Séminaire Claude Chevalley

A. Grothendieck

Généralités sur les groupes algébriques affines. Groupes algébriques affines commutatifs

Séminaire Claude Chevalley, tome 1 (1956-1958), exp. n° 4, p. 1-14

<http://www.numdam.org/item?id=SCC_1956-1958__1__A4_0>

Exposé n° 4

GÉNÉRALITES SUR LES GROUPES ALGÉBRIQUES AFFINES. GROUPES ALGÉBRIQUES AFFINES COMMUTATIFS.

(Exposé de A. GROTHENDIECK, le 26.11.1956)

Le but des prochains exposés est l'exposition des résultats de Borel, Annals Math. 64 n° 1, 1956, page 20-82.

Terminologies et notations.- Pour simplifier, dans toute la suite de ce séminaire, nous supposerons qu'on s'est donné une fois pour toutes un corps de base K algébriquement clos (bien qu'un grand nombre de résultats soient vrais sans cette hypothèse) ; un ensemble algébrique sera alors un (K-K)-ensemble algébrique (exposé 1), une variété est un ensemble algébrique irréductible. Un groupe algébrique n'est pas nécessairement connexe, et n'admet pas nécessairement de représentation linéaire rationnelle fidèle. On appelle groupe algébrique linéaire resp. groupe algébrique de matrices un sous-groupe fermé d'un groupe $G\ell(V)$ (V espace vectoriel de dimension finie) resp. de $G\ell(n, K)$. p désignera l'exposant caractéristique de K, égal à la caractéristique si celle-ci est $\neq 0$, à 1 dans le cas contraire.

1.- Généralités sur les représentations linéaires. Groupes algébriques affines.

Soit G un groupe, u une représentation linéaire de G dans un vectoriel V ; G opère aussi dans le dual V' de V par la représentation contragrédiente de u, le transformé d'un $x \in V$ resp. $x' \in V'$ par $s \in G$ sera noté s.x resp. s.x'. Un coefficient de u est une fonction sur G de la forme

$$u_{x,x'}(s) = \langle s.x , x' \rangle \qquad (x \in V , x' \in V' , s \in G) ;$$

l'espace des coefficients de u est l'espace vectoriel A_u engendré par ses coefficients. G opère sur les fonctions numériques définies sur G par les représentations régulières gauches et droites, définies par

$$L_s f(t) = f(s^{-1}t) \qquad R_s f(t) = f(ts)$$

et on a les formules

$$(1) \qquad L_s u_{x,x'} = u_{x,s.x'} \qquad R_s u_{x,x'} = u_{s.x,x'}$$

ce qui prouve en particulier que l'espace des coefficients A_u est invariant

par translations gauches et droites. Il s'ensuit, si V est de dimension finie (donc A_u de dimension finie), que l'espace vectoriel engendré par les translatés à gauche et à droite d'un coefficient de u est de dimension finie ; réciproquement, soit f une fonction sur G dont les translatés à droite engendrent un espace de dimension finie V, alors f est le coefficient d'une représentation linéaire de dimension finie de G dont l'espace des coefficients est l'espace vectoriel engendré par les translatés gauches et droites de f : il suffit de prendre la représentation u induite sur V par la représentation adjointe droite de G, on a alors $u_{f,\varepsilon}(s) = R_s f(e) = f(s)$ (ε désigne la forme $g \longrightarrow g(e)$ sur V) . Soit toujours V l'espace d'une représentation linéaire u de dimension finie de G, soit (x'_i) un ensemble fini de générateurs de l'espace vectoriel V' ; comme pour $x' \in V'$ fixé, $x \longrightarrow u_{x,x'}$ est une représentation de G-modules de V dans A_u où G opère par les R_s (formule (1)), on obtient une représentation de G-module $V \longrightarrow A_u^I$: $x \longrightarrow (u_{x,x'_i})_{i\in I}$, qui est évidemment injective, et une représentation de G-modules $V^I \longrightarrow A_u$: $(x_i) \longrightarrow \sum_{i\in I} u_{x_i,x'_i}$, qui est évidemment susjective. Donc on a le :

LEMME 1.- Soit V l'espace d'une représentation linéaire u de dimension finie de G, A_u l'espace de ses coefficients, considéré comme G-module par les translations à droite R_s de G. Alors V est isomorphe à un sous-G-module d'un A_u^n, et A_u isomorphe à un G-module quotient de V^n. En particulier les composantes simples de V et A_u (dans une suite de composition des G-modules envisagés) sont les mêmes, et V est semi-simple si et seulement si A_u l'est.

Supposons que G soit un groupe algébrique, soit $A(G)$ l'algèbre des fonctions régulières sur G. Pour qu'une représentation linéaire u de G dans un vectoriel V de dimension finie soit rationnelle, il faut et il suffit que ses coefficients soient des fonctions régulières, i.e. que $A_u \subset A(G)$. D'ailleurs :

LEMME 2.- Soit f une fonction régulière sur G, alors l'espace vectoriel engendré par ses translatées droites est de dimension finie (donc f est le coefficient d'une représentation linéaire rationnelle de G) .

