Conjeerveram Srirangachari Seshadri

L'opération de Cartier. Applications

Séminaire Claude Chevalley, tome 4 (1958-1959), exp. nº 6, p. 1-26
<http://www.numdam.org/item?id=SCC_1958-1959__4__A6_0>

L'OPÉRATION DE CARTIER. APPLICATIONS

par Conjeerveram Srirangachari SESHADRI.

1. Définition de l'opération de Cartier.

On désigne par K un corps de caracteristique $p > 0$ et par L un sous-corps de K contenant le corps K^p des puissances p-ièmes d'éléments de K et tel que $[K : L]$ soit fini.

On désigne par $\mathfrak{D}(K/L)$, ou simplement $\mathfrak{D}$, l'espace des L-dérivations de K ; c'est un espace vectoriel de dimension finie sur K. On désigne par Ω^1 le dual de $\mathfrak{D}$, par Ω l'algèbre extérieure sur Ω^1 et par Ω^r l'espace des éléments homogènes de degré r de Ω ; les éléments de Ω^1 s'appellent les L-différentielles de K. Si $x \in K$, on note dx l'élément $D \longrightarrow D(x)$ $(D \in \mathfrak{D})$ de Ω^1. L'application $x \longrightarrow dx$ se prolonge d'une manière et d'une seule en une application $\omega \longrightarrow d\omega$ de Ω dans lui-même qui possède les propriétés suivantes : on a $d(\omega + \omega') = d\omega + d\omega'$ si $\omega, \omega' \in \Omega$,

$$d(\omega \wedge \omega') = (d\omega) \wedge \omega' + (-1)^r \omega \wedge d\omega'$$

si $\omega \in \Omega^r$, $\omega' \in \Omega$; on a $d(d\omega) = 0$ $(\omega \in \Omega)$. On désigne par Z le noyau de d, par B son image et on pose $Z^r = Z \cap \Omega^r$, $B^r = B \cap \Omega^r$. Si $x \in K$, on a $x^k\, dx \in Z^1$ pour tout $k \geq 0$.

On sait qu'il existe des éléments $x_1, \ldots, x_n$ de K qui forment une p-base de K par rapport à L (i. e. les $x_1^{e_1} \ldots x_n^{e_n}$ pour $0 \leq e_i < p$ $(1 \leq i \leq n)$ forment une base de K par rapport à L). Les dx_i $(1 \leq i \leq n)$ forment alors une base de l'espace vectoriel Ω^1 sur K.

LEMME 1. - Tout élément de Z^1 se met d'une manière et d'une seule sous la forme de la somme d'un élément de B^1 et d'une combinaison linéaire à coefficients dans L des $x_i^{p-1}\, dx_i$ $(1 \leq i \leq n)$.

Nous désignerons par U l'ensemble des polynômes en n lettres $X_1, \ldots, X_n$ à coefficients dans L, nuls ou de degré partiel $\leq p - 1$ par rapport à chaque argument. Tout élément de K se met donc d'une manière et d'une seule sous la forme $x = H(x_1, \ldots, x_n)$, avec $H \in U$, et on a

$$dx = \sum_{i=1}^{n} (D_i H)(x_1, \ldots, x_n)\, dx_i \qquad ,$$

les D_i désignant les opérateurs de dérivation partielle. On a $D_i H \in U$, et $D_i H$ est nul ou de degré partiel $\leq p-2$ par rapport à X_i ; il s'ensuit qu'aucun élément $\neq 0$ de la forme

$$\sum_{i=1}^{n} u_i \, x_i^{p-1} \, dx_i \quad (u_i \in L , \quad 1 \leq i \leq n))$$

ne peut être dans B^1 . Un élément $\omega \in \Omega^1$ se met sous la forme

$$\omega = \sum_{i=1}^{n} H_i(x_1 , \ldots , x_n) \, dx_i , \quad H_i \in U \qquad ;$$

on voit tout de suite qu'une condition nécessaire et suffisante pour que $\omega \in Z^1$ est que l'on ait $D_i H_j = D_j H_i$ $(1 \leq i , j \leq n)$. Supposons qu'il en soit ainsi ; nous allons montrer par récurrence sur k qu'il existe des éléments $u_i \in L$ $(1 \leq i \leq k)$ et $v \in U$ tels que $\omega - dv - \sum_{i=1}^{k} u_i \, x_i^{p-1} \, dx_i$ soit combinaison linéaire à coefficients dans K de $dx_{k+1} , \ldots , dx_n$. C'est vrai pour $k = 0$. Supposons que ce soit vrai pour k . Pour montrer que c'est encore vrai pour $k + 1$, on se ramène tout de suite au cas où l'élément ω de Z^1 est combinaison linéaire de $dx_{k+1} , \ldots , dx_n$:

$$\omega = \sum_{i=k+1}^{n} H_i(x_1 , \ldots , x_n) \, dx_i \quad H_i \in U \qquad .$$

Ecrivant que $\omega \in Z$, il vient en particulier $D_i H_{k+1} = 0$ si $1 \leq i \leq k$. Comme H_{k+1} est nul ou de degrés partiels $\leq p-1$ par rapport à tous ses arguments, ces formules entraînent que H_{k+1} ne dépend pas de ses k-premiers arguments. Ecrivons

$$H_{k+1}(X_1 , \ldots , X_n) = \sum_{d=0}^{p-1} P_d(X_{k+2} , \ldots , X_n) \, X_{k+1}^d$$

où P_d est un polynôme en $n - k - 1$ lettres à coefficients dans L nul ou de degrés partiels $\leq p - 1$. La différentielle de

$$\sum_{d=0}^{p-2} (d+1)^{-1} \, P_d(x_{k+2} , \ldots , x_n) \, x_{k+1}^{d+1}$$

est une combinaison linéaire de $dx_{k+1} , \ldots , dx_n$ dans laquelle le coefficient de dx_{k+1} est

$$\sum_{d=0}^{p-2} P_d(x_{k+2} , \ldots , x_n) \, x_{k+1}^d \qquad .$$

On est donc ramené au cas où $P_0 = P_1 = \ldots = P_{p-2} = 0$.

Or, on a $D_i H_{k+1} = D_{k+1} H_i$ $(i > k + 1)$, et $D_{k+1} H_i$ est nul ou de degré partiel $\leq p-2$ par rapport à X_{k+1} . Comme $D_i H_{k+1}$ contient X_{k+1}^{p-1} en facteur, il est nul. Ceci étant vrai pour $k + 2 \leq i \leq n$, P_{p-1} est une constante u , et $\omega - u x_{k+1}^{p-1}\, dx_{k+1}$ est combinaison linéaire de $x_{k+2}, \ldots , x_n$. Le lemme est donc établi.

Nous introduirons le corps $L^{1/p}$ des racines p-ièmes des éléments de L (dans une clôture algébrique de K). Nous poserons $\tilde{\Omega}^1 = \Omega^1 \otimes_K L^{1/p}$. Les éléments de cet espace s'interprètent comme des applications K-linéaires de $\mathfrak{D}$ dans $L^{1/p}$; si $\omega \in \mathfrak{D}$, nous désignerons par $\langle D , \omega \rangle$ la valeur de ω en un point $D \in \mathfrak{D}$. Soit toujours $(x_1 , \ldots , x_n)$ une p-base de K/L . Il résulte du lemme 1 qu'il existe une application $C : Z^1 \longrightarrow \tilde{\Omega}^1$ et une seule qui possède les propriétés suivantes :

1° Si $\omega_1 , \omega_2 \in \tilde{\Omega}_1$, on a $C(\omega_1 + \omega_2) = C(\omega_1) + C(\omega_2)$

2° Si $f \in L$, $\omega \in \tilde{\Omega}_1$, on a $C(f\omega) = f^{1/p}\, C(\omega)$

3° On a $C(dx) = 0$ pour tout $x \in K$

4° On a $C(x_i^{p-1}\, dx_i) = dx_i \qquad (1 \leqslant i \leqslant n)$

PROPOSITION 1. - <u>On a</u> $C(x^{p-1}\, dx) = dx$ <u>pour tout</u> $x \in K$ <u>et</u> $C(x^{-1}\, dx) = x^{-1}\, dx$ <u>pour tout</u> $x \neq 0$. <u>L'opération</u> C <u>ne dépend pas de la p-base</u> $(x_1 , \ldots , x_n)$ <u>choisie</u>.

Si $x \neq 0$, les conditions $C(x^{p-1}\, dx) = dx$, $C(x^{-1}\, dx) = x^{-1}\, dx$ sont équivalentes en vertu de 2°. Soit N l'ensemble des x tels que $C(x^{p-1}\, dx) = dx$. Cet ensemble contient L , $x_1 , \ldots , x_n$, et il est clair que le produit de deux éléments de N est dans N . Il suffira donc de montrer que la somme de deux éléments de N est dans N , ou même que $x \in N$ entraîne $1 + x \in N$. Or, il est clair que $(1 + x)^{p-1}\, dx$ peut se mettre sous la forme $x^{p-1}\, dx + dy$ avec un $y \in K$, d'où

$$C((1 + x)^{p-1}\, dx) = C(x^{p-1}\, dx) = dx = d(1 + x) \qquad ,$$

et

$$1 + x \in N \qquad .$$

La deuxième assertion de la proposition 1 résulte des premières, puisque celles-ci entraînent que $C(x_i'^{\,p-1}\, dx_i') = dx_i'$ pour toute p-base $(x_1' , \ldots , x_n')$. L'opération C s'appelle <u>l'opération de Cartier</u>.

PROPOSITION 2. - <u>La suite</u>

$$0 \longrightarrow B^1 \longrightarrow Z^1 \xrightarrow{C} \tilde{\Omega}^1 \longrightarrow 0$$

<u>est exacte</u>.

Cela résulte du lemme 1, de la formule

$$C(dx + \sum_{i=1}^{n} u_i\, x_i^{p-1}\, dx_i) = \sum_{i=1}^{n} u_i^{1/p}\, dx_i$$

et du fait que les dx_i forment une base de Ω_1 .

LEMME 2. (HOCHSCHILD). - <u>Soit D une dérivation d'un anneau commutatif A de caractéristique $p > 0$. Si $u \in A$, on a</u> $D^{p-1}(u^{p-1}\, Du) = -(Du)^p + u^{p-1} D^p u$.

