BULLETIN DE LA S. M. F.

PIERRE CARTIER

Isogénies des variétés de groupes

Bulletin de la S. M. F., tome 87 (1959), p. 191-220

<http://www.numdam.org/item?id=BSMF_1959__87__191_0>

Bull. Soc. math. France,
87, 1959, p. 191 à 220.

ISOGÉNIES DES VARIÉTÉS DE GROUPES;

PAR

PIERRE CARTIER
(Paris).

TABLE DES MATIÈRES.

INTRODUCTION.

Dans cet article, nous proposons une théorie des isogénies de variétés de groupes qui permette d'aller plus loin que les méthodes galoisiennes. En

fait, notre théorie est une synthèse de la théorie usuelle des isogénies séparables, et de la théorie des isogénies radicielles de hauteur 1 élaborée par I. BARSOTTI ([1]). On montrera d'ailleurs comment notre théorie redonne les deux cas particuliers précédents.

La nécessité d'une théorie générale des isogénies est manifeste dans un article que nous avons publié antérieurement sur la dualité des variétés abéliennes ([2]); dans cet article, nous nous étions contenté de donner les définitions et résultats strictement requis par le sujet principal, mais la lecture simultanée de cet article et du présent Mémoire peuvent éclairer l'un et l'autre.

Les démonstrations, dans ce qui suit, sont de caractère élémentaire, et n'utilisent que les définitions de base de la géométrie algébrique, telles qu'elles sont résumées au chapitre 1 de notre thèse ([3]), et les résultats courants de la théorie des corps; encore avons-nous redonné au n° 2 du chapitre 2 une démonstration du théorème de Jacobson-Bourbaki sur la correspondance entre sous-corps d'un corps fixe et certains anneaux de transformations linéaires. Le chapitre 1 contient des résultats généraux sur les variétés de groupes, dont les uns sont très élémentaires et bien connus, et ne sont insérés ici que pour la cohérence de l'exposé, et dont les autres sont des conséquences aisées des résultats de A. WEIL sur la construction birationnelle des variétés de groupes. Le chapitre 2 commence par une discussion des cocycles rationnels du groupe $GL(n)$; ces résultats ont été publiés sous une forme plus complète par E. KOLCHIN et S. LANG ([4]). Après avoir redémontré le théorème cité de Jacobson-Bourbaki, nous abordons dans les numéros 3 à 5 les principaux résultats de cet article; les numéros 6 et 7 contiennent des compléments sur les isogénies séparables et les isogénies radicielles de hauteur 1.

Nos méthodes sont celles de la géométrie birationnelle. Cependant, tout semble indiquer que pour dépasser les résultats exposés ici, il faille utiliser le point de vue birégulier et la théorie des schémas de A. GROTHENDIECK; de fait ce n'est que dans ce cadre qu'on peut exposer commodément un théorème de dualité entre les « noyaux généralisés » de deux isogénies transposées de variétés abéliennes, théorème qui étend la « dualité de WEIL-TATE » bien connue dans le cas séparable. Contentons-nous d'indiquer comment on peut définir notre algèbre $\mathbf{N}_k(\alpha)$ pour une k-isogénie α dans ce cadre. Si $\alpha : G \to G'$ est une k-isogénie, l'image directe par α du faisceau des anneaux locaux de la k-variété G est un faisceau localement libre d'algèbres sur G'; il lui correspond donc un fibré algébrique A localement trivial de

([1]) *Cf.* l'exposé de J.-P. SERRE, *Quelques propriétés des variétés abéliennes en caractéristique p* (*Amer. J. Math.*, t. 80, 1958, p. 715-739).

([2]) *Isogenies and duality of abelien varieties* (*Ann. Math.*, à paraître).

([3]) *Questions de rationalité des diviseurs en géométrie algébrique* (*Bull. Soc. math. Fr.*, t. 86, 1958, p. 177-251 (Thèse Sc. math., Paris, 1958)).

([4]) *Existence of invariant basis* (à paraître).

base G' et dont les fibres sont des algèbres. Notre algèbre $\mathbf{N}_k(\alpha)$ est comme espace vectoriel le dual de la fibre A_e en e du fibré précédent sur G'; la multiplication et l'application diagonale dans $\mathbf{N}_k(\alpha)$ sont respectivement transposées de l'application diagonale et de la multiplication dans A_e. D'ailleurs, on peut généraliser la construction précédente pour définir le noyau d'un homomorphisme quelconque de variétés de groupes; ce noyau sera une « variété algébrique avec éléments nilpotents » au sens de A. GROTHENDIECK; il reste là de nombreux problèmes à éclaircir.

NOTATIONS. — Elles sont strictement conformes à celles du chapitre 1 de ma thèse.

Le domaine universel est noté $\mathbf{K}$; une k-variété est une variété définie sur le corps k; un morphisme (resp. k-morphisme) est une application rationnelle partout régulière (resp. et définie sur k); si f est une fonction rationnelle, on note $D(f)$ l'ensemble des points où elle est régulière; le composé de deux applications rationnelles u et v, lorsqu'il est défini, est noté $v \odot u$; enfin $R(X)$ [resp. $R_k(X)$] est le corps des fonctions rationnelles sur la variété X [resp. des fonctions définies sur k], et $\mathfrak{O}_k(x/X)$ le sous-anneau de $R_k(X)$ formé des fonctions régulières au point x de X. Lorsqu'on ne précise pas, la topologie utilisée sur une variété est la $\mathbf{K}$-topologie.

Une k-variété de groupe G est un ensemble muni d'une loi de groupe et d'une structure de k-variété telles que l'application $(g, g') \to g^{-1}.g'$ de $G \times G$ dans G soit un morphisme. Pour tout $g \in G$, on note γ_g la translation à gauche $g' \to g.g'$ et δ_g la translation à droite $g \to g'.g$; ce sont tous deux des automorphismes de G pour sa structure de variété.

CHAPITRE 1.

GÉNÉRALITÉS SUR LES VARIÉTÉS DE GROUPES.

1. Fonctions de deux variables. — Nous démontrerons d'abord un certain nombre de résultats auxiliaires sur les fonctions rationnelles de deux variables.

Soient X et Y deux k-variétés. On identifiera $R(X)$ et $R(Y)$ à des sous-corps de $R(X \times Y)$ au moyen des projections de $X \times Y$ sur ses facteurs.

a. Soit $f \in R_k(X \times Y)$; si l'on pose $D(f) \cap (X \times y) = U_y \times y$ pour $y \in Y$, l'ensemble U_y est ouvert dans X et l'ensemble Y_1 des $y \in Y$ tels que U_y soit non vide est un k-ouvert non vide de Y car $D(f)$ est un k-ouvert non vide. Pour $y \in Y_1$, on notera $f(\bigstar ; y)$ la fonction rationnelle sur X prenant la valeur $f(x, y)$ en $x \in U_y$; si $f \not\equiv 0$, l'ensemble des $y \in Y$ tels que $D(f^{-1}) \cap D(f) \cap (X \times y)$ soit non vide est un k-ouvert non vide Y_2 de Y et l'on a évidemment $f(\bigstar ; y) \not\equiv 0$ pour $y \in Y_2$.

LEMME 1. — *Soient f et f' deux éléments de $R_k(X \times Y)$. S'il existe un ensemble E partout dense dans Y pour la k-topologie et tel que*

$$f(\bigstar ; y) = f'(\bigstar ; y)$$

pour tout $y \in E$ donnant un sens aux termes de cette égalité, alors $f = f'$.

En effet, supposons $f \neq f'$; il existe alors un k-ouvert non vide V de Y tel que $f(\bigstar ; y)$ soit défini pour $y \in V$, un k-ouvert non vide V' de Y tel que $f'(\bigstar ; y)$ soit défini pour $y \in V'$, et un k-ouvert non vide W de Y tel que $(f - f')(\bigstar ; y)$ soit défini et non nul pour $y \in W$. Comme Y est irréductible et E partout dense dans Y pour la k-topologie, l'ensemble $T = E \cap V \cap V' \cap W$ est non vide. D'après la formule :

$$(f - f')(\bigstar ; y) = f(\bigstar ; y) - f'(\bigstar ; y), \tag{1}$$

on a donc $f(\bigstar ; y) \neq f'(\bigstar ; y)$ pour $y \in T$, ce qui est absurde puisque $T \subset E$.

C. Q. F. D.

b. Soit $y \in Y$; l'application $x \to (x, y)$ de X sur $X \times y$ est un isomorphisme de variétés, et par suite $X \times y$ est **K**-irréductible et *a fortiori* k-irréductible dans $X \times Y$. Posons $\mathfrak{O} = \mathfrak{O}_k(X \times y / X \times Y)$; alors $\mathfrak{O}$ se compose des $f \in R_k(X \times Y)$ telles que $f(\bigstar ; y)$ soit définie, et l'application $\zeta : f \to f(\bigstar ; y)$ est un homomorphisme d'anneau de $\mathfrak{O}$ dans $R(X)$. De plus on a

$$\zeta(f) = f \quad \text{pour } f \in R_k(X) ; \qquad \zeta(g) = g(y) \quad \text{pour } g \in \mathfrak{O}_k(y/Y). \tag{2}$$

Mais si A est le sous-anneau de $R_k(X \times Y)$ engendré par $R_k(X)$ et $\mathfrak{O}_k(y/Y)$, tout élément de $\mathfrak{O}$ est de la forme f/f', avec $f, f' \in A$ et $1/f' \in \mathfrak{O}$. Il en résulte que les conditions (2) caractérisent l'homomorphisme ζ et que l'image de ζ est contenue dans le corps $R_{k(y)}(X)$; autrement dit, si f appartient à $R_k(X \times Y)$, on a $f(\bigstar ; y) \in R_{k(y)}(X)$ chaque fois que $f(\bigstar ; y)$ est définie.

c. Soient L un sous-corps de $R_k(X)$ et M le sous-corps de $R_k(X \times Y)$ engendré par L et $R_k(Y)$.

LEMME 2. — *Soient $f \in M$ et $y \in Y$ tels que $f(\bigstar ; y)$ soit définie. Alors $f(\bigstar ; y)$ appartient au sous-corps de $R(X)$ engendré par L et $k(y)$.*

Posons $\mathfrak{O} = \mathfrak{O}_k(X \times y / X \times Y)$ et $\mathfrak{o} = \mathfrak{O}_k(y/Y)$, $F = R_k(X)$, $A = F[\mathfrak{o}]$ et $B = L[\mathfrak{o}]$; enfin notons $\mathfrak{m}$ l'idéal maximal de $\mathfrak{o}$ et posons $\mathfrak{p} = \mathfrak{m} . A \cap B$. L'anneau $(F \otimes \mathfrak{o})/(F \otimes \mathfrak{m})$, étant isomorphe à $F \otimes (\mathfrak{o}/\mathfrak{m})$, est intègre puisque F est extension régulière de k. Mais l'application k-linéaire de $F \otimes \mathfrak{o}$ **dans A** qui associe $f.f'$ à $f \otimes f'$ est bijective, donc l'idéal $F.\mathfrak{m} = A.\mathfrak{m}$ de A

est premier De plus, d'après les propriétés des variétés-produit, on a $\mathfrak{O} = A_{\mathfrak{m}.A}$.

L'idéal maximal de $\mathfrak{O}$ se compose des fonctions qui induisent o sur l'ensemble des points de $X \times y$ où elles sont définies, et c'est donc le noyau de ζ; alors $\mathfrak{m}.A = A \cap \mathfrak{m}.A_{\mathfrak{m}.A}$ est l'ensemble des fonctions de A annulées par ζ et, par suite, $\mathfrak{p}$ est l'ensemble des fonctions de B annulées par ζ. Le lemme 2 est alors une conséquence de la formule

$$\mathfrak{O} \cap M = B_{\mathfrak{p}} \tag{3}$$

que nous allons maintenant démontrer.

Il est clair que $B_{\mathfrak{p}}$ est contenu dans $\mathfrak{O} \cap M$. Par ailleurs, soit f un élément non nul de $\mathfrak{O} \cap M$, et soit $\mathfrak{a}$ l'idéal $A \cap A.f^{-1}$ de A et $\mathfrak{b}$ l'idéal $B \cap B.f^{-1}$ de B. Comme $f \in M$ et que M est le corps des fractions de B, il existe b, $b' \in B$ non nuls tels que $f = b/b'$, d'où $b' = f^{-1}.b \in \mathfrak{b}$; de même, comme $f \in \mathfrak{O} = A_{\mathfrak{m}.A}$, il existe $a \in A$ et $s \in A - \mathfrak{m}.A$, avec $f = a/s$ d'où $s = f^{-1}.a \in \mathfrak{a}$; autrement dit, on a $\mathfrak{b} \neq (0)$ et $\mathfrak{a} \not\subset \mathfrak{m}.A$. Comme les corps $R_k(X)$ et $R_k(Y)$ sont linéairement disjoints sur k, les corps $R_k(X)$ et M sont linéairement disjoints sur L (*Cf.* BOURBAKI, *Algèbre*, chap. V, § 2, prop. 7). Soit alors $\{f_i\}$ une base de $R_k(X)$ sur L; c'est donc une base du B-module A puisque B est contenu dans M. Si $a \in \mathfrak{a}$, on a $a \in A$ et $f.a \in A$; il existe donc des éléments b_i, b_i' de B tels que $a = \Sigma b_i.f_i$ et $f.a = \Sigma b_i'.f_i$; on a alors $b_i' = f.b_i$ pour tout i, d'où $b_i' \in \mathfrak{b}$ et $a \in A.\mathfrak{b}$; comme on a évidemment $\mathfrak{b} \subset \mathfrak{a}$, on a donc $\mathfrak{a} = A.\mathfrak{b}$. Si l'on avait $\mathfrak{b} \subset \mathfrak{p}$, on aurait $\mathfrak{a} = A.\mathfrak{b} \subset A.\mathfrak{p} = A.\mathfrak{m}$, ce qui est absurde; il existe, par suite, $s \in \mathfrak{b}$ tel que $s \notin \mathfrak{p}$, d'où $s' = f.s \in B$ et finalement $f = s'/s \in B_{\mathfrak{p}}$. C. Q. F. D.