On a en effet $R_s f(t) = f(st)$, c'est là une fonction régulière sur $G\times G$ donc de la forme $\sum g_i(s)\, h_i(t)$, (exposé 1) donc $R_s f$ est combinaison linéaire des h_i , d'où la conclusion. Conjuguant les lemmes 1 et 2 , on trouve :

COROLLAIRE.- Pour que toute représentation linéaire rationnelle de G soit semi-simple, il faut et il suffit que $A(G)$ soit semi-simple pour la représentation régulière droite de G ; les représentations simples de G sont isomorphes aux représentations induites sur des sous-espaces de $A(G)$.

La condition envisagée sur G est vérifiée par exemple si la caractéristique est nulle et G semi-simple. Dans le cas de caractéristique quelconque, un exemple important sera étudié dans le n° 3 .

PROPOSITION 1.- Pour qu'un groupe algébrique soit isomorphe à un groupe linéaire, il faut et il suffit que ce soit un ensemble algébrique affine.

C'est évidemment nécessaire, puisque $G\ell(n , K)$ est un ensemble algébrique affine, et qu'il en est donc de même de toute partie fermée de $GL(n , K)$. Supposons inversement G affine, alors $A(G)$ est une algèbre à engendrement fini, et compte tenu de lemme 2 il existe donc un sous-espace vectoriel V de dimension finie de $A(G)$, engendrant l'algèbre $A(G)$, et invariante sous les R_s . Soit u la représentation rationnelle de G dans V définie par les R_s, je dis que c'est là un isomorphisme de G dans $G\ell(V)$, i.e. que toute fonction régulière sur G provient d'une fonction régulière sur $G\ell(V)$. Or il en est ainsi des $f \in V$ puisque ce sont des coefficients de u , donc de toute $f \in A(G)$ puisque V engendre l'algèbre $A(G)$. Nous dirons dorénavant groupe algébrique affine au lieu de groupe algébrique isomorphe à un groupe linéaire.

2.- Sous-groupes fermés d'un groupe algébrique affine.

THÉORÈME 1.- (Chevalley). Soient G un groupe algébrique affine, H un sous-groupe fermé. Alors il existe un nombre fini d'éléments F_i de $A(G)$ tels que H soit l'ensemble des $s \in G$ admettant les F_i comme semi-invariants dans la représentation linéaire régulière gauche de G dans $A(G)$. On peut supposer que les F_i sont des semi-invariants de même poids sous H . Si G est irréductible, il existe un nombre fini de fonctions rationnelles G_i sur G telles que H soit l'ensemble des $s \in G$ tels que $L_s G_i = G_i$ pour tout i .

Rappelons qu'on dit qu'un élément F d'un espace vectoriel où opère un groupe est semi-invariant sous un $A \in G$ si sF est de la forme $\lambda(s)F$, où $\lambda(s)$ est évidemment bien déterminé si $F \neq 0$; l'ensemble des $s \in G$ admettant F comme semi-invariant est évidemment un sous-groupe, et $\lambda(s)$ est un caractère multiplicatif sur ce sous-groupe, appelé poids du semi-invariant. Démontrons le théorème. Soit $\mathfrak{A}$ l'idéal dans $A(G)$ des fonctions nulles sur H;

cet idéal admet un nombre fini de générateurs, et en vertu du lemme 2, l'espace vectoriel invariant à gauche V engendré par ses générateurs est de dimension finie. Soit $W = V \cap \mathfrak{A}$, ce sous-espace engendre l'idéal $\mathfrak{A}$; de plus comme $\mathfrak{A}$ est évidemment invariant sous les L_s $(s \in H)$, il en est de même de W. Réciproquement, soit $s \in G$ tel que $s.W \subset W$, alors $s \in H$ car pour $f \in W$ on a $L_s f \in W$ d'où $L_s f(e) = 0$ d'où $f(s^{-1}) = 0$, et comme les $f \in W$ engendrent $\mathfrak{A}$, on en conclut $s^{-1} \in H$ et $s \in H$. Soit d la dimension de W, soit E la puissance extérieure d-ième de W, u la représentation de G dans E définie par les L_s, a l'élément de E produit des éléments d'une base de W. Il est bien connu que $L_s W \subset W$ équivaut au fait que a soit un semi-invariant sous $u(s)$. Soit $(e_i)_{0 \leqslant i \leqslant n}$ une base de E avec $e_o = a$, soit $(F_{ij}(s))$ la matrice de $u(s)$ par rapport à cette base, on a en vertu de $u(st) = u(s)u(t)$:

$$F_{oi}(st) = \sum_{j=o}^{n} F_{oj}(s) F_{ji}(t) \tag{2}$$

Soit $F_i = F_{oi}$ $(1 \leqslant i \leqslant n)$. En vertu de ce qui précède, $s \in H$ équivaut à $F_{oi}(s) = 0$ pour $1 \leqslant i \leqslant n$, d'où en vertu de (2) $L_s F_i(t) = F_{oo}(s^{-1}) F_i(t)$, donc les F_i sont bien des semi-invariants sous H, de même poids $F_{oo}(s^{-1})$. Inversement, soit $s \in G$ tel que l'on ait $L_s F_i = \lambda_i F_i$ pour $1 \leqslant i \leqslant n$, d'où $F_i(s^{-1}t) = \lambda_i F_i(t)$ pour tout t, et faisant $t = e$ il vient, puisque $F_i(e) = 0$ pour $i > 0$: $F_i(s^{-1}) = 0$ pour $i > 0$, d'où $s^{-1} \in H$ et $s \in H$. Les F_i satisfont aux conditions voulues. Si G est irréductible, on voit de même que les $G_i = F_i / F_{oo}$ satisfont aux conditions de l'énoncé.