Soit A' l'anneau des polynômes en une infinité de variables $x , x_1 , \dots , x_n$, à coefficients dans le corps premier k , et soit D' la dérivation de A' telle que $Dx = x_1$, $Dx_n = x_{n+1}$. Il y a un homomorphisme $\varphi : A' \longrightarrow A$ tel que $\varphi(x) = u$, $\varphi(x_n) = D^n u$ pour tout n , et on a $D \circ \varphi = \varphi \circ D'$. Il suffira donc de démontrer le lemme dans le cas où $A = A'$, $D = D'$, $u = x$. Si $P \in A$, $DP = 0$, P est une puissance p-ième. S'il n'en était pas ainsi, il y aurait un plus petit indice i tel que

$$P \in k[x , x_1 , \dots , x_i , x_{i+1}^p , \dots , x_{i+n}^p , \dots] \quad .$$

Ecrivant que $DP = 0$ et notant P'_x , P'_{x_1} , ... , P'_{x_i} , ... les dérivées partielles de P , il viendrait

$$P'_x x_1 + P'_{x_1} x_2 + \dots + P'_{x_i} x_{i+1} = 0 \qquad P'_{x_i} \neq 0 \quad .$$

Il en résulterait que x_{i+1} appartiendrait au corps

$$k(x , x_1 , \dots , x_i , x_{i+1}^p , \dots , x_{i+n}^p , \dots) \quad ,$$

ce qui est évidemment impossible. Posons

$$P = D^{p-1}(x^{p-1}\, Dx) - x^{p-1}\, D^p\, x \quad .$$

Il est bien connu que D^p est une dérivation ; un calcul facile montre alors que $DP = 0$. Soit donc $P = Q^p$, $Q \in A$. Les éléments $x^{p-1} Dx = x^{p-1} x_1$ et $x^{p-1} D^p x = x^{p-1} x_p$ sont homogènes de degré p ; comme D transforme tout élément homogène en un élément homogène de même degré, P est homogène de degré p , donc Q homogène de degré 1 . Par ailleurs, si on attribue aux variables $x , x_1 , \dots , x_n , \dots$ les poids $0 , 1 , \dots , n$, D transforme tout élément isobare de poids k en un élément isobare de poids $k + 1$; P est isobare de poids p , donc Q isobare de poids 1 , et on a $Q = \alpha x_1$, $\alpha \in k$. Il y a donc un élément $\alpha \in k$ tel que, pour toute dérivation D d'un anneau A de caractéristique p , et tout $u \in A$, on ait

$$D^{p-1}(u^{p-1}\,Du) = \alpha^p (Du)^p + u^{p-1}\,D^p\,u \quad .$$

Prenant $A = F[x]$, $Dx = 1$, il vient $\alpha = -1$.

C. Q. F. D.

PROPOSITION 3. - Soient $\pi \in Z'$ et D une dérivation de $\mathcal{D}(K/L)$. Alors on a :

$$\langle D , C\pi \rangle^p = \langle D^p , \pi \rangle - D^{p-1}(\langle D , \pi \rangle) \quad .$$

Puisque C , D , D^2 , ... sont des opérateurs additifs, si l'identité est vraie pour $\pi = \pi_1$ et $\pi = \pi_2$ elle est aussi vraie pour $\pi = \pi_1 + \pi_2$. De plus si l'identité est vraie pour π , elle est aussi vraie pour $f\pi$, $f \in L$ puisque $C(f\pi) = f^{1/p}\,C\pi$ et $Df = 0$. Donc d'après le lemme 1, il suffit de vérifier l'identité lorsque $\pi = df$ et $\pi = \frac{df}{f}$ $f \neq 0$, $f \in F$. Si $\pi = df$, on a $\langle D , C\pi \rangle^p = 0$ et $\langle D^p , \pi \rangle - D^{p-1}(\langle D , \pi \rangle) = D^p(f) - D^{p-1}.Df = 0$.

Si $\pi = \frac{df}{f}$, on a $\langle D , C\pi \rangle^p = (\frac{Df}{f})^p$, $\langle D^p , \pi \rangle = \frac{D^p(f)}{f}$ et $D^{p-1}(\langle D , \pi \rangle) = D^{p-1}(\frac{D(f)}{f})$. Donc il faut démontrer que

$$(\frac{Df}{f})^p = \frac{D^p\,f}{f} - D^{p-1}(\frac{Df}{f}) \quad ,$$

ou encore que :

$$(Df)^p = f^{p-1}.Df - D^{p-1}(f^{p-1}.Df) \quad ;$$

c'est l'identité du lemme 2 . Donc la proposition est démontrée.

COROLLAIRE. - Si $\langle D , \pi \rangle \in L$, on a $\langle D , C\pi \rangle^p = \langle D^p , \pi \rangle$.

Soit A un anneau (pas nécessairement commutatif) avec élément unité. Pour $u \in A$, on désigne pour S_u l'opérateur $S_u(x) = ux - xu$, $x \in A$. Chaque élément de l'anneau produit tensoriel $A \otimes Z[T]$ peut être écrit de façon unique sous la forme $\sum_i a_i \otimes T^i$ (ou $\sum_i a_i\,T^i$) et on note $A[T] = A \otimes \underset{\sim}{Z}[T]$.

PROPOSITION 4. (Identité de Jacobson). - Soit A un anneau de caractéristique $p > 0$ (p premier). Alors pour u , $v \in A$, on a l'identité suivante :

$$(u + v)^p = u^p + v^p + \sum_{0<i<p} \frac{s_i(u , v)}{i}$$

où $s_i(u , v)$ est le coefficient de T^{i-1} dans le polynôme $S^{p-1}_{Tu+v}(u)$ en T .

Soient L_u et R_u les opérateurs $L_u(x) = u.x$ et $R_u(x) = x.u$, $x \in A$. Alors dans l'anneau $\mathcal{E}$ des endomorphismes additifs de A , on a

$$L_u . R_u = R_u . L_u \quad \text{et} \quad S_u = L_u - R_u \quad .$$

D'après les congruences, $\binom{p-1}{i} \equiv (-1)^i \pmod p$ et $\binom{p}{i} \equiv 0 \pmod p$, pour $0 < i < p$, on a

$$S_u^{p-1} = \sum_{0 \leq i < p} L_u^i R_u^{p-1-i} \quad \text{et} \quad S_u^p = L_u^p - R_u^p \quad .$$

On a donc

$$S_u^{p-1}(v) = \sum_{0 \leq i < p} u^i v u^{p-1-i} \quad .$$

Dans l'anneau $A[T]$, on peut écrire

$$(uT + v)^p = u^p T^p + v^p + \sum_{0<i<p} s_i'(u , v) T^i$$

avec $s_i'(u , v) \in A$. En différenciant par rapport à T, on a

$$\sum_{0 \leq i < p} (Tu + v)^i u(Tu + v)^{p-1-i} = \sum_{0<i<p} is_i'(u , v) T^{i-1} \quad .$$

En appliquant (1), on trouve que

$$S_{Tu+v}^{p-1}(u) = \sum_{0<i<p} is_i'(u , v) T^{i-1} \quad .$$

Finalement, en posant $s_i(u , v) = is_i'(u , v)$ et $T = 1$, on obtient l'identité de la proposition.

COROLLAIRE. - <u>Soient</u> A <u>un anneau de caractéristique</u> $p > 0$, D <u>une dérivation de</u> A, a <u>un élément de</u> A. <u>Pour tout</u> $x \in A$, <u>soit</u> L_x <u>la multiplication par</u> x. <u>On a</u> $(D + L_a)^p = D^p + L_{a^p} + L_{D^{p-1}(a)}$.

On applique la proposition 4 à l'anneau des endomorphismes du groupe additif de A en prenant $u = D$, $v = L_a$. On a

$$S_{Tu+v}(u) = L_a D - DL_a = - L_{D(a)} \quad ,$$

$$S_{Tu+v}(L_{D^j(a)}) = TL_{D^{j+1}(a)} \quad ,$$

d'où

$$S_{Tu+v}^{p-1}(D) = - T^{p-2} L_{D^{p-1}(a)} \quad .$$

Le corollaire résulte alors de la proposition 4.

2. <u>Caractérisation des différentielles logarithmiques.</u>

Soit B un anneau local commutatif, noethérien, ou plus généralement un anneau commutatif tel que chaque B-module projectif de type fini soit libre.

Soient M un B-module libre de type fini et E l'algèbre des endomorphismes de M.

PROPOSITION 5. - Soit σ un endomorphisme de l'algèbre E ; alors σ est un automorphisme intérieur (i. e. il existe un élément inversible Y de E tel que $\sigma(\Theta) = Y\Theta Y^{-1}$ pour chaque Θ de E.

Soient x_i $(1 \leq i \leq n)$ une base de M et e_i $(1 \leq i \leq n)$ les éléments de E définis par la relation $e_i(x_j) = \delta_{ij}$ $(1 \leq i , j \leq n)$. Alors on a

$$(1) \qquad e_i^2 = e_i \ , \quad e_i\, e_j = 0 \ \text{ si } \ i \neq j \ \text{ et } \ \sum_{1 \leq i \leq n} e_i = 1 \quad .$$

Donc si l'on pose $f_i = \sigma(e_i)$, on a aussi

$$(2) \qquad f_i^2 = f_i \ ; \quad f_i\, f_j = 0 \ \text{ si } \ i \neq j \ \text{ et } \ \sum_{1 \leq i \leq n} f_i = 1 \quad .$$

Pour chaque i, $f_i \neq 0$; en effet, si ce n'est pas vrai, il existe un i tel que $f_i = 0$ et on peut supposer que c'est f_1 ; soit Θ_{ij} $(1 \leq i , j \leq n)$ l'élément de E défini par les relations $\Theta_{ij}(x_i) = x_j$; $\Theta_{ij}(x_k) = 0$, $k \neq i , j$; alors on a $\Theta_{1i}\, e_1\, \Theta_{i1} = e_i$ donc $\sigma(e_1) = f_1 = 0$ implique que $\sigma(e_i) = f_i = 0$ pour chaque i, ce qui est en contradiction avec le fait que $\sum_{1 \leq i \leq n} f_i = 1$.

Posons $M_i = f_i(M)$; les relations (2) impliquent que M est somme directe des M_i. Chacun des M_i est donc projectif et d'après l'hypothèse faite sur B, les M_i sont libres. Par ailleurs M_i est de rang 1 puisque $M_i \neq 0$. Il y a donc une base (y_i) $(1 \leq i \leq n)$ de M telle que $M_i = By_i$ $(1 \leq i \leq n)$ et $f_i(y_i) = y_i$; $f_i(y_j) = 0$ si $i \neq j$. Soit t l'automorphisme de M qui transforme x_i en y_i $(1 \leq i \leq n)$; soit $\tau(s) = t\, s t^{-1}$ pour tout $s \in E$. On a $\tau(e_i) = f_i$ $(1 \leq i \leq n)$; d'où $(\tau^{-1}\sigma)(e_i) = e_i$. Nous sommes donc ramenés au cas où $\sigma(e_i) = e_i$ pour tout i.

Soit $e_{ij} = \Theta_{ij}$ (i. e. l'endomorphisme qui applique x_j sur x_i et x_k sur 0 si $j \neq k$), alors on a $e_{ij}.e_{jk} = e_{ik}$; $e_{ii} = e_i$ et $e_{ij} = e_i\, e_{ij}\, e_j$. Donc $\sigma(e_{ij}) = e_i\, \sigma(e_{ij})\, e_j$ et puisque l'élément $e_i\, \sigma(e_{ij})\, e_j$ est de la forme $\lambda.e_{ij}$ avec λ dans B, on a $\sigma(e_{ij}) = a_{ij}\, e_{ij}$; a_{ij} dans B. Les a_{ij} satisfont aux relations $a_{ij}.a_{jk} = a_{ik}$; $a_{ii} = 1$. Il en résulte qu'on peut écrire $a_{ij} = a_j.a_i^{-1}$ les a_i étant des éléments inversibles de B. Soit Y l'automorphisme défini par $Y(x_i) = a_i\, x_i$; alors σ est l'automorphisme intérieur produit par Y, comme on le vérifie tout de suite.