Le lemme 2 admet la réciproque suivante :

LEMME 3. — *Soient $f \in R_k(X \times Y)$ et E un ensemble partout dense dans Y pour la k-topologie. Si $f(\bigstar ; y)$ est dans $\mathbf{K}(L)$ pour tout $y \in E$ pour lequel $f(\bigstar ; y)$ soit définie, alors f appartient à M.*

On peut supposer $f \neq o$; soit $\{f_i\}_{i \in I}$ une base de $R_k(X)$ sur L; comme le corps $R_k(X \times Y)$ est engendré par $R_k(X)$ et M il existe des éléments m_i, m_i' de M non tous nuls et tels que

$$f = (\Sigma m_i.f_i)/(\Sigma m_i'.f_i) \tag{4}$$

et il y a une partie finie J de I non vide telle que $m_i = m_i' = o$ pour $i \in I - J$. Comme J est finie, il y a un k-ouvert non vide U de Y telle que pour $y \in U$, toutes les fonctions $m_i(\bigstar ; y)$, $m_i'(\bigstar ; y)$ et $f(\bigstar ; y)$ sur X soient définies, et $U \cap E$ est non vide puisque E est partout dense pour la k-topologie. Pour $y \in U \cap E$, on a

$$\Sigma \{f(\bigstar ; y)\, m_i'(\bigstar ; y) - m_i(\bigstar ; y)\}.f_i = o \tag{5}$$

d'après la formule (4), puisque $f_i \in R_k(X)$. D'après l'hypothèse faite sur f et le lemme 2 appliqué aux m_i et m_i', le coefficient de f_i dans (5) appartient à $\mathbf{K}(L)$; mais comme $R_k(X)$ et $\mathbf{K}$ sont linéairement disjoints sur k, les corps $R_k(X)$ et $\mathbf{K}(L)$ sont linéairement disjoints sur L et les f_i sont linéairement indépendants sur $\mathbf{K}(L)$. De (5) on déduit alors

$$m_i(\bigstar\,;y) = (f.m_i')(\bigstar\,;y) \qquad \text{pour} \quad y \in U \cap E \qquad \text{et} \qquad i \in J;$$

mais comme E est partout dense et Y irréductible pour la k-topologie, pour tout k-ouvert U' non vide de Y, on a

$$U' \cap (U \cap E) = (U \cap U') \cap E \neq \emptyset$$

et $U \cap E$ est partout dense dans Y pour la k-topologie. D'après le lemme 1, on a donc $f.m_i' = m_i$ pour $i \in J$ d'où $f \in M$ puisque $J \neq \emptyset$ et que les m_i' ne sont pas tous nuls. C. Q. F. D.

2. **Espaces à opérateurs.** — *Soit G une k-variété de groupe.* On dit que G opère (à droite) sur une k-variété P si l'on s'est donné un k-morphisme $(p, g) \to p.g$ de $P \times G$ dans P vérifiant les identités

$$p.e = p, \qquad p.(g.g') = (p.g).g' \tag{6}$$

pour $p \in P$ et $g, g' \in G$ (en notant e l'élément neutre de G). Pour tout $g \in G$, l'application $u_g : p \to p.g$ est alors un $k(g)$-automorphisme de la variété P, et pour tout $p \in P$, l'application $v_p : g \to p.g$ est un $k(p)$-morphisme de G dans P.

Nous établirons d'abord quelques propriétés élémentaires des espaces à opérateurs.

Proposition 1. — *Soit P une k-variété où opère le groupe G, et soit E une partie de P stable par G. Alors l'adhérence H de E pour la $\mathbf{K}$-topologie est stable par G; si E est l'orbite d'un point a rationnel sur k, alors H est k-fermé et $\mathbf{K}$-irréductible, et E est un k-ouvert de H.*

Pour tout $g \in G$, on sait que u_g est un automorphisme de variété de P; comme $u_g(E) \subset E$, on a donc $u_g(H) \subset H$.

Si E est l'orbite de a, c'est l'image du k-morphisme v_a défini plus haut; ceci montre d'abord que E est $\mathbf{K}$-irréductible, donc que H est $\mathbf{K}$-irréductible. Pour tout k-automorphisme σ de $\mathbf{K}$, on a $v_a^\sigma = v_a$ puisque v_a est un k-morphisme, d'où

$$G = v_a^{-1}(H) = v_a^{-1}(H)^\sigma = (v_a^\sigma)^{-1}(H^\sigma) = v_a^{-1}(H^\sigma)$$

ce qui prouve $E \subset H^\sigma$ et donc $H \subset H^\sigma$ puisque H^σ est $\mathbf{K}$-fermé; il en résulte que H est k-fermé.

Enfin, d'après les propriétés des morphismes, l'intérieur E' de E dans H

muni de la **K**-topologie est non vide; mais comme u_g est un automorphisme de P et qu'on a $u_g(E)=E$ et $u_g(H)=H$, on a $u_g(E')=E'$ pour tout $g\in G$; comme G est transitif sur E, on a donc $E'=E$, et E est **K**-ouvert dans H. Soient σ un k-automorphisme de **K** et $F=H-E$; comme F est un **K**-fermé de P, et qu'on a $F^\sigma\subset H^\sigma=H$ et $\varphi_a^{-1}(F^\sigma)=\varphi_a^{-1}(F)^\sigma=\emptyset$, on a $F^\sigma\cap E=\emptyset$ et finalement $H^\sigma\subset F$; alors F est k-fermé et $E=H-F$ est k-ouvert dans H. C. Q. F. D.

PROPOSITION 2. — *Soient P et P' deux k-variétés sur lesquelles opère G. On suppose que G est transitif sur P. Si une application rationnelle f de P dans P' définie sur k vérifie la relation*

$$f(p.g)=f(p).g \tag{7}$$

chaque fois que $f(p)$ et $f(p.g)$ sont définis, f est un k-morphisme.

D'après la formule (7), on a $f\odot u_g=u'_g\odot f$ pour tout $g\in G$, les automorphismes u_g de P et u'_g de P' étant définis par $u_g(p)=p.g$ et $u'_g(p')=p'.g$ pour $p\in P$ et $p'\in P'$. On a alors

$$D(f)=D(u'_g\odot f)=D(f\odot u_g)=u_g^{-1}(D(f))$$

et par suite $D(f)$ est stable par G; comme $D(f)$ est non vide et que G est transitif sur P, on a donc $D(f)=P$. C. Q. F. D.

3. Construction d'espaces homogènes. — *Soit G une k-variété de groupe.* Nous nous proposons de donner une construction des espaces homogènes pour le groupe G avec un point rationnel, munis de leur structure de variété algébrique.

PROPOSITION 3. — *Soit P une k-variété sur laquelle le groupe G opère transitivement, et soit $a\in P$ un point rationnel sur k. Alors si L est l'image de $R_k(P)$ par le cohomomorphisme de $\varphi_a : g\to a.g$ de G dans P, le sous-corps $\mathbf{K}(L)$ de $R(G)$ est invariant par les translations à droite δ_g par les éléments de G; de plus, L caractérise P et a à un isomorphisme près.*

(N. B. — Pour $f\in R(G)$ et $g\in G$, on pose $\gamma_g(f)=f\odot\gamma_g$ et $\delta_g(f)=f\odot\delta_g$).

Soit π le cohomomorphisme de φ_a; on a donc $\mathbf{K}(L)=\pi(R(P))$ puisque $R(P)=\mathbf{K}(R_k(P))$, et par suite $\mathbf{K}(L)$ est l'ensemble des fonctions $f\odot\varphi_a$ pour f parcourant $R(P)$. Mais on a l'identité $u_g\odot\varphi_a=\varphi_a\odot\delta_g$ pour tout $g\in G$ et par suite

$$\delta_g(f\odot\varphi_a)=f\odot\varphi_a\odot\delta_g=(f\odot u_g)\odot\varphi_a,$$

ce qui montre que $\mathbf{K}(L)$ est stable par δ_g.

Soient P' une k-variété où opère transitivement G, a' un point de P' rationnel sur k, π' le cohomomorphisme de $\varphi_{a'}$ et L' l'image de $R_k(P')$ par π'.

Supposons qu'on ait $L' \subset L$; il existe alors une application rationnelle unique φ de P dans P', définie sur k, et telle que $\varphi_{a'} = \varphi \odot \varphi_a$. Mais pour $g \in G$, on a

$$(u'^{-1}_g \odot \varphi \odot u_g) \odot \varphi_a = u'^{-1}_g \odot \varphi \odot \varphi_a \odot \delta_g = u'^{-1}_g \odot \varphi_{a'} \odot \delta_g = \varphi_{a'}$$

en vertu des formules

$$u_g \odot \varphi_a = \varphi_a \odot \delta_g \qquad \text{et} \qquad u'_g \odot \varphi_{a'} = \varphi_{a'} \odot \delta_g$$

(u_g et u'_g sont définis comme dans la démonstration de la proposition 2). D'après l'unicité de φ, on a alors $\varphi = u'^{-1}_g \odot \varphi \odot \delta_g$ pour tout $g \in G$, et comme G est transitif sur P, la proposition 2 montre que φ est un k-morphisme; de plus, on a $\varphi(a.g) = \varphi(\varphi_a(g)) = \varphi_{a'}(g) = a'.g$.

Si alors, on a $L = L'$, il existe un k-morphisme φ' de P' dans P tel que $\varphi'(a'.g) = a.g$ pour tout $g \in G$, ce qui prouve que φ et φ' sont des isomorphismes réciproques. C. Q. F. D.

Après ce résultat d'unicité, voici un théorème d'existence.

Proposition 4. — *Soit L un sous-corps de $R_k(G)$ contenant k. Si le sous-corps $\mathbf{K}(L)$ de $R(G)$ est invariant par δ_g pour tout $g \in G$, il existe une k-variété P sur laquelle G opère transitivement et un point $a \in P$ rationnel sur k, tels que L soit l'image de $R_k(P)$ par le cohomomorphisme de $\varphi_a : g \to a.g$ de G dans P.*

On note p et p' les deux projections de $G \times G$ sur G, et π la loi de groupe $(g, g') \to g.g'$ de $G \times G$ dans G; de plus, on pose $R = R_k(G)$ et $S = R_k(G \times G)$ et l'on note respectivement σ, σ' et Δ les cohomomorphismes de p, p' et π.

Soient $f \in R$ et $F = \Delta(f)$; on a alors

$$F(\bigstar ; g) = \delta_g(f) \qquad (g \in G) \tag{8}$$

et donc si $f \in L$, on aura $F(\bigstar ; g) \in \mathbf{K}(L)$ pour tout $g \in G$, d'après l'hypothèse faite sur L. D'après le lemme 3, on a donc $F \in k(L^\sigma, R^{\sigma'})$, et par suite $L^\Delta \subset k(L^\sigma, R^{\sigma'})$. Mais si u est l'automorphisme $(g, g') \to (g.g', g'^{-1})$ de la variété $G \times G$, et si Σ est la symétrie $g \to g^{-1}$ de G, on a

$$p \odot u = \pi, \qquad p' \odot u = \Sigma \odot p' \qquad \pi \odot u = p. \tag{9}$$

Par suite, si τ est le cohomomorphisme de u et ζ celui de Σ, ce sont des automorphismes de S et de R respectivement et l'on a

$$\tau \circ \sigma = \Delta, \qquad \tau \circ \sigma' = \sigma' \circ \zeta, \qquad \tau \circ \Delta = \sigma. \tag{10}$$

Si l'on applique τ à la formule $L^\Delta \subset k(L^\sigma, R^{\sigma'})$, on trouve la formule $L^\sigma \subset k(L^\Delta, R^{\sigma'})$, d'où finalement

$$k(L^\Delta, R^{\sigma'}) = k(L^\sigma, R^{\sigma'}). \tag{11}$$

Comme l'extension R/k est régulière, il en est de même de l'extension L/k, et il existe donc une k-variété P_1 et une application rationnelle φ de G dans P_1 telle que $\varphi(G)$ soit dense dans P_1 et que L soit l'image de $R_k(P_1)$ par le cohomomorphisme de φ. Soit φ' l'application rationnelle, définie sur k, de $G\times G$ dans $P_1\times G$ définie par $\varphi'(g,g')=(\varphi(g),g')$ pour $g\in D(\varphi)$ et $g'\in G$; comme $k(L^\sigma, R^{\sigma'})$ est l'image de $R_k(P_1\times G)$ par le cohomomorphisme de φ', et que ce cohomomorphisme est injectif, la formule $L^\Delta\subset k(L^\sigma, R^{\sigma'})$ exprime qu'il existe une application rationnelle α définie sur k de $P_1\times G$ dans P_1, et une seule qui vérifie la relation $\alpha\odot\varphi'=\varphi\odot\pi$, soit explicitement

$$\alpha(\varphi(g), g')=\varphi(g.g') \tag{12}$$

chaque fois que les deux membres de cette formule ont un sens. On voit alors immédiatement que la formule (11) exprime que l'application rationnelle u' de $P_1\times G$ dans lui-même définie par

$$u'(p,g)=(\alpha(p,g),g) \tag{13}$$

est birationnelle. Enfin, de la formule (12) et de l'associativité dans G, on déduit immédiatement la relation

$$\alpha(p,g.g')=\alpha(\alpha(p,g),g') \tag{14}$$

valable sur $P\times G\times G$ chaque fois qu'elle a un sens.