COROLLAIRE.- Soit H un sous-groupe invariant fermé du groupe algébrique affine G, alors il existe une représentation linéaire rationnelle de G de noyau H.

Avec les notations du théorème, soit λ le poids commun des semi-invariants F_i de H ; soit E l'espace vectoriel engendré par les F_i et leurs translatés à gauche par G, il est de dimension finie (lemme 2). Soit E_o le sous-espace vectoriel de E formé des f telles que $L_s f = \lambda(s) f$ pour tout $s \in H$. C'est un sous-espace vectoriel de E contenant les F_i, de plus invariant sous G grâce au fait que H est invariant, donc identique à E. Soit u la représentation linéaire rationnelle de G dans E définie par les L_s, alors $s \in H$ équivaut à dire que $u(s)$ est un scalaire, ou encore que $(\check{u} \otimes u)(s)$ est l'identité : on prendra donc la représentation rationnelle $\check{u} \otimes u$ de G dans $E' \otimes E$ déduite de u, elle satisfait à la condition voulue.

3.- Groupes algébriques diagonalisables.

Soit $D(n)$ le sous-groupe de $G\ell(n, K)$ formé des matrices diagonales, ce sous-groupe est canoniquement isomorphe à K^{*n}, où $K^* = G\ell(\ell, K)$ désigne le groupe multiplicatif des éléments non nuls de K. Un sous-groupe de $G\ell(n, K)$ est dit diagonal s'il est contenu dans $D(n)$, diagonalisable s'il est conjugué à un sous-groupe de $D(n)$; plus généralement une représentation linéaire d'un groupe G dans un vectoriel V (de dimension finie) est dite diagonalisable s'il existe une base telle que l'image de G soit un groupe diagonal par rapport à cette base. Enfin, un groupe algébrique diagonalisable G est un groupe algébrique isomorphe à un sous-groupe de $D(n)$ (il résultera du corollaire 3 au théorème 2 ci-dessous que dans le cas où G est un groupe algébrique de matrices, cette dernière terminologie est compatible avec la précédente). Un tore algébrique est un groupe algébrique isomorphe à K^{*n}.

K^* s'obtient à partir de la variété affine K en enlevant la variété des zéros de la fonction X, donc (exposé 1) $A(K^*) = K[X][1/X]$, donc $A(K^*)$ a pour base sur K les monômes X^n $(n \in \underline{Z})$, qui sont d'ailleurs des caractères rationnels multiplicatifs de K^*. Donc $A(K^{*n})$, isomorphe au produit tensoriel de n copies de $A(K^*)$, a comme base les monômes $X_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$, avec $(k_i) \in \underline{Z}^n$. Ce sont encore des caractères rationnels de K^{*n}, et il n'y en a pas d'autres (à cause de l'indépendance linéaire des caractères). Donc

THÉORÈME 2.- $A(K^{*n})$ a pour base les caractères rationnels de K^{*n}, qui sont les monômes $X_1^{k_1} \dots X_n^{k_n}$ avec $(k_i) \in \underline{Z}^n$. Donc (corollaire du lemme 2) toute représentation linéaire rationnelle de K^{*n} est diagonalisable.

Utilisant maintenant le corollaire du théorème 1, on obtient :

COROLLAIRE 1.- Tout sous-groupe fermé de K^{*n} est l'intersection des noyaux d'un nombre fini de caractères.

Soit D un tore isomorphe à K^{*n}, $\hat{D}$ le groupe de ses caractères, isomorphe au groupe additif Z^n d'après ce qui précède. Posons $\{x, \hat{x}\} = \hat{x}(x)$ pour $x \in D$, $\hat{x} \in \hat{D}$. Pour $A \subset D$, soit A° l'ensemble des $\hat{x} \in \hat{D}$ tels que $\{x, \hat{x}\} = 1$ pour tout $x \in A$, définissons de façon symétrique B° pour une partie $B \subset \hat{D}$. D'après le corollaire 1, si A est un sous-groupe fermé de D, on a $A = (A^\circ)^\circ$. D'autre part, A° est un sous-groupe de $\hat{D}$, tel que $p\hat{x} = A^\circ$ implique $\hat{x} \in A^\circ$ (puisque toute racine p-ième de l'unité est égale a 1). On peut donc trouver une base $(e_i)_{1 \le i \le n}$ de $\hat{D}$ et des entiers n_i $(1 \le i \le r)$ tels que les $n_i e_i$ $(1 \le i \le r)$ forment une base de A° ; et les n_i sont alors premiers à p.

