta(f)$ et $\delta(g)$ sont définis. De plus, dans la suite exacte (S') , formée d'espaces de dimension finie, la somme alternée des dimensions est nulle, donc :

$$[N : K] - [N'' : K] + [N' : K] - [C : K] + [C'' : K] - [C' : K] = 0$$

ce qui est la relation cherchée.

Ceci étant démontré, soient K , L , M trois corps tels que $K \subset L \subset M$; on a $M \otimes_L (L \otimes_K D(K)) \cong M \otimes_K D(K)$ et par suite $\varphi_{K,M}$ se factorise en $M \otimes_K D(K) \xrightarrow{f} M \otimes_L D(L) \xrightarrow{g} D(M)$; on a $\delta(f) = d_{K,L}$ d'après a) et comme $\delta(g) = d_{L,M}$ on a d'après b) $d_{K,M} = \delta(g \circ f) = d_{K,L} + d_{L,M}$. Comme le degré de transcendance est aussi additif, on peut se contenter de démontrer la formule (8) lorsque $L = K(x)$; si x est transcendant sur K , on a $N_{K,L} = (0)$, $[D_K(L) : L] = 1$ et $\deg.tr._K L = 1$, d'où la formule dans ce cas. Si x est algébrique de polynome minimal $G(X)$, on a $dG \neq 0$ dans $D(K(X))$ sinon d'après le corollaire du théorème 1, G serait puissance p^e d'un élément de $K(X)$ donc non irréductible, et par suite $dG \neq 0$ dans $D(K[X])$. Comme $K(x) \cong K[X]/(G)$, L est algèbre sur $K[X]$ et on voit tout de suite que $\varphi_{K,L}$ se factorise en $L \otimes D(K) \xrightarrow{f} L \otimes_{K[X]} D(K[X]) \xrightarrow{g} D(L)$ et $d_{K,L} = \delta(f) + \delta(g) = 1 + (-1)$ car l'espace intermédiaire est isomorphe à $L \otimes_K D(K) \oplus D_K(L)$ donc f est injective, et le noyau de g est engendré par $1 \otimes dG$ d'après la proposition 2 .

Avant de démontrer la proposition suivante, remarquons que l'indépendance linéaire sur L des différentielles $dx_i \in D_K(L)$ signifie qu'il existe une K-dérivation à valeurs dans un espace L-vectoriel prenant des valeurs arbitrairement données en les éléments x_i , ou encore que pour tout i , il existe une K-dérivation D_i de L dans L nulle sur les x_j pour $j \neq i$, mais non nulle sur x_i .

Proposition 4.- Pour que les différentielles dx_i soient linéairement indépendantes dans l'espace L-vectoriel $D_K(L)$, il faut et il suffit :

1) si K est de caractéristique 0 , que les x_i soient algébriquement indépendants ; si de plus les dx_i forment une base de $D_K(L)$, les x_i forment une base de transcendance de L sur K .

2) si K est de caractéristique $p \neq 0$, que les monômes $x^\alpha = \prod_i x_i^{\alpha_i}$ soient linéairement indépendants sur le corps $K(L^p)$ pour $0 \leqslant \alpha_i < p$; si les dx_i forment une base de $D_K(L)$, les x^α forment une base de L sur $K(L^p)$ ("p-base") .

En effet, dire que les dx_i sont linéairement indépendantes signifie, dans le cas de caractéristique 0 , d'après le corollaire du théorème 1 et les remarques ci-dessus, que x_i n'est jamais algébrique sur $K(x_j)_{j \neq i}$, i.e. que les x_i sont algébriquement indépendants; et, dans le cas de caractéristique $p \neq 0$, que pour aucun i on n'a $x_i \in K(L^p , x_j)_{j \neq i} = M_i$ ou encore que les monômes $x_i^{\alpha_i}$ $(0 \leqslant \alpha_i < p)$ sont linéairement indépendants sur M_i pour tout i ; ceci équivaut à dire que ces x^α sont linéairement indépendants sur $K(L^p)$ puisque ces monômes sous-tendent L . De plus, si les dx_i forment une base de $D_K(L)$ toute dérivation définie dans L nulle sur K et les x_i est identiquement nulle, ce qui par le corollaire du théorème 1 signifie que L est algébrique sur $K(x_i)_{i \in I}$, ou que $L = K(L^p , x_i)_{i \in I}$ suivant la caractéristique.