Mais il résulte des conditions énumérées ci-dessus et d'un théorème de WEIL ([5]) que G opère sur une k-variété P_2 contenant comme sous-variété k-ouverte un k-ouvert non vide P'_1 de P_1 et qu'on a $\alpha(p,g)=p.g$ chaque fois que $\alpha(p,g)$ est défini et appartient à P'_1 pour $p\in P'_1$ et $g\in G$. On peut alors considérer φ comme une application rationnelle définie sur k de G dans P_2; d'après la formule (12) et la proposition 2, on voit que φ est un k-morphisme et que $\varphi(g.g')=\varphi(g).g'$ pour $g, g'\in$ G. Posons $a=\varphi(e)\in P_2$; comme e est rationnel sur k et que φ est un k-morphisme, a est rationnel sur k, et l'on a $\varphi(g)=a.g$ pour tout $g\in G$. Or l'image de φ est dense dans P_1, donc aussi dans P_2, et d'après la proposition 1, l'image $\varphi(G)$ de φ, qui est l'orbite de a dans P, est une sous-variété k-ouverte de P_2. Il suffira donc de poser $P=\varphi(G)$ pour satisfaire aux conditions exigées.

C. Q. F. D.

REMARQUE. — Soit L un sous-corps de $R_k(G)$ tel que $\mathbf{K}(L)$ soit invariant par δ_g pour tout $g\in G$; soit de plus H le sous-groupe de G formé des g tels que γ_g induise l'identité sur $\mathbf{K}(L)$. Alors pour $f\in L$ et $h\in H$, on a $h.D(f)=D(f)$ et pour $g\in D(f)$, on a $f(h.g)=f(g)$. Par passage au

([5]) *On algebraic groups of transformations* (*Amer. J. Math.*, t. 77, 1955, p. 355-391).

quotient, les éléments de L définissent des applications dans $\mathbf{K}$ de parties de G/H, et l'on peut vérifier directement, sans faire usage du théorème de WEIL, qu'on définit ainsi une structure de k-variété sur G/H, où opère G.

4. Propriétés des homomorphismes. — *Soient G et G' deux k-variétés de groupe.* Nous allons démontrer quelques propriétés élémentaires des variétés de groupe et des homomorphismes de celles-ci.

LEMME 4. — *L'adhérence d'un sous-groupe E de G pour la $\mathbf{K}$-topologie est un sous-groupe de G.*

Pour tout $g \in G$, les applications γ_g et δ_g de G dans G sont continues pour la $\mathbf{K}$-topologie, et il en est de même de la symétrie $S : g \to g^{-1}$. Comme $E^{-1} = S(E) = E$, on a donc $S(\bar{E}) \subset \bar{E}$, en notant $\bar{E}$ l'adhérence de E. Comme $E.E \subset E$ on a $\gamma_x(E) \subset E$ pour $x \in E$, d'où $\gamma_x(\bar{E}) \subset \bar{E}$; on a donc $E.\bar{E} \subset \bar{E}$. Par suite, pour $x \in \bar{E}$, on a $\delta_x(E) \subset \bar{E}$, d'où $\delta_x(\bar{E}) \subset \bar{E}$ et finalement $\bar{E}.\bar{E} \subset \bar{E}$. C. Q. F. D.

LEMME 5. — *Si U et U' sont deux ouverts non vides de G, on a $G = U.U'$.*

Soit $x \in G$; comme les ouverts U et U' de G sont non vides, l'irréductibilité de G montre que $U \cap x.U'^{-1}$ n'est pas vide. Il existe donc $y \in U$ et $y' \in U'$ tels que

$$y = x.y'^{-1}, \qquad \text{d'où} \qquad x = y.y' \in U.U'.$$

C. Q. F. D.

Voici maintenant les propriétés annoncées des homomorphismes; on appelle k-homomorphisme d'une k-variété de groupe dans une autre toute application qui est un k-morphisme de variétés et une représentation pour les lois de groupes.

PROPOSITION 5. — *Pour tout k-homomorphisme f de G dans G', son image $f(G)$ est un sous-groupe k-fermé et $\mathbf{K}$-irréductible.*

Soit H l'adhérence du sous-groupe $f(G)$ de G'; c'est donc un sous-groupe de G' d'après le lemme 4. Mais, si l'on fait opérer G à droite sur G' par l'application $(g', g) \to g'.f(g)$ de $G' \times G$ dans G', alors $f(G)$ est l'orbite de l'élément neutre de G'. D'après la proposition 1, H est k-fermé et $\mathbf{K}$-irréductible et $f(G)$ est k-ouvert dans H; mais comme H est une sous-variété fermée et un sous-groupe de G' on peut le munir d'une structure de variété de groupe induite. Comme $f(G)$ est ouvert dans H, le lemme 5 montre que

$$H = f(G).f(G) = f(G).$$

C. Q. F. D.

PROPOSITION 6. — *Soit f une application rationnelle de G dans G' définie*

sur k. Si l'on a

$$f(x.y) = f(x).f(y) \tag{15}$$

chaque fois que x, y et x.y sont dans D(f), alors f est un k-homomorphisme.

Soit $y \in D(f)$; on a alors la relation (15) pour x dans $D(f) \cap D(f).y^{-1}$, d'où

$$f(x) = f(x.y).f(y)^{-1}$$

dans les mêmes conditions; ceci implique $f = \delta^{-1}_{f(y)} \odot f \odot \delta_y$, et par suite,

$$D(f) = D(\delta^{-1}_{f(y)} \odot f \odot \delta_y) = \delta_y^{-1}(D(f)) = D(f).y^{-1}$$

puisque les translations à droite sont des automorphismes de variété. On a donc $D(f) = D(f).D(f)^{-1}$ et, par conséquent, $D(f) = G$ d'après le lemme 5 puisque $D(f)$ est ouvert dans G. C. Q. F. D.

5. **Construction de groupes quotients.** — *Soit G une k-variété de groupe.* Nous nous proposons d'appliquer les résultats relatifs aux espaces homogènes pour caractériser les k-homomorphismes surjectifs de G sur une k-variété de groupe.

Proposition 7. — *Soit f un k-homomorphisme de G sur une k-variété de groupe G', et soit L l'image de $R_k(G')$ par le cohomomorphisme de f. Alors le sous-corps $\mathbf{K}(L)$ de $R(G)$ est invariant par γ_g et δ_g pour tout $g \in G$, et le sous-corps L de $R_k(G)$ caractérise G' et f à un isomorphisme près.*

Il est clair que $\mathbf{K}(L)$ se compose des fonctions de la forme $h \odot f$ avec $h \in R(G')$; mais la formule $f(g.g') = f(g).f(g')$ pour $g, g' \in G$ s'écrit $\gamma_{f(g)} \odot f = f \odot \gamma_g$ pour tout $g \in G$. Pour $h \in R(G')$, on a alors

$$\gamma_g(h \odot f) = h \odot f \odot \gamma_g = (h \odot \gamma_{f(g)}) \odot f$$

et, par suite, γ_g applique $\mathbf{K}(L)$ dans lui-même; le cas de δ_g se traite de manière analogue.

Soit f_1 un k-homomorphisme de G dans une k-variété de groupe G'_1 et soit L_1 l'image de $R_k(G_1)$ par le cohomomorphisme de f_1. Supposons d'abord $L_1 \subset L$. Il existe alors une application rationnelle α de G' dans G'_1 telle que $\alpha(G')$ soit dense dans G'_1 et que $f_1 = \alpha \odot f$. Soit U le domaine de définition de α; pour $x \in f^{-1}(U)$, on alors $f_1(x) = \alpha(f(x))$. Soient alors $u, v \in U$ tels que $u.v \in U$ et soient $x, y \in G$ tels que $u = f(x)$ et $v = f(y)$. On a $u.v = f(x.y)$ et, par suite,

$$\begin{aligned} \alpha(u.v) &= \alpha(f(x.y)) = f_1(x.y) = f_1(x).f_1(y) \\ &= \alpha(f(x)).\alpha(f(y)) = \alpha(u).\alpha(v) \end{aligned}$$

et la proposition 6 prouve que α est un k-homomorphisme de G' dans G'_1 tel que $f_1 = \alpha \circ f$.

Si l'on a $L = L_1$, il existe alors aussi un k-homomorphisme α' de G'_1 dans G' tel que $f = \alpha' \circ f_1$, et par suite α et α' sont des isomorphismes réciproques. C. Q. F. D.

Aprés ce théorème d'unicité, nous allons utiliser la proposition 4 pour démontrer un théorème d'existence.

PROPOSITION 8. — *Soit L un sous-corps de $R_k(G)$ contenant k et tel que $\mathbf{K}(L)$ soit invariant par γ_g et δ_g pour tout $g \in G$. Il existe alors une k-variété de groupe G' et un k-homomorphisme f de G sur G' tel que L soit l'image de $R_k(G')$ par le cohomomorphisme de f.*

D'après la proposition 4, il existe une k-variété P sur laquelle G opère transitivement et un point a de P rationnel sur k tel que L soit l'image de $R_k(P)$ par le cohomomorphisme π du k-morphisme surjectif $\varphi_a : g \to a.g$ de G sur P.

Pour tout $g \in G$, l'automorphisme γ_g du corps $R(G)$ laisse invariant le sous-corps $\mathbf{K}(L) = \pi(R(P))$; il existe donc une application birationnelle γ'_g de P dans P définie de manière unique par la relation

$$\gamma'_g \odot \varphi_a = \varphi_a \odot \gamma_g. \tag{16}$$

Mais, pour tout $g' \in G$, les automorphismes γ_g et $\delta_{g'}$ de la variété G sont permutables, et si $\delta'_{g'}$ est l'automorphisme $p \to p.g'$ de la variété P, on a

$$\delta'_{g'} \odot \varphi_a = \varphi_a \odot \delta_{g'}. \tag{17}$$

Un calcul facile basé sur les formules (16) et (17) et la permutabilité de γ_g et $\delta_{g'}$ démontre la relation

$$\gamma'_g \odot \delta'_{g'} \odot \varphi_a = \delta'_{g'} \odot \gamma'_g \odot \varphi_a \tag{18}$$

et comme φ_a est un morphisme surjectif, on en déduit que γ'_g et $\delta'_{g'}$ commutent. Mais la proposition 2 montre que γ'_g est un *morphisme* de P dans P et, d'après la formule (18), on a

$$\gamma'_g(a.g') = a.g.g'. \tag{19}$$

Soit H le sous-groupe de stabilité de a dans G. Si $h \in H$ et $g \in G$, on a

$$a.(g.h.g^{-1}) = \gamma'_g(a.h.g^{-1}) = \gamma'_g(a.g^{-1}) = a.g.g^{-1} = a,$$

d'après la formule (19) puisque $a.h = a$; ce calcul prouve donc que H est distingué, et il existe alors sur P une structure de groupe et une seule pour laquelle $\varphi = \varphi_a$ soit une représentation. L'élément neutre de P est a et, d'après la formule (19) et la relation $\varphi(g) = a.g$, on voit que γ'_g est la

translation à gauche par $\varphi(g)$ dans P et que δ'_g est la translation à droite par $\varphi(g)$.

Les translations à gauche et à droite dans P sont des automorphismes de variété. Pour montrer que la structure de k-variété sur P est compatible avec sa loi de groupe, il suffit de montrer que la restriction de la loi de groupe de P à un k-ouvert non vide de $P \times P$ est un k-morphisme; en effet, ceci implique immédiatement que la loi de groupe est un k-morphisme de $P \times P$ dans P d'après ce qu'on a démontré sur les translations.