Les e_i définissent un isomorphisme de D sur K^{*n}, et faisant l'identification $D = K^{*n}$, H est défini par les équations $X_i^{n_i} = 1$ $(1 \leqslant i \leqslant r)$, donc est isomorphe au produit de K^{*n-r} et des groupes $u(n_i)$ des racines n_i-ièmes de l'unité, qui sont des groupes cycliques d'ordre n_i (donc premier à p). Réciproquement, un groupe algébrique ayant cette structure est évidemment diagonalisable, donc :

COROLLAIRE 2.- Pour qu'un groupe algébrique G soit diagonalisable, il faut et il suffit qu'il soit isomorphe au produit d'un tore par un groupe abélien fini d'ordre premier à p.

COROLLAIRE 3.- Soient D un groupe algébrique diagonalisable, $\hat{D}$ le groupe des caractères rationnels de D. Alors on a ce qui suit :

a) $\hat{D}$ est une base de $A(D)$, donc toute représentation linéaire rationnelle de D est diagonalisable.

b) $\hat{D}$ est un groupe abélien de type fini dont le groupe de torsion est d'ordre premier à p, et tout groupe abélien ayant ces propriétés est isomorphe à un groupe $\hat{D}$. D s'identifie à l'ensemble des homomorphismes de $\hat{D}$ dans K^*.

c) Les applications $A \longrightarrow A^\circ$ et $B \longrightarrow B^\circ$ définissent des bijections réciproques l'une de l'autre entre l'ensemble des sous-groupes fermés de D, et l'ensemble des sous-groupes de $\hat{D}$ tels que $\hat{D}/B$ n'ait pas de p-torsion. Si A et B se correspondent ainsi, on a $\widehat{D/A} = A^\circ$, $\hat{A} = \hat{D}/A^\circ$.

Prouvons d'abord b). On a $D = F \times D_o$, où F est un groupe abélien fini d'ordre premier à p, et D_o un tore, d'où $\hat{D} = \hat{F} \times \hat{D}_o$. Comme F est d'ordre premier à p, $\hat{F}$ est isomorphe au groupe dual ordinaire de F, et est donc isomorphe (non canoniquement) à F ; d'autre part $\hat{D}_o$ est isomorphe à un groupe Z^n, d'où la structure annoncée pour $\hat{D}$. Il est classique que $\hat{\hat{F}} = F$, de plus $\hat{\hat{D}}_o = D_o$ comme on voit aussitôt en faisant $D = K^{*n}$, d'où aussitôt $\hat{\hat{D}} = \hat{\hat{F}} \times \hat{\hat{D}}_o = F \times D_o = D$. Enfin, un groupe abélien de type fini sans p-torsion est isomorphe à un groupe $F' \times Z^n$, où F' est fini d'ordre premier à p, donc le groupe envisagé est isomorphe au dual de $\hat{F}' \times K^{*n}$.

a) Soit toujours $D = F \times D_o$. $\hat{F}$ est une base de $A(F)$ pour des raisons de dimension, nous avons déjà vu que $\hat{D}_o$ est une base de $A(D_o)$, donc $\hat{F} \times \hat{D}_o$ est une base de $A(F \times D_o) = A(F) \otimes A(D_o)$.

La deuxième assertion résulte du corollaire au lemme 2.

c) Pour établir la première assertion, il suffit de prouver $A^{oo} = A$ et $B^{oo} = B$ pour A et B comme dans l'énoncé. La première assertion se démontre comme le corollaire 1, en utilisant le corollaire au théorème 1 et la partie a) ci-dessus. $B^{oo} = B$ signifie que B est l'intersection des noyaux des homomorphismes de $\hat{D}$ dans K^*, ou encore (passant au quotient par B) que si E est un groupe abélien de type fini sans p-torsion, alors l'intersection des noyaux des homomorphismes de E dans K^* est réduit à 0, ce qui résulte par exemple de b). Enfin la relation $\widehat{D/A} = A^o$ est triviale, et $\hat{A} = \hat{D}/A^o$ se voit ainsi : en vertu de a) et b), $\hat{D}/A^o$ est le groupe dual du groupe des homomorphismes de $\hat{D}/A^o$ dans K, muni de la structure d'ensemble algébrique dont les fonctions régulières sont les combinaisons linéaires des caractères provenant des éléments de $\hat{D}/A^o$; or les groupes en question est manifestement $A^{oo} = A$, muni de la structure induite par D, d'où la conclusion.

Soient D, D' deux groupes algébriques diagonalisables, u un homomorphisme rationnel de D dans D', on désigne par ${}^t u$ l'homomorphisme $\chi \longrightarrow \chi \circ u$ de $\hat{D}'$ dans $\hat{D}$; on a évidemment ${}^t(uv) = {}^t v\, {}^t u$, ${}^t(\text{identité}) = \text{identité}$ ${}^t(u + v) = {}^t u + {}^t v$ (en supposant D, D' écrits additivement). On peut de même à tout homomorphisme $\hat{u} : \hat{D}' \longrightarrow \hat{D}$, faire correspondre un homomorphisme rationnel ${}^t\hat{u}$ de D dans D', en utilisant le corollaire 3, b). On vérifie alors tout de suite :

COROLLAIRE 4.- L'application $u \longrightarrow {}^t u$ est un isomorphisme du groupe des homomorphismes rationnels de D dans D', dans le groupe $\mathrm{Hom}(\hat{D}', \hat{D})$.

