Séminaire Claude Chevalley

M. Lazard

Groupes algébriques (généralités)

Séminaire Claude Chevalley, tome 1 (1956-1958), exp. n° 3, p. 1-7
<http://www.numdam.org/item?id=SCC_1956-1958__1__A3_0>

Séminaire C. CHEVALLEY
E.N.S., 1956/57
-:-:-:-

Exposé n° 3

GROUPES ALGÉBRIQUES (GÉNÉRALITES)

(Exposé de M. LAZARD, le 19.11.1956)

1.- Lorsqu'on sait définir une catégorie de variétés, les produits de variétés et les morphismes (applications régulières), on en déduit par un procédé standard une catégorie de groupes.

DÉFINITION 1.- Un ensemble G est appelé un groupe algébrique sur le corps (algébriquement clos) K s'il est muni d'une structure de variété (sur K) et d'une structure de groupe telles que les applications :

$$G \times G \longrightarrow G \quad \text{définie par} \quad (x , y) \longrightarrow xy$$

et

$$G \longrightarrow G \quad \text{définie par} \quad x \longrightarrow x^{-1}$$

soient des morphismes.

(La condition que le corps K soit algébriquement clos ne sera pas utilisée pour certains des résultats que nous énoncerons, ceux du n° 2 par exemple).

EXEMPLE.- Le groupe des automorphismes linéaires d'un espace vectoriel V de dimension n sur K est un groupe algébrique, que nous noterons $GL(n , K)$. Un élément de $GL(n , K)$ peut être déterminé par les coefficients u_{ij} de la matrice correspondante pour une certaine base de V ; $GL(n , K)$ apparait alors comme un ouvert de K^{n^2} (d'où il faut retrancher la sous-variété d'équation $\det(u_{ij}) = 0$) . On peut aussi identifier $GL(n , K)$ à une variété affine dans K^{n^2+1} , en introduisant une coordonnée v , avec $v = (\det(u_{ij}))^{-1}$.

Les sous-groupes algébriques de $GL(n , K)$ sont, par définition, les groupes algébriques affines (par exemple les groupes orthogonaux, symplectiques, le groupe des matrices diagonales, ...).

2.- THÉORÈME 1.- Soit H un sous-groupe fermé d'une variété de groupe G ; alors H possède un sous-groupe H_o et un seul qui est à la fois fermé, irréductible et d'indice fini ; H_o est invariant dans H . C'est la composante connexe de l'élément neutre dans H , et les composantes de H sont les classes modulo H_o.

DÉMONSTRATION.- L'ensemble H est la réunion finie de ses composantes irréductibles. Soient $A_1 , \ldots , A_r$ celles de ces composantes qui contiennent l'élément neutre e . Dans $G^n = G \times \ldots \times G$, la partie $A_1 \times \ldots \times A_r$ est fermée

et irréductible. Le morphisme $G^r \longrightarrow G : (x_1, \ldots, x_r) \longrightarrow x_1 \ldots x_r$ applique $A_1 \times \ldots \times A_r$ sur $A_1 \ldots A_r$ qui est par suite irréductible ; cet ensemble est donc contenu dans l'une des composantes de H, soit dans A_1. Comme tous les A_i contiennent e, on a $A_1 \cup \ldots \cup A_r \subset A_1 \ldots A_r \subset A_1$, ce qui prouve que $r = 1$ et que A_1 (noté désormais H_o) est l'unique composante irréductible de H contenant e. Puisque $y \longrightarrow xy$ et $y \longrightarrow yx$ sont des morphismes, l'unique composante de H contenant un $x \in H$ est $xH_o = H_o x$, ce qui prouve que H_o est un sous-groupe invariant d'indice fini. Si H' est un sous-groupe fermé, irréductible et d'indice fini de H, on a $H' \subset H_o$, $[H_o : H'] < \infty$; comme H_o est irréductible et est la réunion de ses classes modulo H', on a $H' = H_o$.

Nous dirons désormais que H_o est <u>la composante connexe</u> (sous-entendu : de l'élément neutre) de H. Les sous-groupes fermés d'indices finis de H sont les sous-groupes qui contiennent H_o.

3.- Rappelons qu'un sous-ensemble A d'une variété algébrique est dit <u>épais</u> s'il est irréductible et s'il contient une partie relativement ouverte non vide de son adhérence $\bar{A}$.

Si V et W sont des variétés, A et B des parties épaisses de V et de W, $A \times B$ est épais dans $V \times W$.

Si A est épais dans V, et si f est un morphisme de V dans W, $f(A)$ est épais dans W. Ce résultat suppose essentiellement le corps de base algébriquement clos ; pour la démonstration, cf. séminaire 1955/56, exposé 7, théorème 3, page 9.