Reprenons les notations de la démonstration de la proposition 4. Soient $f \in L$ et $\Delta(f) = F$; on a $F(g; \bigstar) = \gamma_g(f) \in \mathbf{K}(L)$ pour tout $g \in G$ et, par suite, $F \in k(R^\sigma, L^{\sigma'})$ d'après le lemme 3; autrement dit, $L^\Delta \subset k(R^\sigma, L^{\sigma'})$. Mais on a vu dans la démonstration de la proposition 4 que L^Δ est contenu dans $k(L^\sigma, R^{\sigma'})$, et comme R^σ et $R^{\sigma'}$ sont linéairement disjoints sur k, les corps $k(L^\sigma, R^{\sigma'})$ et $k(R^\sigma, L^{\sigma'})$ sont linéairement disjoints sur $k(L^\sigma, L^{\sigma'})$; finalement, on a

$$L^\Delta \subset k(L^\sigma, R^{\sigma'}) \cap k(R^\sigma, L^{\sigma'}) = k(L^\sigma, L^{\sigma'}).$$

Si π est la loi de groupe sur G, l'image de $R_k(P)$ par le cohomomorphisme de $\varphi \odot \pi$ est L^Δ, tandis que $k(L^\sigma, L^{\sigma'})$ est l'image de $R_k(P \times P)$ par le cohomomorphisme du k-morphisme (φ, φ) de $G \times G$ sur $P \times P$. Comme on a $L^\Delta \subset k(L^\sigma, L^{\sigma'})$, il existe une application rationnelle α de $P \times P$ dans P, définie sur k, et telle que

$$\varphi \odot \pi = \alpha \odot (\varphi, \varphi). \tag{20}$$

Soit alors U l'ensemble k-ouvert de définition de α; si u, v appartiennent à U, on peut trouver x, $y \in G$ tels que $u = \varphi(x)$ et $v = \varphi(y)$ et, d'après (20), on aura

$$\alpha(u, v) = \alpha(\varphi(x), \varphi(y)) = \varphi(x.y) = u.v$$

et ceci prouve que la restriction à U de la loi de groupe de P est un k-morphisme de U dans P.

Pour achever la démonstration, il suffit alors de prendre pour G' la k-variété de groupe obtenue en munissant P de ses deux structures, qui sont compatibles d'après ce qu'on vient de voir, et de poser $f = \varphi_a$.

C. Q. F. D.

CHAPITRE 2.

ISOGÉNIES.

1. Espaces homogènes principaux. — *Soit G une k-variété de groupe.* On dit qu'une k-variété où opère G à droite est un *espace homogène principal* (à droite) si l'application $(p, g) \to (p, p.g)$ est un isomorphisme de

k-variété de $P \times G$ sur $P \times P$. Pour tout $p \in P$, l'application $g \to p.g$ est alors un isomorphisme de $k(p)$-variété de G sur P.

Le groupe des matrices inversibles de degré n à coefficients dans $\mathbf{K}$ est le k-ouvert de l'espace numérique $\mathbf{K}^{n \times n}$ défini par l'équation : $\det M \neq 0$. Muni de sa structure de groupe et de la structure de sous-variété k-ouverte de $\mathbf{K}^{n \times n}$ c'est une k-variété de groupe, notée $GL(n)$. Nous allons démontrer un résultat de notoriété publique sur ce groupe et ses « cocycles » ([6]).

LEMME 1. — *Soit P un espace homogène principal pour G. Si une application rationnelle F de $P \times G$ dans $GL(n)$, définie sur k, vérifie l'identité*

$$F(p; g.g') = F(p.g; g').F(p; g) \tag{1}$$

en tout point de $P \times G \times G$ où elle a un sens, il existe une application rationnelle H de P dans $GL(n)$, définie sur k, et telle que la relation

$$H(p.g) = F(p; g).H(p) \tag{2}$$

ait lieu en tout point de $P \times G$ où elle a un sens.

L'ensemble des $p \in P$ tels que $F(p; \bigstar)$ soit définie est un k-ouvert non vide de P, donc contient un point a algébrique sur k. Comme l'application $g \to a.g$ est un isomorphisme de $k(a)$-variété, il existe une application rationnelle F' de P dans $GL(n)$, définie sur $k(a)$, et telle que

$$F'(a.g) = F(a; g), \tag{3}$$

chaque fois que $F(a; g)$ est défini; en effet, la fonction $F(a; \bigstar)$ sur G est définie sur le corps $k(a)$ (*Cf.* chap. 1, n° 1, *b*). Faisant $p = a$ et $a.g = p'$ dans la formule (1), on a alors la relation

$$F'(p'.g') = F(p'; g').F'(p') \tag{4}$$

en tout point de $P \times G$ où elle a un sens.

Identifions $R(P)$ et $R(G)$ à des sous-corps de $R(P \times G)$ et notons σ le cohomomorphisme de l'application $(p, g) \to p.g$ de $P \times G$ sur P. Soit V l'ensemble des matrices $\mathbf{h}$ à n lignes et une colonne, à coefficients dans $R_{k(a)}(P)$, qui sont solutions de l'équation

$$\sigma(\mathbf{h}) = F.\mathbf{h}. \tag{5}$$

D'après la formule (4), les colonnes de la matrice F' sont des éléments de V, linéairement indépendants sur le corps $R_{k(a)}(P)$ puisque $\det F' \neq 0$; d'autre part, soit $(u_1, \ldots, u_m)$ une base de $k(a)$ sur k; si $\mathbf{h} \in V$, on peut écrire $\mathbf{h} = \Sigma u_i.\mathbf{h}_i$, où les matrices $\mathbf{h}_i$ sont à coefficients dans $R_k(P)$. Mais comme les corps $R_k(P \times G)$ et $k(a)$ sont linéairement disjoints sur k, la formule (5)

([6]) *Cf.* l'article de E. KOLCHIN et S. LANG, cité dans la Note ([4]).

montre que les $\mathbf{h}_i$ sont des solutions de (5); autrement dit, tout élément de V est combinaison linéaire à coefficients dans $k(a)$ d'éléments de V qui soient des matrices à coefficients dans $R_k(P)$. Comme V contient n éléments linéairement indépendants sur $R_{k(a)}(P)$, il contient n éléments $\mathbf{u}_j$ $(1 \leqq j \leqq n)$ à coefficients dans $R_k(P)$, linéairement indépendants sur $R_{k(a)}(P)$. La matrice H dont les colonnes sont les $\mathbf{u}_j$ a alors son déterminant non nul et l'on a $\sigma(H) = F.H$ d'après (5), relation qui équivaut à (2).

C. Q. F. D.

2. Le théorème de Jacobson-Bourbaki. — *Soit M un corps* (commutatif). Pour tout sous-corps L de M, notons $\mathbf{E}_L$ l'annean des endomorphismes de M considéré comme espace vectoriel à droite sur L. L'anneau $\mathbf{E}_L$ contient le corps des homothéties $h_x : y \to xy$ par les éléments de M, de sorte qu'il devient un espace vectoriel à gauche sur M au moyen de la loi externe $(x, u) \to h_x \circ u \quad (x \in M, u \in \mathbf{E}_L)$.

Soit alors L un sous-corps de M tel que $[M : L]$ soit fini. Si $(f_1, \ldots, f_m)$ est une base de M sur L, l'application M-linéaire $u \to (u(f_1), \ldots, u(f_m))$ de $\mathbf{E}_L$ dans M^m est alors bijective; on a donc $[\mathbf{E}_L : M] = m$, c'est-à-dire

$$[\mathbf{E}_L : M] = [M : L] \tag{6}$$

et $\mathbf{E}_L$ est un espace M-vectoriel de dimension finie. Réciproquement, on a le lemme suivant :

Lemme 2. — *Soit A un anneau d'endomorphismes du groupe additif de M, contenant le corps des homothéties de M, et de dimension finie sur M. Il existe alors un sous-corps L de M et un seul tel que $A = \mathbf{E}_L$ et l'on a $[M : L] = [A : M]$.*

L'ensemble des $y \in M$ tels que $u(xy) = u(x)y$ pour tout $u \in A$ et tout $x \in M$ est un sous-corps L de M; soient $f_1, \ldots, f_m$ des éléments de M linéairement indépendants sur L et soit h l'application $u \to (u(f_1), \ldots, u(f_m))$ de A dans M^m. Comme A contient le corps des homothéties de M, $P = h(A)$ est un sous-espace M-vectoriel de M^m, et comme A est un anneau, P est stable par les applications $\tilde{u} : (x_1, \ldots, x_m) \to (u(x_1), \ldots, u(x_m))$ de M^m dans lui-même $(u \in A)$.

Il en résulte alors (7) que P a une base sur M, formée d'éléments de M^m à coordonnées dans L; si l'on avait $P \neq M^m$, il existerait alors des éléments a_i de L non tous nuls pour $1 \leqq i \leqq m$, et tels qu'on ait $\Sigma a_i . x_i = 0$ pour $(x_1, \ldots, x_m)$ dans P; en particulier, on aurait $\Sigma a_i . f_i = 0$, ce qui est absurde puisque les f_i sont linéairement indépendants sur L.

On a donc prouvé que h est surjective, d'où $m \leqq [A : M]$ par suite, $[M : L]$

(7) *Cf.* l'article cité dans la Note (3), lemme 3, chap. IV.

est fini et $\leqq [A : M]$; mais comme $A \subset \mathbf{E}_L$, on a

$$[M : L] \leqq [A : M] \leqq [\mathbf{E}_L : M] = [M : L], \qquad \text{d'où} \qquad A = \mathbf{E}_L.$$

Enfin si L' est un sous-corps de M tel que $A = \mathbf{E}_{L'}$, on a $L' \subset L$ par définition de L; si l'on avait $[M : L'] = \infty$, on aurait aussi $[A : M] = [\mathbf{E}_{L'} : M] = \infty$; on a donc

$$[M : L'] = [\mathbf{E}_{L'} : M] = [A : M] = [M : L], \qquad \text{d'où} \qquad [M : L'] = [M : L]$$

et finalement $L' = L$. C. Q. F. D.

3. **Théorie « galoisienne » des variétés de groupes, I.** — *Soient G une k-variété de groupe et L un sous-corps de $R_k(G)$ ayant les propriétés suivantes :*

1° *L contient k;*
2° *Le degré $[R_k(G) : L]$ est fini;*
3° *Le sous-corps $\mathbf{K}(L)$ de $R(G)$ est invariant par δ_g pour tout $g \in G$.*

On notera A l'anneau des endomorphismes de $R(G)$ considéré comme espace vectoriel sur $\mathbf{K}(L)$; on considérera A comme espace vectoriel sur $R(G)$ comme il est expliqué au n° 2. Pour tout sous-corps k' de $\mathbf{K}$ contenant k, on notera $A_{k'}$ le sous-anneau de A formé des u tels que $u(R_{k'}(G)) \subset R_{k'}(G)$; on notera $\mathbf{N}$ le sous-anneau de A formé des u commutant à δ_g pour tout $g \in G$; enfin, on posera $\mathbf{N}_{k'} = A_{k'} \cap \mathbf{N}$.

Nous allons étudier ces algèbres associées au corps L.

Lemme 3. — *Pour tout sous-corps k' de $\mathbf{K}$ contenant k, une base de A_k sur $R_k(G)$ est une base de $A_{k'}$ sur $R_{k'}(G)$.*

Le corps $R(G)$ est composé de $R_k(G)$ et $\mathbf{K}$ linéairement disjoints sur k, donc aussi de $R_k(G)$ et $\mathbf{K}(L)$ linéairement disjoints sur L. Par suite, une base $(f_1, \ldots, f_n)$ de $R_k(G)$ sur L est aussi une base de $R(G)$ sur $\mathbf{K}(L)$, et l'application $R(G)$-linéaire $u \to (u(f_1), \ldots, u(f_n))$ est une bijection h de A sur $R(G)^n$; mais on a $h(A_k) = R_k(G)^n$, et comme $(f_1, \ldots, f_n)$ est une base de $R_{k'}(G)$ sur $k'(L)$, on a $h(A_{k'}) = R_{k'}(G)^n$, et le lemme résulte de là immédiatement. C. Q. F. D.

Lemme 4. — *Toute base de $\mathbf{N}_k$ sur k est une base de A_k sur $R_k(G)$.*

Nous poserons $R = R_k(G)$ et $S = R_k(G \times G)$ et nous noterons σ et σ' les cohomomorphismes des projections de $G \times G$ sur ses deux facteurs. Le corps S est alors composé de R^σ et $R^{\sigma'}$ linéairement disjoints sur k, donc aussi de R^σ et $k(L^\sigma, R^{\sigma'})$ linéairement disjoints sur L^σ.

Soit $(f_1, \ldots, f_n)$ une base de R sur L, de sorte que $(f_1^\sigma, \ldots, f_n^\sigma)$ est une base de R^σ sur L^σ et donc de S sur $k(L^\sigma, R^{\sigma'})$; soient, de plus,

F_i pour $1 \leq i \leq n$ les éléments de S définis par $F_i(g, g') = f_i(g.g')$ pour $g, g' \in D(f_i)$. On posera $F_i = \sum_j m_{ij}.f_j^{\sigma}$ avec des m_{ij} dans $k(L^{\sigma}, R^{\sigma'})$; si U est l'ensemble k-ouvert non vide de G formé des g tels que les fonctions $m_{ij}(\bigstar; g)$ soient définies, on aura

$$\delta_g(f_i) = F_i(\bigstar; g) = \sum_j m_{ij}(\bigstar; g).f_j \tag{7}$$

pour tout $g \in U$. En notation matricielle, ceci s'écrit

$$\delta_g(\mathbf{f}) = M(\bigstar; g).\mathbf{f} \qquad (g \in U) \tag{8}$$

en notant $\mathbf{f}$ la matrice à n lignes et une colonne formée des f_i, et M la matrice $\| m_{ij} \|$.