PROPOSITION 2.- Soit D un groupe algébrique diagonalisable. Alors pour tout entier n, l'ensemble des éléments x de D tels que $x^n = e$ est un sous-groupe fini, et la réunion de ces sous-groupes est dense dans D. Si D est un tore, q un nombre premier $\neq p$, il suffit de faire parcourir à n l'ensemble des puissances de q.

C'est là une conséquence immédiate de corollaire 2, et du fait que le sous-groupe de K^* formé des racines de l'unité d'ordre une puissance de q est infini, donc dense puisque K^* est de dimension 1.

COROLLAIRE.- Si D est un sous-groupe fermé diagonalisable invariant dans un groupe algébrique connexe G, il est contenu dans le centre.

En effet, pour tout n, le sous-groupe D_n de D formé des éléments d'ordre divisant n est un sous-groupe fini invariant dans G, donc contenu dans le centre de G puisque G est connexe, d'après un raisonnement bien connu.

La réunion des D_n étant dense dans D, et le centre de G étant fermé, la conclusion apparait.

4.- Eléments semi-simples et unipotents.

Soit V un vectoriel de dimension finie. Un endomorphisme x de V est dit semi-simple si V est un module semi-simple sur l'algèbre avec unité engendrée par x dans $L(V, V)$, ou encore (puisque K est algébriquement clos) si x est diagonalisable. Rappelons le fait bien connu : x peut se mettre de façon unique sous la forme $x_s + x_n$, somme d'un endomorphisme semi-simple x_s et d'un endomorphisme nilpotent x_n qui commutent (appelés partie semi-simple et partie nilpotente de x) ; ce sont des polynomes en x (donc tout endomorphisme commutant à x commute à x_s et x_n), de plus les valeurs propres de x et de x_s sont les mêmes. En particulier, x est inversible si et seulement si x_s l'est. Dans ce cas, on peut donc écrire $x = x_s x_u$, où $x_u = \underline{1} + x_s^{-1} x_n$; x_s et x_u commutent, et $x_u = \underline{1}$ + opérateur nilpotent.

DÉFINITION.- Un endomorphisme u de V est dit unipotent s'il est la somme de l'identité et d'un endomorphisme nilpotent, i.e. si toutes ses valeurs propres sont identiques à 1 .

Un tel endomorphisme est donc nécessairement inversible.

PROPOSITION 3.- Soit x un automorphisme de V, alors x se met de façon unique sous la forme $x = x_s x_u$ produit d'un endomorphisme semi-simple et d'un endomorphisme unipotent qui commutent . x_s est la partie semi-simple de x définie plus haut. (x_u s'appelle la partie unipotente de x).

L'existence a été prouvée plus haut, pour l'unicité, posons $x_u = \underline{1} + n$ où n est nilpotent et commute évidemment à x_s, on a donc $x = x_s + x_s n$, c'est là une décomposition de x en somme d'un opérateur semi-simple et d'un opérateur nilpotent qui commutent, donc x_s est la partie semi-simple de x et par suite bien déterminé, donc aussi $x_u = x_s^{-1} x = \underline{1} + x_s^{-1} x_n$. De ces formules on conclut que tout endomorphisme permutant à x permute à x_s et x_u . Tenant compte du fait que le produit de deux opérateurs semi-simples (resp. unipotents) qui commutent est encore semi-simple (resp. unipotent) on conclut :

COROLLAIRE.- Si x et y sont deux endomorphismes de V qui commutent, alors $(xy)_s = x_s y_s$, $(xy)_u = x_u y_u$.

Notons aussi qu'un endomorphisme qui est à la fois semi-simple et unipotent est l'identité.

PROPOSITION 4.- a) Supposons $p \neq 1$. Pour que l'endomorphisme x soit unipotent, il faut et il suffit qu'il soit d'ordre fini égal à une puissance de p . b) Supposons $p = 1$. Pour que l'endomorphisme x soit unipotent, il faut et il suffit qu'il existe une représentation rationnelle u du groupe algébrique K dans V dont l'image contient u . Une telle représentation est ou bien triviale, ou bien un isomorphisme de K sur son image, et si $x \neq 1$ $u(K)$ est le plus petit groupe algébrique fermé contenant x . De plus u est donné par $u(t) = \exp(tn) = \sum_{k=0}^{\infty} t^k n^k/k\,!$, où n est un endomorphisme nilpotent bien déterminé par u .