Ceci démontre évidemment la proposition.

4.- Extensions séparables des corps commutatifs.

Nous dirons que l'extension L/K est séparable, si toute dérivation $D : K \longrightarrow V$, où V est un espace L-vectoriel se prolonge en une dérivation définie dans L .

D définit une application K-linéaire de D(K) dans V , donc une application L-linéaire de $L \otimes_K D(K)$ dans V ; pour que D puisse se prolonger à L , il faut et il suffit que l'on puisse factoriser $L \otimes D(K) \longrightarrow D(L) \longrightarrow V$; si ceci est requis pour toute dérivation D , ceci équivaut à dire que $N_{K,L} = (0)$.

De la définition résulte sans plus que si L/K et M/L sont séparables, il en est de même de M/K , et que si $L \supset L' \supset K$ et si L/K est séparable, il en est de même de L'/K .

Proposition 5 : a) toute extension transcendante pure est séparable ;

b) si K est de caractéristique 0 , ou si $K = K^p$, toute extension L de K est séparable ;

c) pour que $L = K(x)$ soit séparable, il faut et il suffit que x soit transcendant ou algébrique séparable ;

d) pour que l'extension algébrique $L = K[S]$ soit séparable, il faut et il suffit que tous les éléments de S soient séparables sur K .

a) résulte de la proposition 1 et du corollaire de la proposition 2 .

b) résulte du 1) du théorème 1 si $p = 0$; sinon il résulte du fait que $D(K) = (0)$ si $K = K^p$, puisque $D(x^p) = 0$.

c) Si x est transcendant sur K , $K(x)$ est séparable sur K par a) ; si x est algébrique, la formule (8) donne $[N_{K,L} : L] = [D_K(L) : L]$, donc la séparabilité de L/K signifie que toute K-dérivation de $K(x)$ est nulle, i.e. d'après le paragraphe 3, que x est séparable sur K .

d) Si $L = K[S]$ est séparable sur K , il en est de même de $K(x)/K$ pour $x \in S$, donc tous les éléments de S sont séparables sur K , d'après c); inversement si tous les $x \in S$ sont séparables sur K , ils le sont a fortiori sur $K' \supset K$, et par suite si S est fini, toute dérivation D de K se prolonge en $\bar{D}$ à $K[S]$ comme on le montre par récurrence sur le nombre d'éléments de S ; un tel prolongement est unique puisque les $\bar{D}(x)$ sont bien déterminés pour $x \in S$ (cf. paragraphe 3). Enfin si S est infini, D se prolonge avec unicité à tous les sous-corps $K[S']$ de L ($S' \subset S$ fini), d'où l'existence et l'unicité du prolongement à L .

Dans le cas des extensions de type fini, la proposition 3 donne des renseignements précis :

Théorème 2.- Pour que l'extension $L = K(x_1 , \dots , x_n)$ de dimension algébrique r soit séparable, il faut et il suffit que $[D_K(L) : L] \leq r$, et dans ces conditions, il y a même égalité. Pour que L/K soit séparable, il faut et il suffit également que L soit extension algébrique séparable d'une extension transcendante pure $K(B)$ de K , ayant B comme base de transcendance ; une telle base B est caractérisée par le fait que les dy ($y \in B$) forment une base de $D_K(L)$, ce qui permet de choisir B parmi les x_i .