Soient $g, g' \in U$ tels que $g.g' \in U$; on a

$$\begin{aligned} M(\bigstar; g.g').\mathbf{f} &= \delta_{g.g'}(\mathbf{f}) = \delta_g(\delta_{g'}(\mathbf{f})) = \delta_g(M(\bigstar; g').\mathbf{f}) \\ &= \delta_g(M(\bigstar; g')).\delta_g(\mathbf{f}) = \delta_g(M(\bigstar; g')).M(\bigstar; g).\mathbf{f}. \end{aligned}$$

Mais, comme la matrice M a ses coefficients dans $k(L^{\sigma}, R^{\sigma'})$, le lemme 2 du chapitre 1 montre que pour $g \in U$, les coefficients de la matrice $M(\bigstar; g)$ sont dans $\mathbf{K}(L)$, et par hypothèse, on a $\delta_g(\mathbf{K}(L)) \subset \mathbf{K}(L)$ pour tout $g \in G$; par suite, les facteurs de $\mathbf{f}$ dans les deux membres extrêmes de la suite écrite plus haut sont des matrices à coefficients dans $\mathbf{K}(L)$, et comme $(f_1, \ldots, f_n)$ est une base de $R(G)$ sur $\mathbf{K}(L)$, on en déduit

$$M(\bigstar; g.g') = \delta_g(M(\bigstar; g')).M(\bigstar; g). \tag{9}$$

D'après le lemme 1 du chapitre 1, ceci montre que la relation

$$M(a; g.g') = M(a.g; g').M(a; g) \tag{10}$$

a lieu en tout point de $G \times G \times G$ où elle a un sens. Par ailleurs, pour tout $g \in G$, le corps $R(G)$ admet les $\delta_g(f_i)$ pour base sur $\delta_g(\mathbf{K}(L)) = \mathbf{K}(L)$, et d'après la formule (8) le déterminant de la matrice $M(\bigstar; g)$ est non nul pour $g \in U$; *a fortiori*, on a $\det M \neq 0$.

D'après le lemme 1, il existe donc une matrice carrée inversible H de degré n à coefficients dans R et telle qu'on ait

$$H(a.g) = M(a; g).H(a) \tag{11}$$

en tout point de $G \times G$ où ceci est défini; autrement dit, on a

$$\delta_g(H) = M(\bigstar; g).H$$

pour tout $g \in U$. Mais l'application $u \to (u(f_1), \ldots, u(f_n))$ est un isomorphisme d'espace R-vectoriel de A_k sur R^n, et comme $\det H \neq 0$, il existe une

base $(u_1, \ldots, u_n)$ de A_k sur R définie par $u_j(f_i) = H_{ij}$ pour $1 \leq i, j \leq n$. Pour $g \in U$, on a alors

$$\partial_g(u_j(f_i)) = \partial_g(H_{ij}) = \sum_l M_{il}(\bigstar; g).H_{lj} = \sum_l M_{il}(\bigstar; g).u_j(f_l)$$
$$= u_j\left(\sum_l M_{il}(\bigstar; g).f_l\right) = u_j(\partial_g(f_i)),$$

puisque u_j est linéaire par rapport au corps $\mathbf{K}(L)$ et que $M_{il}(\bigstar; g)$ appartient à $\mathbf{K}(L)$. Comme les f_i forment une base de R sur L, il résulte du calcul précédent que u_j commute à ∂_g pour $g \in U$, donc pour tout $g \in G = U.U$ (*cf.* lemme 5 du chapitre 1) et par suite u_j appartient à $\mathbf{N}_k$ pour $1 \leq j \leq n$.

On a vu que $(u_1, \ldots, u_n)$ est une base de A_k sur R; soit alors $u = \Sigma f'_i . u_i$ un élément de $\mathbf{N}_k$; de la formule $\partial_g \circ u = u \circ \partial_g$ on déduit immédiatement $\partial_g(f'_i) = f'_i$ pour tout $g \in G$ et $1 \leq i \leq n$, ce qui prouve que les f'_i sont dans k. C. Q. F. D.

Lemme 5. — *Soit k' un sous-corps de $\mathbf{K}$ contenant k. Toute base de $\mathbf{N}_k$ sur k est une base de $\mathbf{N}_{k'}$ sur k'.*

D'après les lemmes 3 et 4, on a

$$[\mathbf{N}_k : k] = [A_k : R_k(G)] = [A_{k'} : R_{k'}(G)] = [\mathbf{N}_{k'} : k'].$$

De plus, si $(u_1, \ldots, u_n)$ est une base de $\mathbf{N}_k$ sur k, les u_i sont linéairement indépendants sur $R_{k'}(G)$ d'après les lemmes 3 et 4, et *a fortiori* sur k'; comme $[\mathbf{N}_{k'} : k'] = [\mathbf{N}_k : k]$, il en résulte que $(u_1, \ldots, u_n)$ est une base de $\mathbf{N}_{k'}$ sur k'. C. Q. F. D.

Pour tout entier $r > 0$, nous noterons $\mathbf{N}_k^{(r)}$ l'ensemble des applications u de $R(G)^r$ dans $R(G)$ qui sont multilinéaires par rapport au corps $\mathbf{K}(L)$, qui appliquent $R_k(G)^r$ dans $R_k(G)$, et qui commutent à ∂_g pour tout $g \in G$ au sens suivant :

$$\partial_g(u(f_1, \ldots, f_r)) = u(\partial_g(f_1), \ldots, \partial_g(f_r)) \tag{12}$$

pour $f_1, \ldots, f_r \in R(G)$. On posera par convention $\mathbf{N}_k^{(0)} = k$; on a alors $\mathbf{N}_k = \mathbf{N}_k^{(1)}$ et pour tout $r \geq 0$, $\mathbf{N}_k^{(r)}$ est un espace k-vectoriel. Enfin, la formule

$$(u \cup u')(f_1, \ldots, f_{r+s}) = u(f_1, \ldots, f_r).u'(f_{r+1}, \ldots, f_{r+s}) \tag{13}$$

définit une application k-bilinéaire $(u, u') \to u \cup u'$ de $\mathbf{N}_k^{(r)} \times \mathbf{N}_k^{(s)}$ dans $\mathbf{N}_k^{(r+s)}$, comme on le vérifie aisément, et l'on a la formule d'associativité

$$(u \cup u') \cup u'' = u \cup (u' \cup u'') \tag{14}$$

pour $u \in \mathbf{N}_k^{(r)}$, $u' \in \mathbf{N}_k^{(s)}$ et $u'' \in \mathbf{N}_k^{(t)}$. Avec ces notations, on a le lemme suivant :

LEMME 6. — *Pour tout entier $r \geqq 0$, l'application k-linéaire π_r de la puissance tensorielle $T_r(\mathbf{N}_k)$ de $\mathbf{N}_k$ dans $\mathbf{N}_k^{(r)}$ définie par*

$$\pi_r(u_1 \otimes \ldots \otimes u_r) = u_1 \cup \ldots \cup u_r \tag{15}$$

est bijective.

Raisonnant par récurrence sur r, on se ramène à démontrer que pour $r \geqq 0$, l'application k-linéaire φ de $\mathbf{N}_k \otimes \mathbf{N}_k^{(r)}$ dans $\mathbf{N}_k^{(r+1)}$ définie par $\varphi(u \otimes v) = u \cup v$ est bijective, c'est-à-dire que pour toute base $\{u_i\}$ de $\mathbf{N}_k$ sur k, tout $u \in \mathbf{N}_k^{(r+1)}$ s'écrit de manière unique sous la forme

$$u = \Sigma u_i \cup v_i, \qquad \text{avec} \quad v_i \in \mathbf{N}_k^{(r)}.$$

Or, pour $f_2, \ldots, f_{r+1}$ dans $R(G)$, l'application $u_1' : f_1 \to u(f_1, \ldots, f_{r+1})$ appartient à A, et comme $\{u_i\}$ est une base de A sur $R(G)$ d'après les lemmes 3 et 4, il existe des applications v_i de $R(G)^r$ dans $R(G)$ bien déterminées par la condition

$$u_1' = \sum_i u_i . v_i(f_2, \ldots, f_r), \tag{16}$$

soit, plus explicitement,

$$u(f_1, \ldots, f_{r+1}) = \sum_i u_i(f_1) . v_i(f_2, \ldots, f_{r+1}). \tag{17}$$

Le lecteur vérifiera aisément que les v_i sont dans $\mathbf{N}_k^{(r)}$, et la formule (17) s'écrit alors

$$u = \sum_i u_i \cup v_i,$$

ce qui démontre le lemme. C. Q. F. D.

On identifiera désormais $\mathbf{N}_k^{(r)}$ et $T_r(\mathbf{N}_k)$ au moyen de π_r. On a donc, par définition,

$$(u_1 \otimes \ldots \otimes u_r)(f_1, \ldots, f_r) = u_1(f_1) \ldots u_r(f_r). \tag{18}$$

Cette identification faite, on définira des applications $\varepsilon : \mathbf{N}_k \to k$ et $\Delta : \mathbf{N}_k \to \mathbf{N}_k \otimes \mathbf{N}_k$ par les formules

$$\varepsilon(u) = u(1), \tag{19}$$

$$\Delta(u)(f_1, f_2) = u(f_1 . f_2) \tag{20}$$

pour $u \in \mathbf{N}_k$. Pour justifier ces définitions il suffit de remarquer, d'une part qu'on a $u(1) \in R_k(G)$ puisque $1 \in R_k(G)$ et

$$\delta_g(u(1)) = u(\delta_g(1)) = u(1)$$

pour tout $g \in G$, d'où $u(1) \in k$, et, d'autre part, que l'application $(f_1, f_2) \to u(f_1.f_2)$ appartient à $\mathbf{N}_k^{(2)}$, ce qui est immédiat. On a alors les propriétés suivantes :

a. ε *est un homomorphisme de k-algèbres :* en effet, on a $u(f) = \varepsilon(u).f$ pour $u \in \mathbf{N}_k$ et $f \in \mathbf{K}(L)$ puisque u est linéaire par rapport au corps $\mathbf{K}(L)$.

b. Δ *est un homomorphisme de k-algèbres :* soient u, $v \in \mathbf{N}_k$ et posons

$$\Delta(u) = \sum_i u_i \otimes u_i' \qquad \text{et} \qquad \Delta(v) = \sum_j v_j \otimes v_j';$$

on a

$$\Delta(u).\Delta(v) = \sum_{i,j} u_i v_j \otimes u_i' v_j',$$

et pour $f, f' \in R(G)$,

$$\Delta(uv)(f, f') = (uv)(f.f') = u\left(\sum_j v_j(f).v_j'(f')\right)$$
$$= \sum_{i,j} u_i(v_j(f)).u_i'(v_j'(f')) = \{\Delta(u).\Delta(v)\}(f, f'),$$

ce qui démontre notre assertion.

Enfin, les propriétés suivantes ne font que traduire par transposition l'associativité et la commutativité de la multiplication dans $R(G)$, et le fait que 1 est élément unité de $R(G)$.

c. Les applications $(\Delta \otimes 1) \circ \Delta$ et $(1 \otimes \Delta) \circ \Delta$ *de* $\mathbf{N}_k$ *dans* $\mathbf{N}_k \otimes \mathbf{N}_k \otimes \mathbf{N}_k$ *sont égales.*

d. L'image de Δ *se compose de tenseurs symétriques dans* $\mathbf{N}_k \otimes \mathbf{N}_k$.

e. Les applications $(\varepsilon \otimes 1) \circ \Delta$ *et* $(1 \otimes \varepsilon) \circ \Delta$ *de* $\mathbf{N}_k$ *dans* $\mathbf{N}_k$ *sont l'identité.*

4. Théorie « galoisienne » des variétés de groupes, II. — Nous allons démontrer une réciproque aux résultats du numéro précédent.