DÉMONSTRATION.-

a) Si u est d'ordre fini égal à une puissance de p , il en est de même de ses valeurs propres, qui sont donc égales à 1, donc u est unipotent. Si u est unipotent, on a $u = \underline{1} + n$, n nilpotent, donc il existe une puissance q de p telle que $n^q = 0$, d'où $u^q = \underline{1}^q + n^q = \underline{1}$.

b) Soit u une représentation rationnelle de K ; comme K est abélien, on peut trouver une suite de sous-espaces $0 \subset V_1 \subset \ldots \subset V_n = V$ de V stables sous $u(K)$, V_{i-1} de codimension 1 dans V_i $(1 \leq i \leq n)$. La représentation de K dans V_i/V_{i-1} déduite de u est une représentation rationnelle de K dans K^* , donc donnée par un polynome P tel que $P(st) = P(s)P(t)$, d'où résulte facilement $P = 1$. Ainsi les $u(t)$ sont tous unipotents. Supposons x unipotent, donc $x = \underline{1} + m$ avec m nilpotent, posons $\log x = \sum_{k=1}^{\infty} (-1)^{k+1} m^k$, c'est donc un endomorphisme nilpotent, et on peut former $\exp(\log x)$. Comme on a $\exp(\log(1 + N)) = 1 + N$ (identité de séries formelles en N) on a $\exp(\log x) = x$. D'autre part, si n est un endomorphisme nilpotent, $\exp tn = \sum_{k=0}^{\infty} t^k n^k/k\,!$ est une fonction rationnelle en t , multiplicative d'après l'identité bien connue $\exp(T + T')N = (\exp TN)(\exp T'N)$, soit $u_n(t)$; prenant $n = \log x$, on obtient $u_n(1) = \exp \log x = x$. D'ailleurs, si $x \neq 1$, on a $n \neq 0$, et on a pour tout t : $tn = \log \exp(tn)$ (en vertu de l'identité formelle correspondante) $= \log u_n(t) = \sum_{k=1}^{r} (-1)^{k+1} (u_n(t) - \underline{1})^k$ (où $r = \dim V$) , ainsi tn s'exprime par une fonction polynomiale par rapport à $u_n(t)$, donc u_n est un isomorphisme de K sur son image. Il en résulte que cette image est le plus petit groupe algébrique linéaire contenant x : en effet, cela tient au fait que si un sous-groupe fermé de K contient un élément non nul, il est identique à K (puisqu'il contient le groupe engendré par l'élément en question, qui

est un sous-groupe infini, et que K est de dimension 1). Soit enfin u une représentation linéaire rationnelle quelconque de K, montrons qu'elle est de la forme u_n, (où n est évidemment uniquement déterminé par $n = \log u(1)$). Soit en effet $x = u(1)$, on a vu que x est unipotent, et posant $n = \log x$, on a $u_n(1) = x = u(1)$, donc u_n et u coïncident sur le groupe engendré par 1, donc sur K tout entier.

COROLLAIRE 1.- Soit f une représentation rationnelle d'un groupe algébrique linéaire G dans un autre G', alors f transforme les éléments semi-simples (resp. unipotents) en éléments semi-simples (resp. unipotents).

Soit $x \in G$. Si x est semi-simple, x est diagonalisable, donc le sous-groupe fermé H de G qu'il engendre est un groupe algébrique diagonalisable. Donc f induit une représentation linéaire de H qui est diagonalisable (théorème 2, corollaire 3 a) en particulier $f(x)$ est diagonalisable. Si x est unipotent, distinguons deux cas : si $p \neq 1$, x est d'ordre fini égal à une puissance de p en vertu de proposition 4 a), il en est donc de même de $f(x)$ qui est donc unipotent ; si $p = 1$, x est de la forme $u(t)$, où u est une représentation rationnelle de K sont l'image est le plus petit groupe algébrique linéaire contenant x, donc contenue dans G, donc u est une représentation rationnelle de K dans G. Donc $f(x) = (fu)(t)$ est contenu dans l'image d'une représentation rationnelle de K, et est donc unipotent.

Du corollaire 1 résulte en particulier qu'on peut parler d'éléments semi-simples et unipotents d'un groupe algébrique affine sans référence à une réalisation explicite de ce groupe comme groupe algébrique linéaire.

COROLLAIRE 2.- Soit x un endomorphisme unipotent de V, alors le plus petit groupe algébrique linéaire $G(x)$ contenant x est égal au groupe analogue $G(x^m)$ pour tout entier m premier à p.

Ceci résulte aussitôt de la structure explicite de $G(x)$, connue grâce à la proposition 4.

THÉORÈME 3.- Soit G un sous-groupe fermé de $G\ell(V)$, alors pour tout $x \in G$, ses parties semi-simples x_s et unipotente x_u sont dans G.

Pour tout $y \in G\ell(V)$, soit $G(y)$ le plus petit groupe algébrique contenant y. On peut dans l'énoncé ci-dessus remplacer G par $G(x)$, ce qui nous ramène au cas où G est abélien. Soit G_s l'ensemble des parties semi-simples des $y \in G$, alors $G \cup G_s$ est un ensemble d'opérateurs deux à deux permutables. Il existe donc une suite $0 = V_0 \subset V_1 \subset \ldots \subset V_r = V$ de sous-espaces vectoriels de V stables sous $G \cup G_s$, V_{i-1} étant de codimension 1 dans V_i. Notons le

LEMME 3.- Soit $0 = V_0 \subset V_1 \subset \ldots \subset V_r = V$ une suite de composition de l'espace vectoriel V, V_{i-1} de codimension 1 dans V_i $(1 \leq i \leq r)$, soit G un ensemble d'endomorphismes de V tels que pour tout $g \in G$, les V_i soient stables sous g et g_s, supposons enfin l'ensemble G_s des g_s $(g \in G)$ commutatif. Alors il existe une base $(e_1, \ldots, e_r)$ de V telle que pour tout $g \in G$, la matrice de g par rapport à cette base soit triangulaire, et celle de g_s en soit la partie diagonale.