C. Q. F. D.

On utilisera maintenant les notations du paragraphe 1 en faisant de plus les hypothèses suivantes : L est le corps des fractions d'un anneau local noethérien B ; K est le corps des fractions d'un anneau A qui contient B ; il existe une p-base $(x_1, \ldots, x_n)$ de A par rapport à B (i. e. les $x_1^{e_1} \ldots x_n^{e_n}$, $0 \leqslant e_i < p$, forment une base de A comme B-module) ; les x_i forment une p-base de L par rapport à K (on verra plus tard que cette dernière condition est toujours satisfaite ; cf. lemme 3, paragraphe 3).

Soit $\mathfrak{G}$ l'ensemble de toutes les B-dérivations de A dans lui-même ; alors $\mathfrak{G}$ est un A-module libre et les dérivations D_i $(1 \leqslant i \leqslant n)$ définies par les relations $D_i(x_j) = \delta_{ij}$ $(1 \leqslant i , j \leqslant n)$ forment une base de $\mathfrak{G}$. Le module $\mathfrak{G}$ est aussi une p-algèbre, i. e. si $D_1, D_2 \in \mathfrak{G}$ on a $D_1^p \in \mathfrak{G}$ et $D_1 D_2 - D_2 D_1 = [D_1, D_2] \in \mathfrak{G}$. Chaque B-dérivation de A peut être prolongée de façon unique en une L-dérivation de K et donc on peut considérer $\mathfrak{G}$ comme un sous-groupe de l'espace K-vectoriel $\mathfrak{D}$ des L-dérivations de K. Le sous-espace K-vectoriel engendré par $\mathfrak{G}$ est identique à $\mathfrak{D}$ lui-même.

THÉORÈME 1 (Voir aussi [1], chapitre 2, proposition 8). - Soit $\omega = \sum a_i \, dx_i$ une forme différentielle appartenant à $\Omega^1(K/L)$ avec $a_i \in A$. Pour qu'il existe $x \in A^*$ (A^* le sous-groupe multiplicatif des éléments inversibles de A) tel que $\omega = \frac{dx}{x}$, il faut et il suffit qu'on ait $d\omega = 0$, $C\omega = \omega$.

La nécessité a déjà été démontrée. Il reste à démontrer la suffisance. Les deux conditions $d\omega = 0$ et $C\omega = \omega$ entraînent que

(1) $$D_i(a_j) - D_j(a_i) = 0$$

(2) $$D_i^{p-1}(a_i) + a_i^p = 0 \quad ;$$

en effet (1) est une conséquence immédiate de $d\omega = 0$ et (2) est une conséquence facile de la proposition 3 en observant que $D_i^p = 0$. On va démontrer en fait que les conditions (1) et (2) entraînent que $\omega = \frac{dx}{x}$, $x \in A^*$.

Soit M l'algèbre des endomorphismes de A en tant que B-module ; on peut identifier M à l'algèbre des matrices sur B de rang p^n. On peut identifier A à une sous-algèbre de M en considérant pour chaque élément de A l'homothétie définie par cet élément ; d'autre part M contient aussi les dérivations D_i $(1 \leqslant i \leqslant n)$. On a $D_i^p = 0$ et $[D_i D_j] = 0$. Soit U la B-sous-algèbre de M engendrée par les D_i ; alors on voit facilement que les éléments $D_1^{a_1} \ldots D_n^{a_n}$ $(0 \leqslant a_i < p)$ forment une base de U sur B en tant que B-module.

Considérons l'application

$$f : A \otimes_B U \longrightarrow M$$

définie par $f(a \otimes u) = a.u$, $a \in A$, $u \in U$. L'application f est un B-homomorphisme (au sens de modules et pas au sens des algèbres). On va démontrer maintenant que f est bijective.

Introduisons l'ordre lexicographique dans l'ensemble des éléments $(a_1, \ldots, a_n)$, $(0 \leq a_i < p)$. Si $(a_1, \ldots, a_n)$ est le j-ième élément de cet ensemble, on désigne par X_j l'élément $x_1^{a_1}, \ldots, x_n^{a_n}$ et par E_j l'élément $D_1^{a_1} D_2^{a_2} \ldots D_n^{a_n}$. On a $E_i(X_j) = 0$ si $i > j$ et $E_i(X_i)$ est un élément non nul du corps premier. Donc la matrice triangulaire $(E_i(X_j))_{ij}$ est une matrice inversible (sur A). Soient T un élément de M et $T(X_j) = \alpha_j$ $(0 \leq j < p^n)$, $\alpha_j \in A$. Puisque $(E_i(X_j))_{ij}$ est inversible, on peut trouver des éléments $\beta_j \in A$ $(0 \leq j < p^n)$ de façon unique tels que

$$\left(\sum_{j=0}^{p^n} \beta_j E_j\right)(X_i) = \sum_{j=0}^{p^n} \beta_j E_j(X_i) = \alpha_i \qquad (1 \leq i \leq n) \quad .$$

L'élément $\theta = \sum_{j=0}^{p^n} \beta_j \otimes E_j$ de $A \otimes_B U$ possède la propriété $f(\theta) = T$ et c'est le seul élément de $A \otimes_B U$ ayant cette propriété. Donc f est bijective.

On va maintenant utiliser le B-isomorphisme f (au sens des B-modules) pour définir un automorphisme σ de l'algèbre M . D'abord on peut définir un homomorphisme τ d'algèbres $\tau : U \longrightarrow M$ déterminé par les relations $\tau(D_i) = D_i + a_i$ (où les a_i sont les coefficients de la forme différentielle $\omega = \sum a_i \, dx_i$ et donc satisfont aux conditions (1) et (2)) ; pour ceci, il faut seulement vérifier que $(D_i + a_i)^p = 0$ et $[D_i + a_i , D_j + a_j] = 0$; la condition $[D_i + a_i , D_j + a_j] = 0$ équivaut à (1) et $(D_i + a_i)^p = 0$ équivaut, d'après le corollaire à la proposition 4 , à la condition (2). Soit maintenant $\tau_1 : A \otimes_B U \longrightarrow M$ le B-homomorphisme (au sens des B-modules) défini par les relations $\tau_1(u) = \tau(u)$, $u \in U$ et $\tau_1(a) = a$, $a \in A$. Posons

$$\sigma : M \longrightarrow M , \quad \sigma = \tau_1 \circ f^{-1} \quad .$$

Il est immédiat que σ est un B-homomorphisme au sens des modules. De plus, on voit facilement que la restriction de σ à U est un homomorphisme d'algèbres et que $\sigma(a.u) = a.\sigma(u) = \sigma(a).\sigma(u)$, $a \in A$, $u \in U$ (en particulier $\sigma(1) = 1$). Il en résulte que $\sigma(v u) = \sigma(v)\sigma(u)$ si $v \in M$, $u \in U$. Donc pour vérifier que σ est un endomorphisme de l'algèbre M il est suffisant de vérifier que $\sigma(u.a) = \sigma(u).a$, $u \in U$, $a \in A$. Puisque U est engendré par les D_i , ceci se ramène à vérifier que $\sigma(D_i a) = (D_i + a_i).a$. On a $D_i a - a.D_i = D_i(a)$;

par conséquent

$$\sigma(D_i\ a) = \sigma(a.D_i + D_i(a)) = a.(D_i + a_i) + D_i(a) = (D_i + a_i).a \quad .$$

On a ainsi démontré que σ est un homomorphisme d'algèbres avec $\sigma(1) = 1$.

En appliquant maintenant la proposition 5 , il existe un élément inversible Y de M tel que $\sigma(\Theta) = Y^{-1}\,\Theta\,Y$. Puisque $\sigma(a) = a$, $a \in A$, Y commute avec les éléments de A . Donc pour $a \in A$,

$$Y(a) = (Y.a)(1) = a.Y(1) \quad ,$$

ceci implique que Y est un élément (inversible) de A .
On a $Y^{-1}.D_i = (D_i + a_i)$, ou $Y^{-1}(Y.D_i + D_i(Y)) = D_i + a_i$ (i. e.) $Y^{-1}.D_i(Y) = a_i$; ce qui montre que $\omega = \frac{dY}{Y}$.

C. Q. F. D.

3. <u>Variété quotient par un sous-fibré intégrable de vecteurs tangents.</u>

Dans ce paragraphe, on ne considère que des variétés définies sur un corps K algébriquement clos de caractéristique $p > 0$. Soit T une variété non singulière, et soit $\mathfrak{t}(T)$ l'espace fibré des vecteurs tangents à T . Pour tout point $Q \in T$, les germes de sections de $\mathfrak{t}(T)$ au voisinage de Q forment un module libre $\mathfrak{G}_Q$ de rang $n = \dim T$ sur l'anneau local $\mathcal{O}_Q$ de Q ; de plus $\mathfrak{G}_Q$ possède une structure de p-anneau de Lie. Soit $\mathfrak{n}$ un sous-fibré de $\mathfrak{t}(T)$; soit $\mathfrak{H}_Q$ le module des germes de sections de $\mathfrak{n}$ au voisinage de Q . Si, pour tout $Q \in T$, $\mathfrak{H}_Q$ est stable par rapport aux opérations de crochet et de puissance p-ième dans $\mathfrak{G}_Q$, on dit que $\mathfrak{n}$ est <u>intégrable</u>.

Soient T' une variété non singulière et $i : T' \longrightarrow T$ un morphisme de revêtement radiciel sur une variété T . Supposons que le noyau de l'application différentielle di soit un sous-fibré $\mathfrak{n}$ de $\mathfrak{t}(T')$. (Cette condition est satisfaite pour la restriction de i à un ouvert convenable de T'). On voit immédiatement que $\mathfrak{n}$ est intégrable. Si on suppose que T' est une variété de groupe et que i est un homomorphisme algébrique, il est évident que le noyau de l'application différentielle di est un sous-fibré $\mathfrak{n}$ de $\mathfrak{t}(T')$ qui est invariant et intégrable. Réciproquement, étant donné un sous-fibré intégrable $\mathfrak{n}$ de $\mathfrak{t}(T')$ (resp. intégrable et invariant si T' est une variété de groupe) on peut se demander s'il existe un morphisme de revêtement radiciel $i : T' \longrightarrow T$ sur une variété T (resp. un homomorphisme algébrique radiciel $i : T' \longrightarrow T$ sur une variété de groupe T) tel que le noyau de di soit $\mathfrak{n}$. On va démontrer qu'il en est bien ainsi ; de plus T sera unique sous quelques hypothèses ; on l'appelle <u>la variété quotient</u> (resp. <u>la variété du groupe quotient</u>) de T' par $\mathfrak{n}$.