D'après la proposition $N_{K,L} = (0)$ équivaut bien à $[D_K(L) : L] \leq r$ et implique l'égalité dans cette formule. D'après la proposition 5, a), d), toute extension algébrique séparable d'une extension transcendante pure est séparable ; réciproquement soit B une partie de L telle que les dy pour $y \in B$ forment une base de $D_K(L)$; toute dérivation de L nulle sur $K(B)$ est alors

nulle i.e. $D_{K(B)}(L) = (0)$, donc par le début de la démonstration L est séparable sur K(B) et de plus algébrique. Enfin si B est une base de transcendance de L sur K telle que L soit algébrique séparable sur K(B) , on a $D_{K(B)}(L) = (0)$, donc les différentielles des éléments de K(B) engendrent $D_K(L)$ par la suite exacte (S) , et a fortiori les dy $(y \in B)$ engendrent $D_K(L)$. Comme B possède $r = [D_K(L) : L]$ éléments, les dy $(y \in B)$ forment une base de $D_K(L)$.

Corollaire : pour qu'une extension L/K de type fini soit algébrique séparable, il faut et il suffit que toute dérivation de L nulle sur K soit identiquement nulle.

Si L/K n'est pas de type fini, on a le contre-exemple suivant : $L = K^p$, donc si $K \neq K^p$, $D(K) \neq (0)$ et $D(L) = (0)$.

Nous allons maintenant donner un certain nombre de formes équivalentes de la notion de séparabilité :

Théorème 3.- Pour que l'extension L/K soit séparable, il faut et il suffit que l'une des conditions suivantes soit vérifiée :

1) Pour toute extension M de K , l'algèbre $L \otimes_K M$ est sans radical ;

2) Pour toute extension M de K , l'algèbre $L \otimes_K M$ n'a pas d'élément nilpotent non nul ;

3) $p = 0$, ou bien pour toute famille d'éléments x_i linéairement indépendants sur K , les x_i^p sont linéairement indépendants sur K ;

4) si $K \subset L \subset \Omega$, Ω étant algébriquement clos, L est linéairement disjoint du sous-corps Ω_0 des invariants du groupe de tous les K-automorphismes de Ω ;

5) si Ω est un surcorps algébriquement clos de K contenant un sous-corps isomorphe à L , et si pour tout K-homomorphisme f de L dans Ω , on définit $f' : \Omega \otimes_K L \longrightarrow \Omega$ par $f'(\omega \otimes x) = \omega f(x)$, il n'y a aucun élément non nul de $\Omega \otimes_K L$ annulé par tous les homomorphismes f' ;

6) Ω étant comme en 5), si les éléments $x_1 , \ldots , x_n \in L$ sont linéairement indépendants sur K , il existe des homomorphismes $f_1 , \ldots , f_n : L \longrightarrow \Omega$ tels que $\det (f_i(x_j)) \neq 0$.

On rappelle que le radical $r(A)$ d'une algèbre A est l'intersection de ses idéaux maximaux.

1) $\Longrightarrow$ 2) car un élément nilpotent appartient à tout idéal maximal donc au radical.

2) $\Longrightarrow$ 3) supposons que l'on ait une relation $\sum_i a_i x_i^p = 0$ et soit $M = K(\dots , a_i^{1/p} , \dots)$; comme les x_i sont linéairement indépendants, on a $y = \sum_i x_i \otimes a_i^{1/p} \in L \otimes M$ non nul si les a_i ne sont pas tous nuls, mais $y^p = \sum_i x_i^p \otimes a_i = \sum_i a_i x_i^p \otimes 1 = 0$, ce qui contredit 2) .

3) $\Longrightarrow$ 4) il est bien connu que les éléments de Ω qui sont invariants par tout K-automorphisme de Ω sont les éléments algébriques sur K égaux à tous leurs conjugués, donc solutions d'une équation $x^{p^h} - a = 0$ avec $a \in K$ si $p \neq 0$, et sinon $\Omega_o = K$. Soient des $x_i \in L$ linéairement indépendants sur K , donc par récurrence sur h , d'après 3) , les $x_i^{p^h}$ sont linéairement indépendants sur K ; si on a alors $\sum_i a_i x_i = 0$ avec $a_i \in \Omega_o$, on peut trouver un h tel que $a_i^{p^h} \in K$, et par suite $\sum_i a_i^{p^h} x_i^{p^h} = 0$ donc $a_i^{p^h} = 0$ et $a_i = 0$, ce qui prouve que L et Ω_o sont linéairement disjoints sur K .