En effet, il est bien connu, puisque les g_s commutent entre eux et sont semi-simples, que l'algèbre d'endomorphismes qu'ils engendrent est semi-simple, donc pour tout i on peut trouver un supplémentaire L_i de V_{i-1} dans V_i stable sous les g_s. Il suffit alors de prendre pour e_i un élément non nul de L_i. Si G est un groupe algébrique, il résulte alors du lemme 3 que $g \longrightarrow g_s$ est une représentation rationnelle u de G à valeurs dans le groupe diagonal $D(r)$. Nous voulons donc montrer que dans le cas actuel (G commutatif) on a $u(G) \subset G$. Or $u(G)$ est un sous-groupe fermé de $D(r)$, et en vertu de la proposition 2, il suffit de prouver que tout élément d'ordre fini m de ce sous-groupe $u(G)$ est dans G. D'ailleurs, en vertu de la structure des groupes algébriques diagonalisables (théorème 2, corollaire 2) m est premier à p. Soit donc $x \in G$ tel que x_s soit d'ordre m ; de $x = x_s x_u$ on tire $x^m = x_s^m x_u^m = x_u^m$, d'où $x_u^m \in G$ et par suite, en vertu de la proposition 4 corollaire 2, $x_u \in G$, d'où $x_s = x x_u^{-1} \in G$. C.Q.F.D.

Il résulte du théorème 3 que si G est un groupe algébrique affine, tout $x \in G$ se met de façon unique sous la forme $x = x_s x_u$ du produit d'un élément semi-simple et d'un élément unipotent qui commutent, et qui sont donc définis en fonction de x sans référence à une réalisation explicite de G comme groupe algébrique linéaire : on les appelle encore <u>partie semi-simple et partie unipotente de</u> x. Si G est un groupe affine, on désigne par G_s (resp. G_u) l'ensemble de ses éléments semi-simples (resp. unipotents). On a donc $G_s \cap G_u = \{e\}$, $G_s G_u = G_u G_s = G$.

COROLLAIRE.- Soit f une représentation rationnelle d'un groupe algébrique affine G dans un autre G'. Pour tout $x \in G$, on a

$$f(x)_s = f(x_s) \qquad f(x)_u = f(x)_u$$

Tout élément semi-simple (resp. unipotent) de $f(G)$ est image d'un élément semi-simple (resp. unipotent) de G.

Les formules écrites sont conséquence immédiate de la définition et du corollaire 1 de la proposition 4. La dernière assertion en résulte immédiatement.

5.- Groupes algébriques affines commutatifs.

THÉORÈME 4.- Soit G un groupe algébrique affine commutatif. Alors G_s et G_u sont des sous-groupes fermés de G, et G s'identifie à leur produit direct.

Nous avons déjà vu, comme conséquence de lemme 3, que $x \longrightarrow x_s$ est une représentation rationnelle de G dans G, et évidemment de G sur G_s, donc $x \longrightarrow x_u = xx_s^{-1}$ est une représentation rationnelle de G sur G_u. Donc G_s et G_u sont des sous-groupes fermés de G ; d'autre part l'application naturelle $(s , u) \longrightarrow su$ de $G_s \times G_u$ dans G est un homomorphisme rationnel, et $x \longrightarrow (x_s , x_u)$ en est un homomorphisme rationnel réciproque.

C.Q.F.D.

REMARQUE.- L'étude de la structure des groupes algébriques affines commutatifs est donc ramenée, grâce au théorème 4 et au n° 3, à celle des groupes algébriques commutatifs unipotents (un groupe algébrique est dit unipotent si tout ses éléments sont unipotents). En caractéristique 0, il résulte facilement de la proposition 4 qu'un tel groupe est isomorphe à un K^n (et en particulier, il est connexe). En caractéristique $\neq 0$, un groupe unipotent commutatif n'est pas nécessairement connexe (exemple : $Z/(p)$) et même s'il est connexe et de dimension 2, il n'est pas nécessairement isomorphe à un K^n (ce sera alors une extension abélienne non triviale de K par K). Chevalley a montré qu'on peut classifier les groupes algébriques affines commutatifs unipotents à "isogénie près" comme produits de "groupes de Witt" dont les dimensions sont bien déterminées (à l'ordre près) par le groupe donné. Notons que la source de cette différence entre le cas $p = 1$ et $p \neq 1$ semble le fait que si $p \neq 1$, il y a d'autres représentations rationnelles de K dans lui-même que les homothéties, savoir toutes les applications du type $t \longrightarrow t^{p^k}$ et leurs combinaisons linéaires à coefficients dans K (on voit facilement d'ailleurs qu'il n'y en a heureusement plus d'autres). D'où dans K^n un grand nombre de sous-groupes à un paramètre d'allure bizarre ; d'autre part les automorphismes de K^n considéré comme groupe algébrique ne sont en général pas linéaires.