Soient Q' un point de T', $\mathcal{O}_{Q'}$, son anneau local, $\mathfrak{L}_{Q'}$ (resp. $\mathfrak{H}_{Q'}$) le module des germes de sections de $\mathfrak{t}(T')$ (resp. $\mathfrak{n}$) au voisinage de Q' ; $\mathfrak{H}_{Q'}$ est un sous-module libre de $\mathfrak{L}_{Q'}$ et en est facteur direct ; nous désignerons son rang par r. Par ailleurs, les éléments de $\mathfrak{L}_{Q'}$ peuvent évidemment s'interpréter comme des dérivations de l'anneau $\mathcal{O}_{Q'}$; on désignera par $\mathfrak{B}_{Q'}$ le sous-anneau de $\mathcal{O}_{Q'}$ composé des éléments annulés par tous les éléments de $\mathfrak{H}_{Q'}$. On écrira simplement $\mathcal{O}$, $\mathfrak{L}$, $\mathfrak{H}$, $\mathfrak{B}$ au lieu de $\mathcal{O}_{Q'}$, $\mathfrak{L}_{Q'}$, $\mathfrak{H}_{Q'}$, $\mathfrak{B}_{Q'}$ s'il n'y a pas de confusion possible.

PROPOSITION 6. - <u>Il y a une base</u> $(D_1, \dots, D_r)$ <u>de</u> $\mathfrak{H}$ <u>et un système de variables uniformisantes</u> $y_1, \dots, y_n$ <u>de</u> T' <u>en</u> Q' <u>tels que</u>

1° $y_1, \dots, y_r$ <u>forment à la fois une</u> p-<u>base de</u> $\mathcal{O}$ <u>sur</u> $\mathfrak{B}$ <u>et une</u> p-<u>base du corps de fonctions</u> $R(T')$ <u>de</u> T' <u>sur le corps des fractions de</u> $\mathfrak{B}$;

2° $D_i(y_j) = \delta_{ij}$ $(1 \leq i \leq r, \ 1 \leq j \leq n)$

3° $\mathfrak{B}$ <u>est un anneau local régulier et</u> $y_1^p, \dots, y_r^p, y_{r+1}, \dots, y_n$ <u>forment un système de variables uniformisantes de</u> $\mathfrak{B}$.

Soit d'abord $(\bar{y}_1, \dots, \bar{y}_n)$ un système quelconque de variables uniformisantes. L'application $f : \mathfrak{L} \longrightarrow \mathcal{O}^n$ définie par $f(D) = (D(\bar{y}_1), \dots, D(\bar{y}_n))$ est alors un isomorphisme de $\mathfrak{L}$ sur $\mathcal{O}^n$. $f(\mathfrak{H})$ est un facteur direct de $\mathcal{O}^n$. Comme tout $\mathcal{O}$-module projectif de rang fini est libre, il y a une base $(z_1, \dots, z_n)$ de $\mathcal{O}^n$ qui contient une base $(z_1, \dots, z_r)$ de $f(\mathfrak{H})$. Posons $z_k = (a_{1k}, \dots, a_{nk})$ $(1 \leq k \leq n)$; la matrice (a_{ik}) étant inversible dans l'anneau des matrices à coefficients dans $\mathcal{O}$, son déterminant est inversible, d'où il résulte qu'il y a au moins une matrice carrée de degré r extraite de la matrice de type (n, r) formée des r premières colonnes de (a_{ik}) dont le déterminant n'est pas dans l'idéal premier maximal de $\mathcal{O}$, et qui est par suite inversible. Changeant au besoin l'ordre de $\bar{y}_1, \dots, \bar{y}_n$, on peut supposer que la matrice $(a_{ij})_{1 \leq i, j \leq r}$ est inversible. Il en résulte qu'il y a une base $(D_1, \dots, D_r)$ de $\mathfrak{H}$ telle que $D_i(\bar{y}_j) = \delta_{ij}$ $(1 \leq i, j \leq r)$.

LEMME 3 (voir [5]). - <u>Soient</u> $\mathcal{O}$ <u>un anneau commutatif de caractéristique</u> $p > 0$ (p <u>premier</u>) <u>et</u> $\mathfrak{H}$ <u>une</u> p-<u>sous-algèbre de l'algèbre de Lie de toutes les dérivations de</u> $\mathcal{O}$ <u>dans lui-même. Supposons que</u> $\mathfrak{H}$ <u>soit un module libre sur</u> $\mathcal{O}$ <u>de rang fini</u> r <u>et qu'il existe une base</u> $D_1, \dots, D_r$ <u>de</u> $\mathfrak{H}$ <u>et des éléments</u>

$y_1, \dots, y_r$ de $\mathcal{O}$ tels que

$$D_i(y_j) = \delta_{ij}, \quad 1 \le i, j \le r \quad .$$

Alors $y_1, \dots, y_r$ forment une p-base de $\mathcal{O}$ sur le sous-anneau $\mathfrak{B}$ formé par tous les éléments de $\mathcal{O}$ annulés par $\mathcal{D}$; en particulier, une dérivation de $\mathcal{O}$ qui s'annule sur $\mathfrak{B}$ appartient à $\mathcal{D}$.

Chaque élément D de $\mathcal{D}$ est de la forme $\sum a_i D_i$, $a_i \in \mathcal{O}$. Donc $D = 0$ si et seulement si $D(y_i) = 0$ pour $1 \le i \le r$. Or pour les dérivations D_i^p et $[D_i, D_j]$, qui appartiennent à $\mathcal{D}$ puisque c'est une p-algèbre, on a $D_i^p[y_j] = 0$ et $[D_i, D_j](y_k) = 0$ pour $1 \le i, j, k \le r$; par conséquent $D_i^p = 0$ et $[D_i, D_j] = 0$ (D_i et D_j commutent).

Il est évident que les éléments $y_1^{a_1} \dots y_n^{a_n}$ $(0 \le a_i < p)$ sont linéairement indépendants sur $\mathfrak{B}$. Donc il suffit de démontrer que

$$\mathfrak{B}[y_1, \dots, y_r] = \mathcal{O} \quad .$$

Supposons qu'il existe un élément $v_1 \in \mathcal{O}$ tel que $v_1 \notin \mathfrak{B}[y_1, \dots, y_r]$. Alors considérons l'assertion suivante : Étant donné un entier $q \geq 1$, il existe un élément $v_q \notin \mathfrak{B}[y_1, \dots, y_r]$ tel que $D_i[v_q] = 0$ $(i \le q - 1)$. Cette assertion est satisfaite pour $q = 1$ d'après la supposition faite ci-dessus ; supposons que ce soit vrai pour tous les entiers $\le q$; on va la démontrer pour l'entier $q + 1$.

Puisque $D_i^p = 0$, il existe un entier e, $0 \le e < p$ tel que $D_q^{e+1}(v_q) \in \mathcal{B}[y_1, \dots, y_r]$ et $D_q^e(v_q) \notin \mathcal{B}[y_1, \dots, y_r]$. Puisque D_i et D_j commutent, on a $D_i D_q^e(v_q) = D_q^e D_i(v_q)$. Si $i < q$, $D_i(v_q) = 0$ et par conséquent $D_i(D_q^e(v_q)) = 0$.
Donc on peut supposer qu'il existe v_q tel que $v_q \notin \mathfrak{B}[y_1, \dots, y_r]$, $D_i(v_q) = 0$ pour $i \le q - 1$ et $D_q(v_q) \in \mathfrak{B}[y_1, \dots, y_r]$. Pour l'élément $D_q(v_q)$ de $\mathfrak{B}[y_1, \dots, y_r]$, on a la propriété $D_i(D_q(v_q)) = D_q(D_i(v_q)) = 0$ pour $i \le q - 1$. Ceci implique, en utilisant le fait que $y_1, \dots, y_r$ forment une p-base de $\mathfrak{B}[y_1, \dots, y_r]$ sur $\mathfrak{B}$, qu'on peut écrire $D_q(v_q)$ comme un polynôme en $y_q, \dots, y_r$ à coefficients dans $\mathfrak{B}$ (avec degré $< p$ en chaque y_i). Puisqu'on a aussi $D_q^{p-1}(D_q(v_q)) = 0$, le coefficient de y_q^{p-1} dans ce polynôme est nul. Donc on peut intégrer ce polynôme par rapport à la dérivation D_q et il existe $w \in B[y_q, \dots, y_r]$ tel que $D_q(w) = D_q(v_q)$. Posons $v_{q+1} = v_q - w$. Alors $v_{q+1} \notin \mathfrak{B}[y_1, \dots, y_r]$ et on a $D_i(v_q - w) = 0$ pour $i \le q$.

Par cet argument de récurrence, l'assertion faite ci-dessus est vraie pour tout entier q. En particulier si $q = r + 1$, il existe v_{r+1} de $\mathcal{O}$ tel que $v_{r+1} \notin \mathfrak{B}[y_1, \ldots, y_r]$ et $D_i(v_{r+1}) = 0$ pour $i \leq r$; ce qui implique que $v_{r+1} \in \mathfrak{B}$ puisque les D_i $(1 \leq i \leq r)$ forment une base de $\mathfrak{D}$. Ceci conduit à une contradiction ; on a donc bien $\mathcal{O} = \mathfrak{B}[y_1, \ldots, y_r]$.

C. Q. F. D.

Revenons à la démonstration de la proposition 6. Les sections rationnelles de $\mathfrak{n}$ constituent une p-algèbre de Lie $\mathfrak{G}$ de dérivations du corps des fonctions rationnelles $R(T')$ de T'. Soit L le sous-corps de $R(T')$ formée par tous les éléments de $R(T')$ annulés par les dérivations de $\mathfrak{G}$. On a évidemment $\mathfrak{B} = L \cap \mathcal{O}$. En appliquant le lemme 3, on obtient que $\bar{y}_1, \ldots, \bar{y}_r$ forment une p-base de $\mathcal{O}$ sur $\mathfrak{B}$ et de $R(T')$ sur L. Donc pour (1), il suffit de voir que L est le corps des fractions de $\mathfrak{B}$. Soit M le corps des fractions de $\mathfrak{B}$. On a d'abord $M \subset L$. L'anneau $M[\bar{y}_1, \ldots, \bar{y}_r]$ est un sous-anneau de l'extension finie $R(T')$ de M ; donc $M[\bar{y}_1, \ldots, \bar{y}_r]$ est un corps. On sait que $\mathfrak{B}[\bar{y}_1, \ldots, \bar{y}_r] = \mathcal{O}$ et que $R(T')$ est le corps des fractions de $\mathcal{O}$, d'où $R(T') = M[\bar{y}_1, \ldots, \bar{y}_r]$. De plus, comme $\bar{y}_1, \ldots, \bar{y}_r$ forment une p-base de $\mathcal{O}$, $R(T')$ est de degré p^r sur M. Comme $\bar{y}_1, \ldots, \bar{y}_r$ forment une p-base de $R(T')$ sur L, $[R(T') : L]$ est aussi p^r, d'où $L = M$.

Nous poserons $y_1 = \bar{y}_1, \ldots, y_r = \bar{y}_r$; la condition 1° de la proposition 6 sera donc satisfaite. Utilisant le fait que les $y_1^{e_1} \ldots y_r^{e_r}$ $(0 \leq e_i < p)$ forment une base de $\mathcal{O}$ sur $\mathfrak{B}$, on voit que, si $j > r$, y_j se met sous la forme $\sum_{k=1}^{r} \lambda_{jk} y_k + \bar{v}_j$ avec $\lambda_{jk} \in \mathcal{O}$, $v_j \in \mathfrak{B}$. Il est clair que $y_1, \ldots, y_n$ forment encore un système de variables uniformisantes de $\mathcal{O}$; la condition (2) de la proposition 6 est satisfaite pour ce système.