Soient G une k-variété de groupe et $\mathbf{M}$ *une k-algèbre d'applications* $\mathbf{K}$*-linéaires de* $R(G)$ *dans* $R(G)$, *vérifiant les conditions suivantes :*

1° $\mathbf{M}$ *est de dimension finie sur k;*

2° *Tout* $u \in \mathbf{M}$ *applique* $R_k(G)$ *dans lui-même et commute à* δ_g *pour tout* $g \in G$,

3° *Pour tout* $u \in \mathbf{M}$, *il existe des éléments* u_i *et* u_i' *de* $\mathbf{M}$ *tels qu'on ait*

$$u(f.f') = \sum_i u_i(f).u_i'(f') \qquad (f, f' \in R(G)) \tag{21}$$

Soit H le corps des homothéties de $R(G)$, et soit H_k le sous-corps de H formé des homothéties dont le rapport est dans $R_k(G)$. La formule (21) peut s'écrire

$$u \circ h_f = \sum h_{u_i(f)} \circ u_i' \qquad (u \in \mathbf{M},\ f \in R(G)) \tag{22}$$

et, par suite, on a $H.\mathbf{M} \supset \mathbf{M}.H$, d'où

$$(H.\mathbf{M}).(H.\mathbf{M}) = H.(\mathbf{M}.H).\mathbf{M} \subset H.(H.\mathbf{M}).\mathbf{M} \subset H.\mathbf{M}$$

puisque H et $\mathbf{M}$ sont des anneaux. Autrement dit, $H.\mathbf{M}$ est l'anneau engendré par H et $\mathbf{M}$ dans l'anneau $\mathbf{E}$ de toutes les applications k-linéaires de $R(G)$ dans $R(G)$. De même, comme on a $u_i(f) \in R_k(G)$ pour $f \in R_k(G)$, on voit par un raisonnement analogue que $H_k.\mathbf{M}$ est le sous-anneau de $\mathbf{E}$ engendré par H_k et $\mathbf{M}$. Tous les éléments de $H_k.\mathbf{M}$ appliquant $R_k(G)$ dans lui-même, on peut considérer l'ensemble B des restrictions à $R_k(G)$ des éléments de $H_k.\mathbf{M}$, de sorte que B est un anneau d'endomorphismes k-linéaires de $R_k(G)$. Les homothéties du corps $R_k(G)$ appartiennent à B, et l'on a

$$[B : R_k(G)] \leqq [H_k.\mathbf{M} : H_k] \leqq [\mathbf{M} : k];$$

d'après le lemme 2, il existe un sous-corps L de $R_k(G)$ contenant k, et un seul, tel que B soit l'ensemble des applications L-linéaires de $R_k(G)$ dans lui-même. De plus, on a

$$[\mathbf{R}_k(G) : L] = [B : R_k(G)] \leqq [\mathbf{M} : k].$$

Soit $(f_1, \ldots, f_n)$ une base de $R_k(G)$ sur L ; l'application $u \to (u(f_1), \ldots, u(f_n))$ de $H_k.\mathbf{M}$ dans $R_k(G)^n$ est surjective, puisque B est l'ensemble des applications L-linéaires de $R_k(G)$ dans lui-même. Il en résulte que l'application $\varphi : u \to (u(f_1), \ldots, u(f_n))$ de $H.\mathbf{M}$ dans $R(G)^n$ est surjective. Mais, en vertu d'un raisonnement déjà fait, $(f_1, \ldots, f_n)$ est une base de $R(G)$ sur $\mathbf{K}(L)$. Comme tout élément de $\mathbf{M}$ est linéaire par rapport à $\mathbf{K}$ et à L, les éléments de $H.\mathbf{M}$ sont linéaires par rapport à $\mathbf{K}(L)$, et comme φ est surjective, $H.\mathbf{M}$ *est l'ensemble des applications* $\mathbf{K}(L)$*-linéaires de* $R(G)$ *dans lui-même.*

D'après la démonstration du lemme 2, $\mathbf{K}(L)$ est l'ensemble des $f \in R(G)$ tels que h_f commute aux éléments de $H.\mathbf{M}$, donc est l'ensemble des f tels que $h_f \circ u = u \circ h_f$ pour $u \in \mathbf{M}$, c'est-à-dire tels que $u(f.f') = f.u(f')$ pour $u \in \mathbf{M}$ et $f' \in R(G)$. Pour $f \in \mathbf{K}(L)$, on a donc $u(f) = f.u(1)$ pour tout $u \in \mathbf{M}$; mais, si $f \in \mathbf{R}(G)$ vérifie cette condition, on a

$$u(f.f') = \Sigma u_i(f).u_i'(f') = \Sigma f.u_i(1).u_i'(f') = f.u(f')$$

pour $u \in \mathbf{M}$ et $f' \in R(G)$, d'après la formule (21), et l'on a donc $f \in \mathbf{K}(L)$. Soit $\mathbf{M}^+$ l'ensemble des $u \in \mathbf{M}$ tels que $u(1) = 0$; on a donc prouvé

que $\mathbf{K}(L)$ est l'ensemble des éléments de $R(G)$ annulés par $\mathbf{M}^+$, donc que $L = \mathbf{K}(L) \cap R_k(G)$ *est l'ensemble des éléments de* $R_k(G)$ *annulés par* $\mathbf{M}^+$.

Comme tout élément de $\mathbf{M}$ commute à δ_g pour tout $g \in G$, on voit par transport de structure que $\mathbf{K}(L)$ est invariant par δ_g pour tout $g \in G$. Soit $\mathbf{N}_k$ l'ensemble des applications $\mathbf{K}(L)$-linéaires de $R(G)$ dans lui-même, appliquant $R_k(G)$ dans $R_k(G)$ et commutant à δ_g pour tout $g \in G$. On a $\mathbf{M} \subset \mathbf{N}_k$ et d'après les lemmes 3 et 4, on a $[\mathbf{N}_k : k] = [R_k(G) : L]$, d'où

$$[R_k(G) : L] \leqq [\mathbf{M} : k] \leqq [\mathbf{N}_k : k] = [R_k(G) : L]$$

et finalement $\mathbf{M} = \mathbf{N}_k$.

Résumons les résulats obtenus :

PROPOSITION 1. — *Supposons que* $\mathbf{M}$ *vérifie les conditions du début de ce numéro, et soient* $\mathbf{M}^+$ *l'ensemble des* $u \in \mathbf{M}$ *tels que* $u(1) = 0$, *et* L *l'ensemble des éléments de* $R_k(G)$ *annulés par* $\mathbf{M}^+$. *Alors le sous-corps* $\mathbf{K}(L)$ *de* $R(G)$ *est invariant par* δ_g *pour tout* $g \in G$, *on a* $[R_k(G) : L] = [\mathbf{M} : k]$, *et* $\mathbf{M}$ *est l'ensemble des applications* $\mathbf{K}(L)$*-linéaires de* $R(G)$ *dans* $R(G)$, *qui commutent à* δ_g *pour tout* $g \in G$, *et appliquent* $R_k(G)$ *dans lui-même.*

5. **Isogénies.** — *Soit* G *une* k*-variété de groupe.* On appelle *k-isogénie* un k-homomorphisme α de G sur une k-variété de groupe G' de même dimension que G; si π est le cohomomorphisme de α, on a

$$[R_k(G) : \pi(R_k(G'))] = [R(G) : \pi(R(G'))] < \infty$$

et l'on appelle cet entier le *degré de* α, noté $\nu(\alpha)$. Si $\alpha : G \to G'$ et $\beta : G' \to G''$ sont des k-isogénies, il en est de même de $\beta \circ \alpha$ et l'on a

$$\nu(\beta \circ \alpha) = \nu(\beta) . \nu(\alpha).$$

Soit $\alpha : G \to G'$ une isogénie et soit π le cohomomorphisme de α; pour tout sous-corps k' de $\mathbf{K}$ contenant k, on posera $L_{k'}(\alpha) = \pi(R_{k'}(G))$ et l'on notera $\mathbf{N}_{k'}(\alpha)$ l'ensemble des applications $\mathbf{K}$-linéaires u de $R(G)$ dans lui-même qui satisfont aux conditions :

1° u applique $R_{k'}(G)$ dans lui-même;
2° u commute à δ_g pour tout $g \in G$;
3° u est linéaire par rapport au corps $L_{k'}(\alpha)$.

On a alors $L_{k'}(\alpha) = k'(L_k(\alpha))$; de plus, $\mathbf{N}_{k'}(\alpha)$ est une algèbre de dimension finie sur k' égale à $\nu(\alpha)$, et toute base de $\mathbf{N}_k(\alpha)$ sur k est une base de $\mathbf{N}_{k'}(\alpha)$ sur k'. Enfin, au n° 3, on a défini un homomorphisme ε de $\mathbf{N}_k(\alpha)$ dans k, dont nous noterons le noyau $\mathbf{N}_k^+(\alpha)$, et un homomorphisme Δ de $\mathbf{N}_k(\alpha)$ dans $\mathbf{N}_k(\alpha) \otimes_k \mathbf{N}_k(\alpha)$ et ces homomorphismes satisfont aux conditions c à e du n° 3. Soient enfin $u \in \mathbf{N}_k(\alpha)$ et $g \in G$; comme γ_g

commute à $\delta_{g'}$ pour tout $g' \in G$ et conserve le corps $L_{\mathbf{K}}(\alpha)$, on voit immédiatement que $\rho_g(u) = \gamma_g^{-1} \circ u \circ \gamma_g$ est dans $\mathbf{N}_{\mathbf{K}}(\alpha)$; on définit ainsi une représentation linéaire ρ de G dans l'algèbre $\mathbf{N}_{\mathbf{K}}(\alpha)$ de dimension finie sur $\mathbf{K}$, appelée *représentation adjointe.*

Ces notions obéissent à certaines lois qui résultent des raisonnements des numéros précédents.

a. Le corps $L_k(\alpha)$ est l'ensemble des éléments de $R_k(G)$ annulés par $\mathbf{N}_k^+(\alpha)$: *cf.* proposition 1.

b. Pour qu'un sous-corps L de $R_k(G)$ soit de la forme $L_k(\alpha)$, il faut et il suffit que $[R_k(G):L]$ soit fini, et que $\mathbf{K}(L)$ soit invariant par γ_g et δ_g pour tout $g \in G$: *cf.* proposition 8 du chapitre 1.

c. Pour qu'une k-algèbre $\mathbf{M}$ d'applications $\mathbf{K}$-linéaires de $R(G)$ dans lui-même soit de la forme $\mathbf{N}_k(\alpha)$, il faut et suffit qu'elle soit de dimension finie sur k, que tout $u \in \mathbf{M}$ applique $R_k(G)$ dans lui-même et commute à δ_g pour tout $g \in G$, qu'il existe des u_i et u_i' dans $\mathbf{M}$ vérifiant la condition (21), et enfin, que pour $u \in \mathbf{M}$ et tout $g \in G$, on ait $\gamma_g \circ u \circ \gamma_g^{-1} \in \mathbf{M}$: cela résulte de la proposition 1, de *b.* et de la remarque que la dernière condition énoncée assure que le corps des éléments de $R(G)$ annulés par $\mathbf{M}^+$ est invariant par γ_g pour tout $g \in G$.

d. Soient α et β deux k-isogénies définies dans G; pour qu'on ait $L_k(\alpha) \subset L_k(\beta)$ [resp. $L_k(\alpha) = L_k(\beta)$], il faut et suffit qu'il existe une k-isogénie (resp. un k-isomorphisme) γ tel que $\alpha = \gamma \circ \beta$: *cf.* démonstration de la proposition 7 du chapitre 1.

e. Soient α et β deux k-isogénies; pour qu'on ait $L_k(\alpha) \subset L_k(\beta)$, il faut et suffit qu'on ait $\mathbf{N}_k(\alpha) \supset \mathbf{N}_k(\beta)$: cela résulte des conditions *a* et 3° ci-dessus.

Enfin, nous énoncerons un théorème de correspondance « galoisienne » :

PROPOSITION 2. — *Soient G une k-variété de groupe et α une k-isogénie de G dans une k-variété de groupe G'. Soit $\mathbf{M}$ une sous-algèbre de $\mathbf{N}_k(\alpha)$; pour qu'il existe une k-isogénie β telle que $\mathbf{M} = \mathbf{N}_k(\beta)$, il faut et suffit que $\mathbf{K}.\mathbf{M}$ soit stable par la représentation adjointe de G dans $\mathbf{N}_{\mathbf{K}}(\alpha)$ et qu'on ait $\Delta(\mathbf{M}) \subset \mathbf{M} \otimes \mathbf{M}$. De plus, β est déterminée à un isomorphisme près par $\mathbf{M}$, et l'on obtient ainsi toutes les k-isogénies β telles que α se factorise en $\alpha = \gamma \circ \beta$.*

6. Isogénies séparables. — *Soient G une k-variété de groupe et $\alpha : G \to G'$ une k-isogénie.* On note ν_s et ν_i respectivement le facteur séparable et le facteur inséparable du degré $\nu(\alpha)$ de l'extension $R_k(G)/L_k(\alpha)$; on a donc $\nu(\alpha) = \nu_s . \nu_i$. D'après un résultat bien connu sur les « revêtements », il existe au moins un point $g' \in G'$ tel que $\alpha^{-1}(g')$ se compose de ν_s éléments; comme $\alpha^{-1}(g')$ est une classe modulo le noyau H de α, il en résulte que H est fini et se compose de ν_s éléments.