Pour finir, nous donnons un résultat d'intérêt surtout technique, dont la démonstration n'utilise pas d'ailleurs les théorèmes 3 et 4.

PROPOSITION 5.- Soient G un groupe algébrique affine, N un sous-groupe invariant fermé commutatif. Pour tout $g \in G$, soit σ_g l'automorphisme $n \longrightarrow gng^{-1}$ de N qu'il définit, et soient N'_g resp. N''_g le noyau et l'image de l'endomorphisme $n \longrightarrow \gamma_g n = (\sigma_g n)n^{-1} = gng^{-1}n^{-1}$ de N. Si g est semi-simple (resp. unipotent) et si $N = N_u$ (resp. $N = N_s$) on a $N'_g N''_g = e$, et

γ_g est un homomorphisme bijectif de N''_g sur lui-même ; si de plus N est connexe, alors on a $N = N'_g N''_g$ et N'_g et N''_g sont connexes.

Comme N est commutatif, γ_g est évidemment un homomorphisme rationnel de N dans lui-même, donc N'_g et N''_g sont des sous-groupes fermés de N dont la somme des dimensions est égale à la dimension de N (exposé 3) . Si on prouve que $N'_g \cap N''_g = e$, il s'ensuit que γ_g est injectif sur N''_g , donc bijectif pour des raisons de dimensions, (car $\gamma_g(N''_g)$ est un sous-groupe fermé de N''_g qui a même dimension que N''_g ; l'image par γ_g de la composante $N''_{g,o}$ se e dans N''_g est donc $N''_{g,o}$ tout entier, d'où $\gamma_g(N''_g) = N''_g$ puisque γ_g est injectif). De plus l'application $(n' , n'') \longrightarrow n'n''$ de $N'_g \times N''_g$ dans N est alors une représentation rationnelle injective, dont l'image a donc la dimension dim. N , et est par suite identique à N si N est connexe. Comme la composante connexe de e dans $N'_g \times N''_g$ est transformée en la composante connexe de e dans N , on en conclut aussi que N'_g et N''_g sont connexes. Il reste donc à prouver seulement, sous les conditions indiquées, que $N'_g \cap N''_g = (e)$. Soit donc $n \in N$ tel que $\gamma_g n \in N'_g$, et montrons que $\gamma_g n = e$. Soit M le sous-groupe fermé de N engendré par N'_g et n , on a alors $\sigma_g n \in N'_g n$ et σ_g induit (par définition de N'_g) l'identité sur N'_g . Ainsi g normalise M , et σ_g induit l'identité sur $M' = N'_g$ et sur M/M' . Notre assertion résulte alors du résultat plus général :

COROLLAIRE 1.- Soient G un groupe algébrique affine, M un sous-groupe fermé, M' un sous-groupe fermé invariant de M , g un élément de G appartenant au normalisateur de M , et tel que l'automorphisme $\sigma_g : m \longrightarrow gmg^{-1}$ de M induise l'identité sur M' , et sur M/M' . Si de plus g est semi-simple (resp. nilpotent) et si $M' = M'_u$ (resp. $M' = M'_s$) alors g centralise M .

L'ensemble des $x \in G$ normalisant M et tels que $\sigma_x : m \longrightarrow xmx^{-1}$ soit un automorphisme de M induisant l'identité sur M' et sur M/M' est un sous-groupe fermé de G contenant g , donc contenant le plus petit sous-groupe fermé H de G contenant g . Comme les g^n $(n \in Z)$ sont aussi semi-simples (resp. unipotents) et que H est abélien, il s'ensuit que $H = H_s$ (resp. $H = H_u$) . Soit $m \in M$, nous voulons montrer que tout $x \in H$ centralise m , i.e. que $f_m(x) = m^{-1}xmx^{-1}$ est l'identité. Or par construction de H on a $f_m(x) \in M'$, et on vérifie aussitôt que $f_m(xy) = f_m(x)f_m(y)$. Donc f_m est un homomorphisme rationnel de H dans M' . Il transforme donc les éléments semi-simples en éléments semi-simples, les éléments unipotents en éléments unipotents, et est donc réduit à la représentation triviale en vertu des hypothèses faites. C.Q.F.D.

Dans le même ordre d'idées, signalons le

COROLLAIRE 2.- Soient T un tore, H un sous-groupe de T, u un automorphisme d'ordre fini m de T, induisant l'identité sur H et T/H. Alors u est l'identité.

En vertu de la proposition 2, il suffit de prouver que pour tout entier n premier à m, u induit l'identité sur le sous-groupe T_n de T formé des éléments t tels que $t^n = e$. Or si $t \in T_n$, on a $u(t) = ts$, où $s \in T_n \cap H$, d'où $u^i(t) = ts^i$ pour tout i, d'où pour $i = m$: $s^m = e$ d'où enfin $s = e$ puisque s est d'ordre premier à m.