4) $\Longrightarrow$ 5) soit $y = \sum_{i=1}^{n} \omega_i \otimes x_i \neq 0$ un élément de $\Omega \otimes L$ annulé par tous les f' ; on peut supposer les x_i linéairement indépendants sur K et que n a été choisi le plus petit possible. Après division par ω_n et comme f' est Ω-linéaire, on peut supposer $\omega_n = 1$; on a donc $\sum_{i=1}^{n} \omega_i f(x_i) = 0$ pour tout homomorphisme f de L dans Ω . Remplaçant f par $g^{-1} \circ f$, où g est un automorphisme de Ω , et appliquant g à l'identité obtenue, on trouve $\sum_{i=1}^{n} g(\omega_i) f(x_i) = 0$ d'où $f'(y') = 0$ avec $y' = \sum_{i=1}^{n-1} (g(\omega_i) - \omega_i) \otimes x_i$, ce qui contredit la définition de n si on n'a pas $g(\omega_i) = \omega_i$, i.e. $\omega_i \in \Omega_o$. Mais prenant pour f l'application identique de L dans Ω , on trouverait alors $\sum \omega_i x_i = 0$, ce qui contredit la disjonction linéaire de L et Ω_o .

5) $\Longleftrightarrow$ 6) : si V est un sous-espace de L ayant pour K-base $x_1 , \dots , x_n$, la condition 6) signifie que l'ensemble des restrictions à $\Omega \otimes V$ des formes Ω-linéaires est de rang $n = [\Omega \otimes V : \Omega]$ donc équivaut à dire qu'il n'y a aucun élément de $\Omega \otimes V$ annulé par toutes les formes f' . Comme $\Omega \otimes L$ est réunion des sous-espaces $\Omega \otimes V$, ceci équivaut bien à 5) .

6) $\Longrightarrow$ 1) : prenons pour Ω une clôture algébrique de L , d'où résulte que $\Omega \otimes M$ est entier sur $L \otimes M$; la proposition 7 de l'exposé 1 montre alors

que le radical de $L \otimes M$ est contenu dans le radical de $\Omega \otimes M$; si g est K-automorphisme de Ω , $I \otimes g$ est un automorphisme de l'anneau $\Omega \otimes M$ qui permute donc les idéaux maximaux de $\Omega \otimes M$ et laisse fixe $\underline{r}(\Omega \otimes M)$. Soit alors $x = \sum x_i \otimes m_i$ un élément de $\underline{r}(L \otimes M) \subset \underline{r}(\Omega \otimes M)$, les x_i étant linéairement indépendants ; on peut trouver d'après la condition 6) des isomorphismes $f_i : L \to \Omega$ (qu'on peut prolonger en des automorphismes f_i' de la clôture algébrique Ω de L) et une matrice $\| a_{ij} \|$ à coefficients dans Ω inverse de la matrice $\| f_i(x_j) \|$. On a :

$$\sum_K a_{jk} \cdot (f_k \otimes I)(x) = \sum_{i,k} a_{jk} f_k(x_i) \otimes m_i = m_j \in \underline{r}(\Omega \otimes M) \quad .$$

Comme M est un corps, si on avait $m_i \neq 0$, il serait inversible, ce qui est absurde car le radical d'un anneau est un idéal distinct de cet anneau. Donc $m_i = 0$ pour tout i et $x = 0$, ce qui prouve que $L \otimes M$ est sans radical.