Il reste à établir (3). Soit $\mathcal{O}^{[p]}$ l'anneau des puissances p-ièmes des éléments de $\mathcal{O}$. C'est un anneau isomorphe à $\mathcal{O}$, donc noethérien. C'est l'ensemble des éléments de $\mathcal{O}$ annulés par tous les éléments de $\mathfrak{G}$, car, si $u \in \mathcal{O}$, $D(u) = 0$ pour tout $D \in \mathfrak{G}$, u est annulé par toute dérivation de $R(T')$, donc est puissance p-ième d'un élément $v \in R(T')$; on a $v \in \mathcal{O}$ parce que $\mathcal{O}$ est intégralement clos. Il résulte alors du lemme 3 que $y_1, \ldots, y_n$ forment une p-base de $\mathcal{O}$ sur $\mathcal{O}^{[p]}$, donc que $\mathcal{O}$ est un module de type fini sur $\mathcal{O}^{[p]}$. On a $\mathcal{O}^{[p]} \subset \mathfrak{B} \subset \mathcal{O}$, de sorte que $\mathfrak{B}$ est un module de type fini sur $\mathcal{O}^{[p]}$, donc un anneau noethérien. Soit $\mathfrak{m}$ l'idéal premier maximal de $\mathcal{O}$; il est évident que $\mathfrak{B}$ est un anneau local d'idéal premier maximal $\mathfrak{m} \cap \mathfrak{B}$. Comme $\mathcal{O}$ est entier sur $\mathfrak{B}$ (puisque $\mathcal{O}^{[p]} \subset \mathfrak{B}$), on a $\dim \mathfrak{B} = \dim \mathcal{O}$. Pour montrer que la condition 3° de la proposition 6 est satisfaite, il suffira de montrer que $y_1^p, \dots, y_r^p, y_{r+1}, \dots, y_n$ engendrent l'idéal $\mathfrak{m} \cap \mathfrak{B}$. Or, soit $u \in \mathfrak{m} \cap \mathfrak{B}$; on peut écrire $u = H(y_1, \dots, y_n)$, H étant un polynôme à coefficients dans $\mathcal{O}^{[p]}$, nul ou de degré partiel $< p$ par rapport à chaque argument. Comme $u \in \mathfrak{B}$, les r premières dérivées partielles de H sont nulles, d'où $u = H'(y_{r+1}, \dots, y_n)$, H' polynôme à coefficients dans $\mathcal{O}^p$. Le terme constant de H' est dans $\mathfrak{m} \cap \mathcal{O}^{[p]}$, donc dans l'idéal engendré par $y_1^p, \dots, y_n^p$ dans $\mathcal{O}^{[p]}$, d'où le résultat. La proposition 6 est donc établie.

REMARQUE. - Lorsque $\mathfrak{h} = \mathfrak{G}$, $y_1^p, \dots, y_n^p$ forment un système de variables uniformisantes de $\mathfrak{B}$ et il en résulte que $\mathfrak{B} = \mathcal{O}^p$.

THÉORÈME 2. - Soient T' une variété non singulière et $\mathfrak{n}$ un sous-fibré intégrable de l'espace fibré des vecteurs tangents $\mathfrak{T}(T')$ sur T'. Alors il existe une structure unique de variété T sur le même espace topologique que T' telle que l'application identique $i : T' \to T$ soit un morphisme de revêtement radiciel de hauteur 1 (i. e. $R(T') \supset R(T) \supset R(T')^p$) et que $\mathfrak{n}$ soit le noyau de l'application différentielle di ; la variété T est non singulière. Si on suppose en outre que T' soit une variété de groupe et $\mathfrak{n}$ invariant, T est en plus une variété de groupe et i un homomorphisme algébrique.

Considérons d'abord le cas où T' est affine, soit P' son algèbre affine. Les sections de $\mathfrak{n}$ tout entier forment un module N sur P', dont les éléments peuvent s'interpréter comme des dérivations de P' et se prolongent en des dérivations de $R(T')$; soit P l'ensemble des éléments de $R(T')$ qui sont annulés par toutes ces dérivations. On a $P' \supset P \supset P'^{[p]}$, où $P'^{[p]}$ est l'ensemble des puissances p-ièmes d'éléments de P' ; on en déduit que P est un module de type fini sur $P'^{[p]}$, donc est une algèbre affine. Tout homomorphisme de P dans K se prolonge d'une manière et d'une seule en un homomorphisme de P' dans K ; on en déduit qu'on peut munir l'ensemble T' d'une structure de variété affine, soit T, admettant P comme algèbre affine. Comme tout ensemble fermé de T' peut s'obtenir en égalant à 0 certaines fonctions de $P'^{[p]}$, donc de P, un pareil ensemble est aussi fermé dans T, et T, T' ont le même espace topologique sous-jacent. Soit Q' un point de T' ; utilisons les notations introduites avant la proposition 6. Puisque T' est affine, il résulte de la théorie des faisceaux cohérents que $\mathfrak{N}_{Q'} = \mathcal{O}_{Q'} \otimes_{P'} N$; $\mathfrak{B}_{Q'}$ est donc l'ensemble des éléments de $\mathcal{O}_{Q'}$ annulés par les dérivations appartenant à N. Tout élément de $\mathcal{O}_{Q'}$ peut évidemment se mettre sous la forme uv^{-p}, où $u, v \in P'$, $v(Q') \neq 0$; pour que cet élément appartienne à $\mathfrak{B}_{Q'}$, il faut et il suffit que $D(u) = 0$

pour tout $D \in \mathbb{N}$, donc que $u \in P$. Il en résulte que $\mathcal{B}_{Q'}$ n'est autre que l'anneau local de Q' sur T . De plus, il existe un système de variables uniformisantes $y_1 , \ldots , y_n$ en Q' sur T' tel que

$$y_1^p , \ldots , y_r^p , y_{r+1} , \ldots , y_n$$

forment un système de variables uniformisantes en Q' sur T , où r est le rang du $\mathcal{O}_{Q'}$-module $\mathfrak{H}_{Q'}$. Soit i l'application identique $T' \longrightarrow T$, qui est un morphisme ; il résulte de ce qu'on vient de dire que le noyau de l'application linéaire $d_{Q'} i$ tangente à i en Q' est de dimension r . Or ce noyau ~~contient~~ le sous-espace $(\mathfrak{H}_{Q'} + \mathfrak{m}\,\mathfrak{G}_{Q'})/\mathfrak{m}\,\mathfrak{G}_{Q'}$ de l'espace tangent $\mathfrak{G}_{Q'}/\mathfrak{m}\,\mathfrak{G}_{Q'}$ à T' en Q' . Or ce sous-espace, qui est la fibre de Q' dans $\mathfrak{n}$, est de dimension r ; il est donc égal au noyau de $d_{Q'} i$; il en résulte que le fibré $\mathfrak{n}$ est bien le noyau de di .

Montrons maintenant que toute structure de variété T_1 sur l'ensemble T' telle que l'application identique $i_1 : T' \longrightarrow T_1$ soit un morphisme radiciel de hauteur 1 et que le noyau de di_1 soit $\mathfrak{n}$ est identique à T . Si $Q' \in T'$, soit $\mathcal{O}_{Q'}(T_1)$ (resp. $\mathcal{O}_{Q'}(T)$) l'anneau local de Q' sur T_1 (resp. T) . Il est clair que les éléments de $\mathcal{O}_{Q'}(T_1)$ sont annulés par les dérivations appartenant à $\mathfrak{H}_{Q'}$, donc sont contenus dans $\mathcal{O}_{Q'}(T)$. L'application i_1 se factorise donc en $i_1 = j \circ i$, j étant un morphisme de T dans T_1 . Utilisant les mêmes notations que plus haut, posons $z_k = y_k^p$ si $k \leq r$, $z_k = y_k$ si $r < k \leq n$. Alors l'espace tangent à T en Q' admet une base $(L_1 , \ldots , L_n)$ telle que $\langle L_k , z_{k'} \rangle = \delta_{kk'}$ $(1 \leq k , k' \leq n)$; l'image de $d_{Q'} i$ est l'espace engendré par $L_{r+1} , \ldots , L_n$. Comme i_1 est de hauteur 1 , $z_1 , \ldots , z_r$ appartiennent à $\mathcal{O}_{Q'}(T_1)$; si donc L est un élément du noyau de l'application linéaire $d_{Q'} j$ tangente à j en Q' , on a $\langle L , z_k \rangle = 0$ $(1 \leq k \leq r)$, et L appartient à l'image de $d_{Q'} i$. Mais $d_{Q'} i$ et $d_{Q'} i_1$ ont par hypothèse même noyau, à savoir la fibre de Q' dans $\mathfrak{n}$. On a donc $L = 0$, et $d_{Q'} j$ est un monomorphisme. Cela signifie que j n'est pas ramifié ; comme c'est un morphisme radiciel, c'est un isomorphisme, d'ou $T_1 = T$.

Passons maintenant au cas général. Recouvrons T' par des morceaux affines U'_k en nombre fini. Chaque ensemble U'_k est muni d'une structure de variété U_k telle que l'application identique $i_k : U'_k \longrightarrow U_k$ soit un morphisme radiciel de hauteur ≤ 1 et que le noyau de di_k soit le fibré induit par $\mathfrak{n}$ sur U'_k ; de plus i_k est un homéomorphisme. Faisant usage de l'assertion d'unicité établie ci-dessus et du fait que les $U'_k \cap U'_{k'}$ sont affines, on voit que, pour tout couple (k , k') , $U_k \cap U_{k'}$ est ouvert dans U_k et $U_{k'}$ et que les structures de variétés induites sur cet ouvert par celles de U_k et $U_{k'}$ coïncident. On peut donc définir par recollement une structure de pré-variété T sur l'ensemble T' dont les U_k soient des sous-variétés ouvertes. Les applications identiques

$$U'_k \times U'_{k'} \longrightarrow U_k \times U'_{k'}$$

sont des morphismes radiciels, ce qui montre que la variété $U_k \times U_{k'}$ a même topologie que $U'_k \times U'_{k'}$. On en conclut que la topologie de la pré-variété $T \times T$ est la même que celle de $T' \times T'$, donc que la diagonale y est fermée. Ceci montre que T est une variété. Il est clair que T est l'unique variété admettant T' comme ensemble de points telle que l'application identique $i : T' \longrightarrow T$ soit un morphisme radiciel de hauteur $\leqslant 1$ et que $\mathfrak{n}$ soit le noyau de di .

Les anneaux $\mathfrak{O}_{Q'} = \mathfrak{O}_{Q'}(T)$ étant réguliers comme on l'a vu, T est non singulière.

On notera qu'il résulte immédiatement de la manière dont la variété T a été définie que, si f est un morphisme de T' dans une variété quelconque X tel que $\mathfrak{n}$ soit contenu dans le noyau de df , l'application f est aussi un morphisme de T dans X .