Nous supposerons désormais que les points de H sont rationnels sur k; il en est ainsi si k est algébriquement clos puisque H est k-fermé et fini. Pour tout $h \in H$, la translation à gauche γ_h est alors un k-automorphisme de la variété G, donc définit un automorphisme $\gamma_h : f \to f \odot \gamma_h$ du corps $R(G)$, qui laisse stable $R_k(G)$; comme les translations à gauche commutent aux translations à droite, les γ_h sont des éléments de $\mathbf{N}_k(\alpha)$, linéairement indépendants sur k d'après le théorème de Dedekind. De plus, il résulte des définitions qu'on a $\Delta(\gamma_h) = \gamma_h \otimes \gamma_h$ et $\varepsilon(\gamma_h) = 1$ pour tout $h \in H$; l'ensemble $\mathbf{M}$ des combinaisons linéaires à coefficients dans k des γ_h pour $h \in H$ est alors une sous-algèbre de $\mathbf{N}_k(\alpha)$, telle que $\mathbf{K}.\mathbf{M}$ soit stable par la représentation adjointe puisque H est un sous-groupe invariant de G, et l'on a $\Delta(\mathbf{M}) \subset \mathbf{M} \otimes \mathbf{M}$ d'après les formules précédentes; enfin on a $[\mathbf{M} : k] = \nu_s$. D'après la proposition 2, il existe alors une k-isogénie α_s telle que $\mathbf{M} = \mathbf{N}_k(\alpha_s)$. Comme $\mathbf{M}^+$ est sous-tendu par les $\gamma_h - 1$ pour $h \in H$, le corps $L_k(\alpha_s)$ est l'ensemble des invariants des $\gamma_h - 1$ pour $h \in H$; comme γ_h est l'identité sur $L_k(\alpha_s)$, on a $\alpha_s \circ \gamma_h = \alpha_s$ pour tout $h \in H$, ce qui signifie que H est contenu dans le noyau de α_s; mais comme $\nu(\alpha_s) = \nu_s$ est l'ordre du noyau de α_s, il en résulte que H est le noyau de α_s.

Nous poserons $L = L_k(\alpha)$, $L_i = L_k(\alpha_s)$ et nous noterons L_s la plus grande extension séparable de L contenue dans $R_k(G) = R$. L'extension R/L_i est galoisienne et son groupe de Galois $\mathcal{G}$ se compose des γ_h pour $h \in H$; d'autre part, R est purement inséparable sur L_s qui est la plus grande extension séparable de L contenue dans R; par suite, si $\sigma \in \mathcal{G}$ induit l'identité sur L_s, il est l'identité sur R, et $\mathcal{G}$ induit donc un groupe de ν_s automorphismes de L_s/L; donc $[L_s : L]$ est égal à ν_s, l'extension L_s/L est galoisienne et $L_i \cap L_s$ est l'ensemble des éléments de L_s invariants par $\mathcal{G}$, donc est égal à L. Un élément de L_i séparable sur L est dans $L = L_i \cap L_s$, par conséquent L_i/L est purement inséparable. D'après le critère de MacLane, les corps L_s et L_i sont alors linéairement disjoints sur L; de plus, on a $L_i(L_s) \supset L_i$, et si $\sigma \in \mathcal{G}$ est l'identité sur $L_i(L_s)$, il est l'identité sur L_s donc sur R; la théorie de Galois montre alors qu'on a $R = L_i(L_s)$. Par conséquent, $R(G)$ est composé des corps $\mathbf{K}(L_i)$ et $\mathbf{K}(L_s)$ linéairement disjoints sur $\mathbf{K}(L)$; comme $\mathbf{K}(L_i)$ est purement inséparable sur $\mathbf{K}(L)$ et $\mathbf{K}(L_s)$ est séparable sur $\mathbf{K}(L)$, il en résulte que $\mathbf{K}(L_i)$ est la plus grande extension séparable de $\mathbf{K}(L)$ contenue dans $R(G)$; comme γ_g et δ_g conservent le corps $\mathbf{K}(L)$, ils conservent $\mathbf{K}(L_s)$ pour tout $g \in G$, et par suite, il existe une k-isogénie α_i telle que $L_s = L_k(\alpha_i)$. On notera que R est purement inséparable sur L_s, donc que $\nu_s(\alpha_i) = 1$, et donc que α_i est bijective.

L'algèbre $\mathbf{N}_k(\alpha)$ contient donc les deux sous-algèbres

$$\mathbf{N}_k(\alpha_s) = \mathbf{N}_s \qquad \text{et} \qquad \mathbf{N}_k(\alpha_i) = \mathbf{N}_i.$$

Ces *deux algèbres commutent* : tout d'abord, comme H est le noyau de α_s, les translations à droite δ_h par les éléments de H forment un groupe d'ordre ν_s

d'automorphismes de R/L_i; comme $\nu_s = [R:L_i]$, la théorie de Galois montre que L_i est l'ensemble des $f \in R$ tels que $\delta_h(f) = f$ pour tout $h \in H$ et comme on a $u \circ \delta_h = \delta_h \circ u$ pour $u \in \mathbf{N}_k(\alpha)$ et $h \in H$, on a $u(L_i) \subset L_i$ pour $u \in \mathbf{N}_k(\alpha)$. Soient alors $u \in \mathbf{N}_i$ et $h \in H$; pour $f \in L_i$, on a $u(f) \in L_i$, et u est linéaire par rapport au corps L_s; on a donc

$$u(\gamma_h(f.f')) = u(\gamma_h(f).f') = \gamma_h(f).u(f') = \gamma_h(f.u(f')) = \gamma_h(u(f.f'))$$

pour $f \in L_s$ et $f' \in L_i$, et comme R est l'anneau engendré par L_s et L_i, ceci prouve que u et γ_h commutent.

Montrons maintenant que $\mathbf{N}_s$ *et* $\mathbf{N}_i$ *sont linéairement disjointes dans* $\mathbf{N}_k(\alpha)$; on a vu que les γ_h pour $h \in H$ forment une base de $\mathbf{N}_s$ sur k; supposons qu'on ait une relation $\sum_h u_h.\gamma_h = 0$ avec des $u_h \in \mathbf{N}_i$; pour $f \in L_s$, et $f' \in L_i$, on a

$$0 = \sum_h u_h(\gamma_h(f.f')) = \sum_h \gamma_h(f).u_h(f').$$

D'après le théorème de Dedekind, on a donc $u_h(f') = 0$ pour $h \in H$ et $f' \in L_i$, d'où $u_h = 0$ pour tout h puisque u_h est linéaire par rapport au corps L_s et que toute base de L_i sur L est une base de R sur L_s, donc de $R(G)$ sur $\mathbf{K}(L_s)$.

Enfin, on a

$$[\mathbf{N}_k(\alpha):k] = \nu(\alpha) = \nu_i.\nu_s = \nu(\alpha_i).\nu(\alpha_s) = [\mathbf{N}_i:k].[\mathbf{N}_s:k].$$

En résumé, on a prouvé le résultat suivant :

PROPOSITION 3. — *Soit $\alpha : G \to G'$ une k-isogénie; on suppose que tous les éléments du noyau H de α sont rationnels sur k. Il existe alors deux isogénies α_s et α_i définies dans G et telles que* :

1° *Le noyau de α_s est H et l'algèbre $\mathbf{N}_k(\alpha_s)$ admet pour base sur k les translations à gauche γ_h par les éléments de H*;

2° *α_i est bijective*;

3° *L'application φ de $\mathbf{N}_k(\alpha_s) \otimes \mathbf{N}_k(\alpha_i)$ dans $\mathbf{N}_k(\alpha)$ définie par $\varphi(u \otimes v) = u.v$ est un isomorphisme de k-algèbres.*

REMARQUES. — 1° Nous dirons qu'une *k-isogénie α est séparable* si l'extension $R_k(G)/L_k(\alpha)$ est séparable; on définit de manière analogue une *k-isogénie purement inséparable*. Avec les notations de la proposition 3, α_s est séparable et α_i est purement inséparable.

2° Si l'isogénie α est séparable, on peut supposer $\alpha = \alpha_s$, de sorte que $\mathbf{N}_k(\alpha)$ est l'algèbre du groupe fini H à coefficients dans le corps k. Réciproquement, on montre facilement que si H est un sous-groupe invariant fini

de G dont tous les points sont rationnels sur k, c'est le noyau d'une k-isogénie séparable.

7. Isogénies et algèbres de Lie. — *Dans ce numéro nous supposerons que le corps* $\mathbf{K}$ *est de caractéristique* $p \neq 0$, *et nous noterons* G *une* k*-variété de groupe.*

L'application $x \to x^p$ étant un automorphisme du domaine universel $\mathbf{K}$, le sous-corps $R_k(G)^p$ de $R_k(G)$ détermine sur G une structure de k^p-variété de groupe; on notera G^p la k-variété de groupe obtenue par extension des scalaires de k^p à k, de sorte que la structure de variété de G^p est définie par le sous-corps $k(R_k(G)^p)$ de $R_k(G)$. L'application identique de G est alors une isogénie ι de G sur G^p; comme l'extension $R_k(G)/k$ est séparable de type fini, on a $\nu(\iota) = p^d$ en notant d la dimension de G.

Nous poserons $L = k(R_k(G)^p) = R_k(G^p)$, et les notations A, A_k, $\mathbf{N}_k$ ont la même signification qu'au n° 3. Enfin, nous noterons $\mathfrak{D}(G)$ l'ensemble des $\mathbf{K}$-dérivations de $R(G)$; comme l'extension $R_k(G)/k$ est séparable de type fini, $\mathfrak{D}(G)$ est un espace vectoriel de dimension d sur le corps $R(G)$. Nous nous proposons de déterminer la structure de l'isogénie ι et de déterminer les isogénies en lesquelles on puisse factoriser ι.

LEMME 7. — *Soit* k' *un sous-corps de* $\mathbf{K}$ *contenant* k. *Toute base de* $\mathbf{N}_k \cap \mathfrak{D}(G)$ *sur* k *est une base de* $\mathbf{N}_{k'} \cap \mathfrak{D}(G)$ *sur* k', *une base de* $A_k \cap \mathfrak{D}(G)$ *sur* $R_k(G)$ *et une base de* $A_{k'} \cap \mathfrak{D}(G)$ *sur* $R_{k'}(G)$.

D'après les lemmes 3, 4 et 5, il suffit de prouver que l'espace vectoriel $\mathfrak{D}(G)$ sur le corps $R(G)$ est engendré par des éléments de $\mathbf{N}_k$.

Pour $u \in A$ et $g \in G$ posons $\varphi_g(u) = \gamma_g^{-1} \circ u \circ \gamma_g$; comme γ_g est un automorphisme du corps $R(G)$, on voit facilement qu'on a

$$\varphi_g(f.u) = \gamma_g(f).\varphi_g(u) \tag{23}$$

pour tout $f \in R(G)$; en particulier, pour $f \in R(G)$ et $u \in \mathfrak{D}(G) \cap \mathbf{N}_k$ on a

$$\varphi_g(f.u) = \gamma_g(f).u.$$

Montrons maintenant que $\mathfrak{D}(G)$ est engendré sur $R(G)$ par des éléments de A_k. Soit $(f_1, \ldots, f_n)$ une base de $R_k(G)$ sur L, et donc aussi de $R(G)$ sur $\mathbf{K}(L)$, et soit $(u_1, \ldots, u_n)$ une base de A_k sur $R_k(G)$, donc aussi de A sur $R(G)$; comme tout élément de A est linéaire par rapport au corps $\mathbf{K}(L)$, pour que $u = \Sigma c_i.u_i$ soit une dérivation du corps $R(G)$, il faut et suffit qu'on ait

$$\Sigma c_i \{ u_i(f_j.f_l) - f_j.u_i(f_l) - u_i(f_j).f_l \} = 0, \tag{24}$$

ce qui est un système linéaire homogène à coefficients dans $R_k(G)$ en les c_i; ceci démontre évidemment notre assertion.

Soit alors φ un projecteur $R_k(G)$-linéaire de $R(G)$ sur $R_k(G)$; comme $\mathfrak{D}(G)$ est engendré sur $R(G)$ par des éléments de A_k, il est stable par l'application additive $\tilde{\varphi}$ de A dans A définie par

$$\tilde{\varphi}(f.u) = \varphi(f).u \qquad [f \in R(G),\ u \in \mathbf{N}_k]. \tag{25}$$

Soit $\mathfrak{M}$ l'ensemble des applications additives de $R(G)$ dans $R(G)$ égales à φ ou à l'une des translations γ_g. Si $f' \in k$, on a évidemment

$$\psi(f.f') = \psi(f).f' \qquad [\psi \in \mathfrak{M},\ f' \in R(G)], \tag{26}$$

réciproquement si $f' \in R(G)$ vérifie cette relation, on a $\psi(f') = \psi(1).f'$ pour tout $\psi \in \mathfrak{M}$; si l'on fait $\psi = \varphi$, on trouve $\varphi(f') = f'$, d'où $f' \in R_k(G)$, puis si l'on fait $\psi = \gamma_g$, on trouve $\gamma_g(f') = f'$ pour tout $g \in G$, d'où $f' \in k$. Le lemme résulte alors du lemme 3 du chapitre IV de l'article cité en (3).