3) équivaut à la séparabilité de L/K ; on peut supposer $p \neq 0$ d'après la proposition 3, b . Il est clair que 3) signifie que L^p et K sont linéairement disjoints sur K^p . S'il en est ainsi, soit D une dérivation définie dans K , donc nulle dans K^p ; puisque $K[L^p] \simeq K \otimes_{K^p} L^p$, D se prolonge de manière unique en une dérivation définie dans $K[L^p]$ nulle sur L^p , donc d'après le corollaire de la proposition 2 et le théorème 1, 2) en une dérivation définie dans L , ce qui prouve que L/K est séparable. Inversement, supposons L/K séparable, et soit $\sum_{i=1}^{n} a_i x_i^p = 0$ une relation linéaire entre les x_i^p : on suppose les x_i linéairement indépendants sur K , n choisi le plus petit possible. Après division par a_n , on se ramène au cas où $a_n = 1$, puis si D est une dérivation de L , on en déduit $\sum_{i=1}^{n-1} D(a_i) x_i^p = 0$ puisque $D(a_n) = D(1) = 0$. D'après la définition de n , on a donc $D(a_i) = 0$, mais comme L/K est séparable, toute dérivation de K est induite par une dérivation de L , donc a_i est annulé par toute dérivation de K ,

ce qui par le théorème 1 prouve que $a_i = b_i^p \in K^p$; on a finalement $\sum_{i=1}^{n} b_i^p x_i^p = 0$ donc $\sum_{i=1}^{n} b_i x_i = 0$ et comme $b_n = 1 \neq 0$, on a une contradiction.

C.Q.F.D.

Complément au théorème 3 : avec les méthodes employées dans la démonstration du théorème 3, on va montrer que, si L et M sont deux extensions de K , le radical de l'anneau $L \otimes_K M$ est composé d'éléments nilpotents. Soit en effet Ω une clôture algébrique de M , Ω_0 l'ensemble des éléments de Ω invariants par tous les K-automorphismes de Ω , i.e. les $x \in \Omega$ tels que pour f assez grand $x^{p^f} \in K$; $L \otimes_K \Omega$ est entier sur $L \otimes_K M$, donc (exposé 1, proposition 7) $\underline{r}(L \otimes M) \subset \underline{r}(L \otimes \Omega)$ et il suffit donc de démontrer que le radical de $L \otimes \Omega$ est composé d'éléments nilpotents. Or un K-automorphisme g de Ω définit un automorphisme $\bar{g}$ de l'anneau $L \otimes \Omega$ par $\bar{g}(x \otimes \omega) = x \otimes g(\omega)$; $\bar{g}$ permute les idéaux maximaux de $L \otimes \Omega$ donc laisse stable son radical. Soit $\{x_i\}$ une base de L sur K , donc $L \otimes \Omega$ admet les $x_i \otimes 1$ comme base sur Ω ; si $x = \sum_i x_i \otimes \omega_i$ est un élément primordial de $\underline{r}(L \otimes \Omega)$ pour cette base, on a $\bar{g}(x) = \sum_i x_i \otimes g(\omega_i) \in \underline{r}(L \otimes \Omega)$, ce qui d'après les propriétés des éléments primordiaux et le fait que $\omega_i = 0$ implique $g(\omega_i) = 0$, montre que x et $\bar{g}(x)$ sont proportionnels (sur Ω) et comme un des ω_i vaut 1 , on a $x = \bar{g}(x)$, soit $\omega_i = g(\omega_i)$ ou encore comme g est arbitraire, $\omega_i \in \Omega_0$. Dans ces conditions, on peut trouver un f tel que ${\omega_i}^{p^f} \in K$, d'où $x^{p^f} = \sum_i x_i^{p^f} \otimes \omega_i^{p^f} = (\sum_i x_i^{p^f} \omega_i^{p^f}) \otimes 1$; x^{p^f} appartient au corps $L \otimes 1$ et n'est pas inversible, puisqu'il est dans le radical de $L \otimes \Omega$; donc il est nul, et x est nilpotent. Comme $\underline{r}(L \otimes \Omega)$ est l'espace vectoriel sur Ω engendré par ses éléments primordiaux, il en résulte, que tous les éléments de ce radical sont nilpotents.

Remarque finale : les critères 3) et 6) du théorème 3 sont évidemment de caractère fini, ce qui prouve que pour qu'une extension L/K soit séparable, il faut et il suffit que toutes les extensions de type fini contenues dans L soient séparables.