Supposons maintenant que T' soit une variété de groupe et que $\mathfrak{n}$ soit invariant par les translations (à gauche et à droite). Il résulte alors de l'assertion d'unicité que les translations de T' sont des automorphismes de la variété T . Soit, par ailleurs, I l'application identique de $T' \times T'$ sur $T \times T$. Les images réciproques de $\mathfrak{n}$ par les deux projections $T' \times T' \longrightarrow T'$ sont des sous-fibrés $\mathfrak{n}_1$ et $\mathfrak{n}_2$ de l'espace fibré $\mathfrak{T}(T' \times T')$ des vecteurs tangents à $T' \times T'$; il est clair que I est un morphisme radiciel de hauteur $\leqslant 1$ et que le noyau de dI est exactement $\mathfrak{n}_1 + \mathfrak{n}_2$. Soit $\mathfrak{m}$ la multiplication de T' ; considérons $\mathfrak{m}$ comme un morphisme de $T' \times T'$ dans T . Pour tout $t \in T'$, l'application $s \longrightarrow \mathfrak{m}(s , t)$ (resp. $s \longrightarrow \mathfrak{m}(t , s)$ est un morphisme de T dans T ; il en résulte aussitôt que le noyau de $d\mathfrak{m}$ contient $\mathfrak{n}_1$ (resp. $\mathfrak{n}_2$) , donc $\mathfrak{n}_1 + \mathfrak{n}_2$. Ceci montre que $\mathfrak{m}$ est un morphisme de $T \times T$ dans T . On sait qu'il en résulte que l'application $s \longrightarrow s^{-1}$ est un morphisme de T dans T ; T est donc un groupe algébrique.

Soient X et T' des variétés, et soit (x , t') un point de $X \times T'$. Les projections de $X \times T'$ sur ses deux facteurs définissent des isomorphismes π_x de l'anneau local $\mathfrak{O}_x$ de x sur X sur un sous-anneau de l'anneau local $\mathfrak{O}_{(x,t')}$ de (x , t') sur $X \times T'$ et $\pi_{T'}$ de l'anneau local $\mathfrak{O}_{t'}$ de t' sur

T' sur un sous-anneau de $\mathcal{O}_{(x,t')}$. Si $u \in \mathcal{O}_{t'}$, nous dirons que l'élément $\pi_{T'}(u)$ de $\mathcal{O}_{(x,t')}$ provient de u.

PROPOSITION 7. - Soit h un morphisme radiciel de hauteur ≤ 1 d'une variété non singulière T' dans une variété T ; supposons que le noyau de dh soit un sous-fibré du fibré tangent de T'. Soit X une variété, et soit g l'application $(x , t') \longrightarrow (x , h(t'))$ de $X \times T'$ sur $X \times T$. Soient (x , t') un point de $X \times T'$, $(x , t) = g(x , t')$, $\mathcal{O}_{(x,t)}$ l'anneau local de (x , t) identifié à un sous-anneau de l'anneau local $\mathcal{O}_{(x,t')}$ de (x , t'). Il existe alors des éléments $y_1 , \dots , y_r$ de $\mathcal{O}_{(x,t')}$ qui proviennent de certains éléments d'un système de variables uniformisantes sur T' en t' et qui forment une p-base de $\mathcal{O}_{(x,t')}$ sur $\mathcal{O}_{(x,t)}$, et aussi de $R(X \times T')$ sur $R(X \times T)$, il y a des dérivations $\partial/\partial y_i$ $(1 \leq i \leq r)$ de $\mathcal{O}_{(x,t')}$ qui appliquent $\mathcal{O}_{(x,t)}$ sur $\{0\}$ telles que $\partial y_j/\partial y_i = \delta_{ij}$ $(1 \leq i , j \leq r)$.

Cela résulte facilement des résultats précédemment établis.

4. Théorèmes de descente pour les familles algébriques de diviseurs et classes de diviseurs dans le cas d'un revêtement radiciel.

Soient T' une variété non singulière, n un sous-fibré intégrable de $\mathfrak{t}(T')$ et $i : T' \longrightarrow T$ le morphisme canonique sur la variété quotient T de T' par n. Soient X une variété et g le morphisme $g : X \times T' \longrightarrow X \times T$, $g(x , t') = (x , i(t'))$. On désigne par (x , t) le point $g(x , t')$ et on identifie l'anneau local $\mathcal{O}_{x,t}$ à un sous-anneau de $\mathcal{O}_{x,t'}$ par le cohomomorphisme de g.

THÉORÈME 3. (Voir [1], proposition 13, chap. 4). - Soit $\{D_{t'}\}_{t' \in T'}$ une famille algébrique de diviseurs sur X paramétrée par T' telle que pour chaque vecteur tangent $L \in n$, on ait $\langle L , \{D_{t'}\} \rangle = 0$. Alors la famille algébrique de diviseurs $\{D_{t'}\}_{t' \in T'}$ est l'image réciproque par i d'une famille algébrique de diviseurs sur X paramétrée par T.

Soient D le diviseur sur $X \times T$ qui définit la famille algébrique $\{D_{t'}\}_{t' \in T'}$ et f une fonction de définition de D en un point (x_0 , t'_0) de $X \times T'$. D'après la proposition 7, il existe $y_1 , \dots , y_r$ de $\mathcal{O}_{(x_0,t'_0)}$ qui proviennent d'une partie d'un système de variables uniformisantes de l'anneau local $\mathcal{O}_{t'_0}$ de T' en t'_0 et qui forment une p-base de $\mathcal{O}_{x_0,t'_0}$ sur $\mathcal{O}_{x_0,t_0}$ (et aussi de $R(X \times T')$ sur $R(X \times T)$). Soient $\frac{\partial}{\partial y_i}$ $(1 \leq i \leq r)$ les dérivations de $\mathcal{O}_{(x_0,t'_0)}$

nulles sur $\mathcal{O}_{(x_0,t_0)}$ telles que $\frac{\partial}{\partial y_i}(y_j) = \delta_{ij}$ $(1 \leqslant i , j \leqslant r)$ et T'_0 un voisinage affine de t'_0 ou tout y_i est régulier et tel que les $\frac{\partial}{\partial y_i}$ proviennent de sections de $\mathcal{E}(T')$ au dessus de T'_0.

S'il existe, pour tout (x_0 , t'_0), une fonction θ régulière et inversible en (x_0 , t'_0) telle que $f.\theta$ appartienne au sous-corps $R(X \times T)$ de $R(X \times T')$, on voit facilement que le diviseur D provient d'un diviseur sur $X \times T$ et le théorème sera démontré. On va trouver maintenant une telle θ. Chaque $\frac{\partial}{\partial y_i}$ $(1 \leqslant i \leqslant r)$ est une section de h au-dessus de T'_0 ; $\langle \frac{\partial}{\partial y_i} , D \rangle$ représente donc un diviseur additif sur $X \times T'_0$. D'après l'hypothèse, la restriction de $\langle \frac{\partial}{\partial y_i} , D \rangle$ à chaque variété parallèle $X \times t'$ $(t' \in T'_0)$ est le diviseur additif nul. Soit X_0 un voisinage affine de x_0 ; comme $H'(X_0 \times T'_0 , \mathcal{O}) = 0$, (voir [4], ou théorème 3, p. 230, [S1]), chaque classe de diviseurs additifs sur $X_0 \times T'_0$ est triviale. Par conséquent, il existe une fonction h_i de $R(X \times T')$ telle que h_i soit une fonction de définition de $\langle \frac{\partial}{\partial y_i} , D \rangle$ en chaque point de $X_0 \times T'_0$. La fonction h_i possède la propriété que sa restriction à chaque variété parallèle $X_0 \times t'$ $(t' \in T'_0)$ est régulière. Il en résulte que h_i est régulière dans $X_0 \times T'_0$; en effet, h_i définit une famille algébrique de diviseurs (multiplicatifs) positifs sur X_0 paramétrée par T'_0 et en appliquant le théorème 1, exposé 5, on voit que le diviseur sur $X_0 \times T'_0$ qui définit cette famille est lui-même positif, ce qui implique que h_i est régulière dans $X_0 \times T'_0$. Comme $\frac{\partial f}{\partial y_i}/f$ est aussi une fonction de définition de $\langle \frac{\partial}{\partial y_i} , D \rangle$ en (x_0 , t'_0), il en résulte que $\frac{\partial f}{\partial y_i}/f$ est régulière en (x_0 , t'_0). Donc la forme

$$\omega = \frac{df}{f} = \frac{\sum \frac{\partial f}{\partial y_i} dy_i}{f}$$

est régulière en (x_0 , t'_0). On a évidemment $d\omega = 0$, $C\omega = \omega$ (on opère sur les formes différentielles de $\Omega'(R(X \times T')/R(X \times T))$ et de plus, en appliquant le théorème 1, on voit qu'il existe un élément inversible θ de $\mathcal{O}_{x_0,t'_0}$ tel que $\frac{d\theta}{\theta} = \omega$. Si l'on pose $g = f\theta$, g est aussi une fonction de définition de D en (x_0 , t'_0) et en plus, on a $dg = 0$, ce qui implique que g appartient à $\mathcal{O}_{x_0,t_0}$.

C. Q. F. D.

THÉORÈME 4 (voir [1], proposition 14, chapitre 4). - Soient T', T, i, X comme dans le théorème précédent et de plus X complète. Soit $\{\lambda_{t'}\}_{t' \in T'}$

une famille algébrique de classes de diviseurs sur X paramétrée par T' telle que pour chaque vecteur tangent $L \in \mathfrak{n}$, on ait $\langle L , \{\lambda_{t'}\} \rangle = 0$. Alors $\{\lambda_{t'}\}_{t' \in T'}$ est l'image réciproque par i d'une famille algébrique de classes de diviseurs sur X paramétrée par T.

Soit λ une classe de diviseurs sur $X \times T'$ qui définit la famille algébrique $\{\lambda_{t'}\}_{t' \in T'}$; d'après le théorème de recollement (théorème 5, exposé 5), il suffit de montrer que pour chaque point de T', il existe un voisinage ouvert T'_0 tel que λ provienne d'une classe de diviseurs sur $X \times i(T'_0)$. En fait, on va démontrer qu'étant donné un point t'_0 de T' il existe un voisinage affine de t'_0 et un diviseur D sur $X \times T'_0$ dans la classe λ tels que la famille algébrique de diviseurs sur X définie par D (et paramétrée par T'_0) satisfasse aux hypothèses du théorème précédent (i. e. pour chaque vecteur tangent $L \in \mathfrak{n}$ en un point de T'_0, $\langle L , D \rangle = 0$). Alors le théorème sera démontré.

Soit, comme dans le théorème précédent, y_i $(1 \leq i \leq r)$ une p-base de l'anneau local $\mathcal{O}_{x_0,t'_0}$ sur $\mathcal{O}_{x_0,t_0}$ (x_0 étant un point choisi de X) ; choisissons un ouvert affine T'_0 de t'_0 de telle sorte que les y_i $(1 \leq i \leq r)$ soient régulières sur T'_0 et que les dérivations $\frac{\partial}{\partial y_i}$ $(1 \leq i \leq r)$ forment une base de $\mathfrak{n}$ sur T'_0. On peut choisir T'_0 et un diviseur D_1 sur $X \times T'_0$ dans la classe λ de telle sorte que la restriction de D_1 à la sous-variété $x_0 \times T'_0$ soit définie et nulle. On suppose que ce choix est fait.