C. Q. F. D.

D'après le lemme 7, $\mathfrak{g} = \mathfrak{D}(G) \cap \mathbf{N}_{\mathbf{K}}$ est un espace vectoriel de dimension d sur $\mathbf{K}$. Comme toute dérivation de $R(G)$ est linéaire par rapport au corps $R(G)^p$, on voit que $\mathfrak{g}$ n'est autre que l'ensemble des dérivations du corps $R(G)$ qui commutent aux translations à droite δ_g par les éléments de G. Il en résulte que $\mathfrak{g}$ est stable par les opérations $(\mathfrak{d}, \mathfrak{d}') \to [\mathfrak{d}, \mathfrak{d}']$ et $\mathfrak{d} \to \mathfrak{d}^p$, donc que c'est une p-algèbre de Lie, qu'on appelle l'*algèbre de Lie de* G. Pour tout sous-corps k' de $\mathbf{K}$ contenant k, on note $\mathfrak{g}_{k'}$ l'ensemble des éléments de $\mathfrak{g}$ qui appliquent $R_{k'}(G)$ dans lui-même; comme $\mathfrak{g}_k = \mathfrak{g} \cap A_k = \mathfrak{D}(G) \cap \mathbf{N}_k$, le lemme 7 montre que toute base de $\mathfrak{g}_k$ sur k est une base de $\mathfrak{g}_{k'}$ sur k'; de plus, il est clair que $\mathfrak{g}_{k'}$ est stable par le crochet et la puissance $p^{\text{ième}}$.

Nous allons déterminer la structure de l'algèbre $\mathbf{N}_k$. Auparavant, nous rappellerons quelques notions sur les algèbres enveloppantes. Soient B une algèbre associative sur le corps k et $\mathfrak{h}$ un sous-espace de B stable par crochet et puissance $p^{\text{ième}}$. On dit que B est *algèbre enveloppante* de $\mathfrak{h}$ si les deux conditions suivantes sont satisfaites :

1° $\mathfrak{h}$ *engendre l'algèbre* B;

2° *Si* f *est une application* k*-linéaire de* $\mathfrak{h}$ *dans une algèbre associative* B' *telle que* $f([x, y]) = [f(x), f(y)]$ *et* $f(x^p) = f(x)^p$ *pour* $x, y \in \mathfrak{h}$, *alors* f *se prolonge en un homomorphisme de* B *dans* B'.

Soit $(x_1, \ldots, x_n)$ une base de $\mathfrak{h}$ sur k; la condition 1° signifie que les monomes $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, avec $0 \leq \alpha_i < p$ pour $1 \leq i \leq n$ engendrent l'espace k-vectoriel B, et les conditions 1° et 2° signifient que ces monomes forment une *base* de B sur k (théorème de Birkhoff-Witt-Jacobson).

Proposition 4. — *L'algèbre associative* $\mathbf{N}_k(\iota)$ *est algèbre enveloppante de la* p*-algèbre de Lie* $\mathfrak{g}_k$.

Soit S l'ensemble des suites $(\alpha_1, \ldots, \alpha_d)$ d'entiers compris entre 0 et

$p-1$; nous choisirons une base $(u_1, \ldots, u_d)$ de $\mathfrak{g}_k$ sur k, et pour tout $\alpha=(\alpha_1, \ldots, \alpha_d)\in S$, nous poserons

$$Z_\alpha = u_1^{\alpha_1}\ldots u_d^{\alpha_d}/\alpha_1!\ldots\alpha_d!. \tag{27}$$

Comme $\mathbf{N}_k(\iota):\nu(\iota)=p^d$, tout revient à démontrer que les Z_α sont linéairement indépendants sur k.

Or, pour $u\in\mathfrak{g}_k$, la formule

$$u(f.f')=u(f).f'+f.u(f') \qquad \text{pour} \quad f,\ f'\in R(G)$$

s'exprime par la formule

$$\Delta(u)=u\otimes 1+1\otimes u. \tag{28}$$

Par la formule du binome, on a alors

$$\Delta(u^m/m!)=\sum_{i+j=m} u^i/i!\otimes u^j/j! \tag{29}$$

pour tout entier m tel que $0\leqq m<p$; on en déduit immédiatement

$$\Delta(Z_\alpha)=\sum_{\beta+\gamma=\alpha} Z_\beta\otimes Z_\gamma \tag{30}$$

pour $\alpha\in S$, l'addition dans S étant définie composante par composante. De plus, on a $\varepsilon(u)=u(1)=0$ pour $u\in\mathfrak{g}_k$, d'où

$$\varepsilon(Z_\alpha)=0 \qquad [\alpha\neq(0, \ldots, 0)]. \tag{31}$$

Pour $\alpha\in S$, nous poserons $|\alpha|=\sum_i \alpha_i$; nous allons démontrer par récurrence sur m que les Z_α avec $|\alpha|\leqq m$ sont linéairement indépendants sur k. Pour $m=0$, on a $\alpha=(0, \ldots, 0)$ et il n'y a rien à démontrer. Soit donc $m\geqq 1$, et supposons les Z_α avec $|\alpha|<m$ linéairement indépendants; supposons qu'on ait une relation linéaire

$$\sum_{|\alpha|\leqq m} c_\alpha Z_\alpha=0 \qquad (c_\alpha\in k). \tag{32}$$

D'après (31), on a $c_0=0$; puis appliquant à la relation (32) l'opérateur $u\to\Delta(u)-u\otimes 1-1\otimes u$, on trouve

$$\sum_{\beta,\gamma} c_{\beta+\gamma} Z_\beta\otimes Z_\gamma=0, \tag{33}$$

où la sommation s'étend sur les couples (β, γ) d'éléments de S tels que

$$0<|\beta|\leqq m, \qquad 0<|\gamma|\leqq m \qquad \text{et} \qquad |\beta|+|\gamma|=|\beta+\gamma|\leqq m;$$

mais ces conditions impliquent $|\beta| < m$ et $|\gamma| < m$, et par l'hypothèse de récurrence, les éléments $Z_\beta \otimes Z_\gamma$ de $\mathbf{N}_k \otimes \mathbf{N}_k$, avec $|\beta| < m$ et $|\gamma| < m$, sont linéairement indépendants sur k. Finalement, on a $c_{\beta+\gamma} = 0$ si $|\beta| > 0$ et $|\gamma| > 0$, c'est-à-dire $c_\alpha = 0$ pour $|\alpha| > 1$; mais comme $c_0 = 0$, la relation (32) se réduit à une relation linéaire entre les Z_α avec $|\alpha| = 1$, c'est-à-dire les u_i; comme les u_i sont linéairement indépendants, on a donc $c_\alpha = 0$ pour tout α, avec $|\alpha| \leq m$, et ceci montre que les Z_α avec $|\alpha| \leq m$ sont linéairement indépendants sur k.

C. Q. F. D.

PROPOSITION 5. — *L'application* $\mathbf{M} \to \mathbf{M} \cap \mathfrak{g}_k$ *est une bijection de l'ensemble des sous-algèbres de* $\mathbf{N}_k$ *telles que* $\Delta(\mathbf{M}) \subset \mathbf{M} \otimes \mathbf{M}$ *sur l'ensemble des p-sous-algèbres de Lie de* $\mathfrak{g}_k$. *De plus,* $\mathbf{M}$ *est une algèbre enveloppante de* $\mathbf{M} \cap \mathfrak{g}_k$.

Soit $\mathbf{M}$ une sous-algèbre de $\mathbf{N}_k$ telle que $\Delta(\mathbf{M}) \subset \mathbf{M} \otimes \mathbf{M}$ et posons $\mathfrak{h} = \mathbf{M} \cap \mathfrak{g}_k$; il est clair que $\mathfrak{h}$ est une p-sous-algèbre de Lie de $\mathfrak{g}_k$. Soit alors $(u_1, \ldots, u_d)$ une base de $\mathfrak{g}_k$ sur k telle que $(u_1, \ldots, u_r)$ avec $0 \leq r \leq d$ soit une base de $\mathfrak{h}$ sur k; nous noterons S' l'ensemble des suites $\alpha \in S$ (même notation que dans la démonstration de la proposition 4) telles que $\alpha_i = 0$ pour $r < i \leq d$.

D'après ce qu'on a rappelé sur les algèbres enveloppantes, l'algèbre $\mathbf{M}'$ engendrée par $\mathfrak{h}$ dans $\mathbf{N}_k$ admet pour base les Z_α avec $\alpha \in S'$. On a évidemment $\mathbf{M}' \subset \mathbf{M}$; de plus $\mathbf{N}_k$ est réunion de la suite croissante des sous-espaces U_m $(m \geq 0)$, où U_m est le sous-espace de $\mathbf{N}_k$ ayant pour base les Z_α avec $|\alpha| \leq m$. On a $\mathbf{M}' \cap U_0 = \mathbf{M} \cap U_0 = k$; supposons qu'on ait $\mathbf{M}' \cap U_m = \mathbf{M} \cap U_m$ pour un entier $m \geq 0$ et soit $u = \sum_{|\alpha| \leq m+1} c_\alpha . Z_\alpha$ un élément de $\mathbf{M} \cap U_{m+1}$; si l'on pose $v = \Delta(u) - u \otimes 1 - 1 \otimes u$, on a $v \in \mathbf{M} \otimes \mathbf{M}$ et, d'après la formule (30), on a

$$v = \sum_\beta Z_\beta \otimes u_\beta, \tag{34}$$

avec

$$u_\beta = \sum_\gamma c_{\beta+\gamma} . Z_\gamma, \tag{35}$$

où le couple $(\beta, \gamma) \in S \times S$ satisfait aux relations

$$0 < |\beta| \leq m+1, \qquad 0 < |\gamma| \leq m+1, \qquad |\beta| + |\gamma| \leq m+1. \tag{36}$$

Comme $v \in \mathbf{M} \otimes \mathbf{M}$, on a $u_\beta \in \mathbf{M}$ dans ces conditions, mais d'après (36), on a $|\beta| \leq m$ et $|\gamma| \leq m$ et comme $\mathbf{M} \cap U_m$ admet pour base les Z_α avec $|\alpha| \leq m$ et $\alpha \in S'$, on a donc $c_{\beta+\gamma} = 0$ dans les conditions (36) si $\gamma \notin S'$. Autrement dit, on a $c_\alpha = 0$ si $\alpha \notin S'$ ou $|\alpha| > 1$; alors u est somme d'un

élément u' de $\mathbf{M}' \cap U_{m+1}$ et d'un élément u'' de $\mathfrak{g}_k$; mais alors on a

$$u'' = u - u' \in \mathfrak{g}_k \cap \mathbf{M}' = \mathfrak{h} \cap \mathbf{M}',$$

d'où finalement

$$u \in \mathbf{M}' \cap U_{m+1}.$$

Ce raisonnement par récurrence démontre l'égalité $\mathbf{M} = \mathbf{M}'$.

Réciproquement, soit $\mathfrak{h}$ une p-sous-algèbre de Lie de $\mathfrak{g}_k$. Choisissons encore une base $(u_1, \ldots, u_d)$ de $\mathfrak{g}_k$ telle que $\mathfrak{h}$ admette $(u_1, \ldots, u_r)$ pour base avec $0 \leq r \leq d$. Les notations S, S' et Z_α ayant la même signification que plus haut, l'algèbre $\mathbf{M}$ engendrée par $\mathfrak{h}$ dans $\mathbf{N}_k$ admet pour base les Z_α avec $\alpha \in S'$. On a par suite $\mathbf{M} \cap \mathfrak{g}_k = \mathfrak{h}$, et comme $\beta + \gamma \in S'$ implique $\beta \in S'$ *et* $\gamma \in S'$, la formule (3o) montre que $\Delta(\mathbf{M})$ est contenu dans $\mathbf{M} \otimes \mathbf{M}$.

C. Q. F. D.

COROLLAIRE. — *Pour toute k-isogénie α définie dans G pour laquelle il existe une isogénie β avec $\iota = \beta \circ \alpha$, le sous-espace $\mathfrak{g}_k(\alpha) = \mathfrak{g}_k \cap \mathbf{N}_k(\alpha)$ est une p-sous-algèbre de Lie de $\mathfrak{g}_k$ telle que $\mathbf{K}.\mathfrak{g}_k(\alpha)$ soit stable par la représentation adjointe de G dans $\mathfrak{g}_\mathbf{K}$, et $\mathbf{N}_k(\alpha)$ est algèbre enveloppante de $\mathfrak{g}_k(\alpha)$. La p-algèbre de Lie $\mathfrak{g}_k(\alpha)$ caractérise α à un isomorphisme près, et l'on obtient ainsi toute p-sous-algèbre de Lie $\mathfrak{h}$ de $\mathfrak{g}_k$ telle que $\mathbf{K}.\mathfrak{h}$ soit stable par la représentation adjointe de G dans $\mathfrak{g}_\mathbf{K}$.*

[*N. B.* — La représentation adjointe de G dans $\mathbf{N}_\mathbf{K}(\iota)$ laisse évidemment stable le sous-espace $\mathfrak{g}_\mathbf{K}$].

Cela résulte des propositions 2 et 5.

REMARQUE. — On démontre immédiatement que, sous les hypothèses du corollaire précédent, $L_k(\alpha)$ est l'ensemble des éléments de $R_k(G)$ annulés par $\mathfrak{g}_k(\alpha)$, et que $\mathfrak{g}_k(\alpha)$ est l'ensemble des éléments de $\mathfrak{g}_k$ nuls sur $L_k(\alpha)$.

(Manuscrit reçu le 24 juillet 1959).

Pierre CARTIER,
Chargé de Recherches au C. N. R. S.,
La Résidence, n° 57,
Orsay (Seine-et-Oise).