D'après l'hypothèse, la classe de diviseurs additifs $\langle \frac{\partial}{\partial y_i} , \lambda \rangle$ sur $X \times T'_0$ possède la propriété que sa restriction à chaque $X \times t$ $(t \in T'_0)$ est la classe de diviseurs additifs triviale. Ceci implique que la classe de diviseurs $\langle \frac{\partial}{\partial y_i} , \lambda \rangle$ sur $X \times T'_0$, elle-même est triviale ; en effet, soit plus généralement[1] μ un élément de $H^1(X \times T'_0 , \mathcal{O})$ tel que sa restriction à chaque $X \times t$, (voir [2], lemme 1, paragraphe 3, chapitre IV ; voir aussi [3]), $(t \in T'_0)$ soit nulle. Alors en appliquant le théorème de Künneth, on a

$$H^1(X \times T'_0 , \mathcal{O}) = H^0(X , \mathcal{O}) \otimes_K H^1(T'_0 , \mathcal{O}) + H^1(X , \mathcal{O}) \otimes_K H^0(T'_0 , \mathcal{O}) .$$

Puisque T'_0 est affine, $H^1(T'_0 , \mathcal{O}) = 0$ (cf. [4], ou [8], théorème 3, p. 238) ; donc

$$H^1(X \times T'_0 , \mathcal{O}) = H^1(X , \mathcal{O}) \otimes_K H^0(T'_0 , \mathcal{O}) .$$

Donc on peut exprimer l'élément μ sous la forme $\sum_{i=0}^{s} \theta_i(t) Z_i$, les θ_i étant des fonctions régulières sur T'_0 et $Z_1 , \dots , Z_s$ formant une partie finie d'une <u>base</u> de $H^1(X, \mathcal{O})$ sur K (il n'est pas nécessaire ici de supposer X complète). Pour chaque t fixe de T'_0, $\sum_{i=0}^{s} \theta_i(t) Z_i$ est l'élément zéro de $H^1(X, \mathcal{O})$ d'après l'hypothèse faite sur μ, ce qui implique que $\theta_i(t) = 0$ pour chaque i et $t \in T'_0$. Donc $\mu = 0$ et, en particulier, les classes de diviseurs additifs $\langle \frac{\partial}{\partial y_i}, \lambda \rangle$ sur $X \times T'_0$ sont triviales. Par conséquent, les <u>diviseurs additifs</u> $\langle \frac{\partial}{\partial y_i}, D_1 \rangle$ sur $X \times T'_0$ peuvent être représentés par des fonctions g_i $(1 \leq i \leq r)$ sur $X \times T'_0$ tout entier.

Comme on a supposé que la restriction de D_1 à $x_0 \times T'_0$ est définie et triviale, chaque g_i possède la propriété que sa restriction à $x_0 \times T'_0$ est régulière. Donc pour chaque g_i il existe une fonction régulière h_i sur $X \times T'_0$ qui provient d'une fonction régulière de T'_0 telle que la restriction de $g_i + h_i$ à $x_0 \times T'_0$ soit nulle. Par conséquent, on peut supposer que le diviseur additif principal $\langle \frac{\partial}{\partial y_i}, D_1 \rangle$ est représenté par une fonction g_i telle que la restriction de g_i à $x_0 \times T'_0$ soit nulle.

Soit $\omega = \sum g_i \, dy_i$, $\omega \in \Omega^1(R(X \times T')/R(X \times T))$. S'il existe une fonction h du corps $R(T')$ telle que $\frac{dh}{h} = \omega$, alors pour le diviseur $D = D_1 - \operatorname{div} h$, on aura $\langle \frac{\partial}{\partial y_i}, D \rangle = 0$ pour chaque $\frac{\partial}{\partial y_i}$ et le théorème sera démontré en appliquant le théorème précédent. Pour trouver une telle fonction h, il s'agit de démontrer que $d\omega = 0$ et $C\omega = \omega$ ou encore (voir le théorème 1) que

$$\frac{\partial}{\partial y_i}(g_j) - \frac{\partial}{\partial y_j}(g_i) = \lambda_{ij}(\omega) = 0$$

$$\left(\frac{\partial}{\partial y_i}\right)^{p-1}(g_i) + g_i^p = \mu_i(\omega) = 0$$

D'abord on voit sans difficulté que λ_{ij}, μ_i sont des fonctions rationnelles sur $X \times T'_0$ dont les restrictions à $x_0 \times T'_0$ sont définies et nulles. Par ailleurs, si f est une fonction de définition de D_1 en un point (x, t') de $X \times T'_0$; les fonctions $(g_i - \frac{\partial f}{\partial y_i}/f)$ $(1 \leq i \leq r)$ sont régulières en (x, t'). Si l'on pose

$$\omega_1 = \sum \left(\frac{\partial f}{\partial y_i}/f\right) dy \quad ;$$

on a évidemment $C\omega_1 = \omega_1$, $d\omega_1 = 0$ et ceci entraîne que $\lambda_{ij}(\omega_1) = 0$, $\mu_i(\omega_1) = 0$. Mais on a

$$\lambda_{ij}(\omega) = \lambda_{ij}(\omega - \omega_1) + \lambda_{ij}(\omega_1)$$

$$\mu_i(\omega) = \mu_i(\omega - \omega_1) + \mu_i(\omega_1)$$

et en plus

$$\lambda_{ij}(\omega - \omega_1)\ , \quad \mu_i(\omega - \omega_1)$$

sont régulières en $(x\ ,\ t')$. Par conséquent λ_{ij} et μ_i sont régulières en $(x\ ,\ t')$ et donc en chaque point de $X \times T'_0$. Puisqu'elles s'annulent sur $x_0 \times T'_0$, elles sont nulles partout.

REMARQUE. - Soient T' , T deux variétés, $i : T' \longrightarrow T$ un morphisme de revêtement radiciel de T' sur T de hauteur $\leqslant 1$ et $\{\lambda_{t'}\}_{t' \in T'}$ une famille algébrique de diviseurs (resp. classes de diviseurs) sur une variété X (resp. une variété complète X) paramétrée par T' . Supposons que, pour chaque vecteur tangent L de T' tel que $di(L) = 0$, on ait $\langle L\ ,\ \{\lambda_{t'}\}\rangle = 0$ (resp. $\langle L\ ,\ \{\lambda_{t'}\}\rangle = 0$ comme une classe de diviseurs additifs), alors, d'après les théorèmes 3 et 4 , la famille algébrique $\{\lambda_{t'}\}_{t' \in T'}$ se descend à T pour un <u>ouvert</u> (non vide) de T' puisqu'on peut voir facilement que les hypothèses des théorèmes 3 et 4 sont satisfaites sur un ouvert de T' .

5. <u>Le théorème de Cartier en caractéristique</u> $p > 0$ ([2], chapitre 4 , paragraphe 4).

On se restreint encore aux variétés définies sur un corps K algébriquement clos de caractéristique $p > 0$.

Soient X une variété complète et $f : G \longrightarrow \mathfrak{C}(X)$ un homomorphisme algébrique d'une variété de groupe dans le groupe des classes de diviseurs sur X . On rappelle que si L est un vecteur tangent de G , $\langle L\ ,\ f\rangle$ est un élément de $H^1(X\ ,\ \mathcal{O})$ et que si λ est un champ de vecteurs sur G , $\langle \lambda\ ,\ f\rangle$ est un élément de $H^1(X \times G\ ,\ \mathcal{O})$. Soit $l_a : G \longrightarrow G$ (resp. $r_a : G \longrightarrow G$) le morphisme de translation à gauche (resp. à droite) par l'élément a de G .

PROPOSITION 8. - <u>Soit</u> L_a <u>un vecteur tangent à</u> G <u>en un point</u> a <u>de la forme</u> $(dl_a)(L_e)$ (resp. $dr_a(L_e)$), L_e <u>étant un vecteur tangent à</u> G <u>en l'élément neutre ; alors on a</u>

$$\langle L_a\ ,\ f\rangle = \langle L_e\ ,\ f\rangle \quad .$$

D'après l'analogue de la proposition 4 , exposé 5 , pour une famille algébrique de classes de diviseurs, on a

$$\langle dl_a(L_e)\ ,\ f\rangle = \langle L_e\ ,\ l_a^*(f)\rangle \qquad (\text{resp. } \langle dr_a(L_e)\ ,\ f\rangle = \langle L_e\ ,\ r_a^*(f)\rangle\ )$$

$l_a^*(f)$ (resp. $r_a^*(f)$) étant l'image réciproque par l_a (resp. r_a) de la famille algébrique définie par f. Mais on a :

$$l_a^*(f)(x) = f(x) + f(a) \quad (\text{resp. } r_a^*(f)(x) = f(x) + f(a)) , \; x \in G \quad ;$$

ce qui implique que l'application algébrique $f - l_a^*(f)$ (resp. $f - r_a^*(f)$) de G dans $\mathfrak{G}(X)$ est constante. Il en résulte que

$$\langle L_e , l_a^*(f) \rangle = \langle L_e , f \rangle \quad (\text{resp. } \langle L_e , r_a^*(f) \rangle = \langle L_e , f \rangle) \quad .$$

La proposition 8 est donc établie.

REMARQUE. - Soient p , q les projections de $X \times G$ sur X et G respectivement et λ un champ de vecteurs invariant (soit à gauche, soit à droite, soit les deux à la fois) sur G. Alors la proposition implique qu'il existe un élément α de $H^1(X , \mathcal{O})$ tel que la restriction de $\langle \lambda , f \rangle - p^*(\alpha)$ à chaque variété parallèle $X \times g$, $(g \in G)$, soit nulle. Comme on a vu dans la démonstration du théorème 4 , il en résulte que pour chaque ouvert affine T de G , la restriction de $\langle \lambda , f \rangle - p^*(\alpha)$ à $X \times T$ est nulle. Ceci entraîne, en vertu de la formule de Künneth et puisque X est complète, qu'il y a un élément $\beta \in H^1(G , \mathcal{O})$ tel que

$$\langle \lambda , f \rangle = p^*(\alpha) + q^*(\beta) \quad .$$

D'autre part, on voit aussi que pour chaque vecteur tangent L de λ, $\langle L , f \rangle = 0$ si (et seulement si) $\langle \lambda , f \rangle$ est de la forme $q^*(\beta)$, $\beta \in H^1(G , \mathcal{O})$.

PROPOSITION 9. - Soient λ_1 , λ_2 deux champs de vecteurs invariants sur G (à gauche ou à droite ou les deux à la fois). Alors il existe β , β_1 de $H^1(G , \mathcal{O})$ tels que

(1) $$\langle \lambda_1^p , f \rangle = \langle \lambda_1 , f \rangle^p + q^*(\beta)$$

(2) $$\langle [\lambda_1 , \lambda_2] , f \rangle = q^*(\beta_1) \quad .$$

En particulier, les vecteurs tangents L à G tels que $\langle L , f \rangle = 0$ forment un sous-fibré intégrable et invariant de l'espace fibré $\mathfrak{t}(G)$ des vecteurs $\mathfrak{t}(G)$ sur G .

Soit θ une classe de diviseurs sur $X \times G$ qui définit l'application algébrique $f : G \longrightarrow \mathfrak{G}(X)$ et $\{\theta_{ij}\}$ un système de fonctions de transition de θ relative à un recouvrement $\{U_i\}$ de $X \times G$. Alors la classe de diviseurs additifs $\langle \lambda_1 , f \rangle$ est définie par les fonctions de transition

$\dfrac{\lambda_1(\theta_{ij})}{\theta_{ij}}$ relative au même recouvrement. En appliquant le lemme 2 , on trouve que

$$\frac{\lambda_1^p(\theta_{ij})}{\theta_{ij}} - \left(\frac{\lambda_1(\theta_{ij})}{\theta_{ij}}\right)^p = \lambda_1^{p-1}\left(\frac{\lambda_1(\theta_{ij})}{\theta_{ij}}\right) .$$

Les fonctions de transition

$$\left\{\frac{\lambda_1^p(\theta_{ij})}{\theta_{ij}}\right\} \quad \text{et} \quad \left\{\left(\frac{\lambda_1(\theta_{ij})}{\theta_{ij}}\right)^p\right\}$$

(relatives à $\{U_i\}$) définissent respectivement les diviseurs additifs $\langle \lambda_1^p , f\rangle$ et $\langle \lambda_1 , f\rangle^p$. Donc pour (1) il s'agit de démontrer que la classe de diviseurs additifs définie par les fonctions de transition

$$\left\{\lambda_1^{p-1}\left(\frac{\lambda_1(\theta_{ij})}{\theta_{ij}}\right)\right\}$$

est de la forme $q^*(\beta)$, $\beta \in H^1(G , \mathcal{O})$. D'après la proposition 8 , la classe de diviseurs additifs définie par les fonctions de transition $\left\{\dfrac{\lambda_1(\theta_{ij})}{\theta_{ij}}\right\}$ est de la forme $p^*(\alpha) + q^*(\beta)$, $\alpha \in H^1(X , \mathcal{O})$, $\beta \in H^1(G , \mathcal{O})$. Donc la classe de diviseurs additifs définie par les fonctions de transition $\lambda_1\left(\dfrac{\lambda_1(\theta_{ij})}{\theta_{ij}}\right)$ est de la forme $q^*(\beta)$, $\beta \in H^1(G , \mathcal{O})$ et a fortiori la classe de diviseurs additifs définie par les fonctions de transition $\lambda_1^{p-1}\left(\dfrac{\lambda_1(\theta_{ij})}{\theta_{ij}}\right)$. Ceci démontre (1).

On a maintenant l'identité suivante :

$$\frac{[\lambda_1 , \lambda_2](\theta_{ij})}{\theta_{ij}} = \lambda_1\left(\frac{\lambda_2(\theta_{ij})}{\theta_{ij}}\right) - \lambda_2\left(\frac{\lambda_1(\theta_{ij})}{\theta_{ij}}\right) .$$

Comme on l'a vu pour démontrer (1) , les classes de diviseurs additifs définies respectivement par les fonctions de transition $\left\{\dfrac{\lambda_1(\theta_{ij})}{\theta_{ij}}\right\}$ et $\left\{\dfrac{\lambda_2(\theta_{ij})}{\theta_{ij}}\right\}$ sont de la forme $p^*(\alpha) + q^*(\beta)$, $\alpha \in H^1(X , \mathcal{O})$ et $\beta \in H^1(G , \mathcal{O})$ et alors l'identité ci-dessus entraîne (2).

C. Q. F. D.

THÉORÈME 5. - Soient X une variété complète et $f : G \longrightarrow \mathfrak{G}(X)$ un homomorphisme algébrique, G étant une variété de groupe. Alors on peut construire une variété de groupe H et un homomorphisme $q : G \longrightarrow H$ de revêtement radiciel tels que

1° Si $\mathfrak{n}$ est le noyau de l'application $\sigma(f) : \mathfrak{t}(G) \longrightarrow H^1(U, \mathcal{O})$, $\mathfrak{n}$ coïncide avec le noyau de l'application différentielle $dq : \mathfrak{t}(G) \longrightarrow \mathfrak{t}(H)$.

2° L'homomorphisme algébrique f se descend en un homomorphisme algébrique $f' : H \longrightarrow \mathfrak{G}(X)$, i. e. on a $f = f' \circ q$.

D'après la proposition 9, $\mathfrak{n}$ est un sous-fibré intégrable invariant de $\mathfrak{t}(G)$. Donc, en vertu du théorème 2, on peut construire une variété de groupe H et un homomorphisme $q : G \longrightarrow H$ de revêtement radiciel (de hauteur 1) tels que le noyau de l'application différentielle dq soit $\mathfrak{n}$. Maintenant il résulte du théorème 4, que f se descend en un homomorphisme algébrique $f' : H \longrightarrow \mathfrak{G}(X)$, (voir aussi [2], chapitre 4, paragraphe 4, théorème 1).

6. Le théorème de Cartier en caractéristique 0.

Pour démontrer le théorème de Cartier en caractéristique 0, on peut supposer que le corps de base est le corps de nombres complexes $\mathbb{C}$.

THÉORÈME 5'. - Soient X une variété complexe définie sur $\mathbb{C}$ et $f : G \to \mathfrak{G}(X)$ un homomorphisme algébrique injectif, G étant une variété de groupe définie sur $\mathbb{C}$. Alors l'application linéaire canonique

$$\sigma(f) : \mathfrak{t}_e(G) \longrightarrow H^1(X, \mathcal{O})$$

est injective.

Supposons qu'il y ait un vecteur tangent à G en son élément neutre e dont l'image par $\sigma(f)$ soit nulle. Soit λ le champ de vecteurs invariant à gauche sur G tel que $\lambda(e) = L$, on a alors $\langle \lambda(s), f \rangle = 0$ pour tout $s \in G$ (cf. proposition 8, paragraphe 4). Le symbole $\langle \lambda, f \rangle$ représente une classe de diviseurs additifs sur $X \times G$; cette classe induit 0 sur $X \times s$ si $s \in G$. Procédant comme dans la démonstration du théorème 4, paragraphe 3, on voit que, pour tout morceau affine T de G, la classe de diviseurs additifs induite par $\langle \lambda, f \rangle$ sur $X \times T$ est nulle. Nous choisirons un morceau affine T_0 de G contenant e tel que la restriction de f à T_0 puisse être définie par un diviseur D sur $X \times T_0$. Si λ_0 est la restriction de λ à T_0 le diviseur additif $\langle \lambda_0, D \rangle$ sur $X \times T_0$ est principal. Nous pouvons associer à D un diviseur analytique D^h sur l'espace analytique $X \times T_0$. Il y a un voisinage ouvert T_1 de e dans la variété analytique T_0 et un recouvrement ouvert fini (U_i) de l'espace analytique X (qui est compact) tels que, pour chaque i, le diviseur induit par D sur $U_i \times T_1$ soit représenté par une fonction méromorphe f_i sur $U_i \times T_1$; on peut de plus supposer qu'il y a un système de coordonnées $(z_1 , \dots , z_n)$ sur la variété analytique T_1 tel que la restriction λ_1 de λ à T_1 soit le champ de vecteurs $\partial/\partial z_1$ et que l'image de T_1 par l'application $s \longrightarrow (z_1(s) , \dots , z_n(s))$ soit un ensemble convexe de $\underset{\sim}{C}^n$; on peut de plus supposer que $z_i(e) = 0$. Le diviseur analytique additif $\langle \lambda_0 , D^h \rangle$, qui est le diviseur analytique associé au diviseur additif $\langle \lambda_0 , D \rangle$, est principal. On en déduit qu'il existe une fonction méromorphe g sur $X \times T_1$ telle que, pour chaque i ,

$$h_i = f_i^{-1} \frac{\partial f_i}{\partial z_1} - g$$

soit holomorphe sur $U_i \times T_1$. On peut représenter h_i sous la forme $\partial h_i'/\partial z_1$, h_i' étant une fonction holomorphe sur $U_i \times T_1$; posant $f_i' = f_i\, e^{-h_i'}$, on a $f_i'^{-1}(\partial f_i'/\partial z_1) = g$ sur $U_i \times T_1$. De plus, la restriction de D_i à $U_i \times T_1$ est représentée par f_i' . Posons $f_i''(x , s) = f_i'(x , s)\, f_i'^{-1}(x , e)$ (il est clair que f_i' est définie en au moins un point de $U_i \times e$). On a alors

$$(f_i'')^{-1}\, \partial f_i''/\partial z_1 = (f_j'')^{-1}\, \partial f_j''/\partial z_1$$

dans $(U_i \cap U_j) \times T_1$ et

$$(f_i''/f_j'')(x , e) = 1 \quad (x \in U_i \cap U_j) \quad .$$

Si z est assez voisin de 0 , soit $s(z)$ le point de T_1 de coordonnées $(z , 0 , \dots , 0)$; on voit alors que $f_i''(x , s(z))$ et $f_j''(x , s(z))$ coïncident sur $U_i \cap U_j$. Or, pour chaque $t \in T_1$, soit D_t l'image réciproque de D par l'application $x \longrightarrow (x , t)$; pour t donné, les fonctions $x \longrightarrow f_i''(x , t)$ représentent $D_t - D_e$ dans les U_i ; on voit donc que $D_{s(z)} - D_e$ est principal, d'où $f(s(z)) = f(e)$, en contradiction avec l'hypothèse que f est injectif.

BIBLIOGRAPHIE.

[1] CARTIER (Pierre). - Questions de rationalité des diviseurs en géométrie algébrique, Bull. Soc. math. France, t. 86, 1958, p. 177-251 (Thèse Sc. math. Paris. 1958).

[2] CARTIER (Pierre). - Isogénies des variétés de groupes, Bull. Soc. math. France, t. 87, 1959 (à paraître) (Thèse Sc. math. Paris. 1958, Chapitre 4).

[3] GODEMENT (Roger). - Topologie algébrique et théorie des faisceaux. - Paris, Hermann, 1958 (Act. scient. et ind., 1252 ; Publ. Inst. Math. Univ. Strasbourg, 13).

[4] GROTHENDIECK (Alexander). - Sur les faisceaux algébriques et les faisceaux analytiques cohérents, Séminaire Cartan, t. 9, 1956/57 : Quelques questions de topologie, n° 2.

[5] HOCHSCHILD (G.). - Simple algebras with purely inseparable splitting fields of exponent 1 , Trans. Amer. math. Soc., t. 79, 1955, p. 477-489.

[6] Séminaire H. CARTAN, t. 4, 1951/52 : Fonctions analytiques de plusieurs variables complexes.

[7] Séminaire SCHWARTZ, t. 1, 1953/54 : Produits tensoriels topologiques d'espaces vectoriels topologiques, Espaces vectoriels topologiques nucléaires, Applications.

[8] SERRE (Jean-Pierre). - Faisceaux algébriques cohérents, Annals of Math., Series 2, t. 61, 1955, p. 197-278.

[9] SERRE (Jean-Pierre). - Géométrie algébrique et géométrie analytique, Ann. Inst. Fourier Grenoble, t. 6, 1955-56, p. 1-42.