<u>LEMME.- Soient H un sous-groupe fermé connexe d'un groupe algébrique et A un ensemble épais dense dans H. Alors $H = AA$ (i.e. tout élément de H est un produit de deux éléments de A).</u>

Soit $x \in H$. Les parties A et xA^{-1} sont épaisses et ont pour adhérence H ; elles contiennent donc deux parties relativement ouvertes dans H, et leur intersection est non vide puisque H est irréductible (comme sous-groupe connexe). Si $a_1 \in A \cap xA^{-1}$, on a $x = a_1 a_2$ avec un $a_2 \in A$.

<u>COROLLAIRE.- Tout sous-groupe épais d'un groupe algébrique est fermé.</u>

<u>THÉORÈME 2.- Soient G un groupe algébrique, et $(A_1, \ldots, A_r)$ une famille finie de parties épaisses de G contenant chacune l'élément neutre e. Alors le sous-groupe H engendré par $A_1, \ldots, A_r$ est fermé connexe.</u>

DÉMONSTRATION.- On voit d'abord en utilisant le morphisme $(x_1 , \dots , x_r) \longrightarrow x_1 \dots x_r$ que H est engendré par l'unique ensemble épais $A_1 \dots A_r = A$ contenant e . On peut de même remplacer A par $B = AA^{-1}$. Tout élément de H est alors produit d'une famille finie d'éléments de B , soit $H = \bigcup_n B^n$, où B^n est l'ensemble des produits de n éléments de B . Or, pour tout entier n , B^n est épais et $B^n \subset B^{n+1}$. La suite des adhérences $\bar{B} \subset \dots \subset \bar{B}^n \subset \bar{B}^{n+1} \subset \dots$ est stationnaire, sinon les dimensions de ces sous-variétés iraient en croissant indéfiniment. Par conséquent, il existe un n tel que $\bar{B}^n = \bar{B}^{n+m}$ pour $m \geqslant 0$. Il est clair que $\bar{B}^n = \bar{H}$, puisque H est la réunion des B^{n+m} ; donc B^n est épais et son adhérence est le sous-groupe connexe $\bar{H}$. D'après le lemme, $B^{2n} = \bar{H}$, donc, en particulier, $H = B^{2n} = \bar{H}$.

COROLLAIRE.- Soient A et B deux sous-groupes fermés d'un groupe algébrique tels que B soit dans le normalisateur de A . Alors le sous-groupe AB est fermé.

Soient en effet A_o et B_o les composantes connexes de A et de B . Puisque $bAb^{-1} = A$ si $b \in B$, on a $bA_ob^{-1} = A_o$ (théorème 1) . Donc A_oB_o est un sous-groupe fermé connexe (théorème 2) . Si $a_1 , \dots , a_r$ et $b_1 , \dots , b_s$ sont des représentants des classes de A et de B modulo A_o et B_o respectivement, AB est la réunion finie des fermés $a_iA_oB_ob_j$, et est par suite fermé.

4.- Etant donnés deux sous-groupes A et B d'un groupe G , leur groupe de commutateurs (A , B) est engendré par les éléments $aba^{-1}b^{-1}$, où $a \in A$, $b \in B$.

Rappelons qu'un groupe ("abstrait") G est dit résoluble (resp. nilpotent) s'il admet une suite de composition

$$G = H_1 \supset H_2 \supset \dots \supset H_n \supset H_{n+1} = \{e\} \tag{1}$$

telle que

$$(H_i , H_i) \subset H_{i+1} \qquad (\text{resp. } (G , H_i) \subset H_{i+1})) . \tag{2}$$

DÉFINITION 2.- Un groupe algébrique G est dit résoluble (resp. nilpotent) s'il admet une suite de composition (1) constituée par des sous-groupes fermés et vérifiant la condition (2) .

THÉORÈME 3.- Pour qu'un groupe algébrique soit résoluble (resp. nilpotent), il faut et suffit qu'il soit résoluble (resp. nilpotent) en tant que groupe abstrait.

DÉMONSTRATION.- Parmi les suites de composition (1) satisfaisant aux conditions (2), il en est qui décroissent plus vite que toutes les autres. On les obtient en posant, dans le cas des groupes résolubles, $H_2 = (G , G) , \dots , H_{i+1} = (H_i , H_i) , \dots$ et, dans le cas des groupes nilpotents, $H_2 = (G , G) , \dots , H_{i+1} = (G , H_i)$. Le théorème 3 est alors une conséquence du résultat suivant :

PROPOSITION 1.- Si A et B sont deux sous-groupes invariants fermés d'un groupe algébrique, leur groupe des commutateurs (A , B) est fermé.

Traitons d'abord le cas où A est connexe. Soient $B_0 , B_1 , \dots , B_n$ les composantes de B . Pour tout i , l'ensemble des $aba^{-1}b^{-1}$ (avec $a \in A$, $b \in B_i$) est épais, comme image de $A \times B_i$ par un morphisme ; de plus, il contient e (faire a = e) . Nous sommes donc dans les conditions d'application du théorème 2 , et le groupe (A , B) est fermé connexe.

Dans le cas général, soient A_0 et B_0 les composantes connexes de A et B . Nous venons de voir que (A_0 , B) et (A , B_0) sont fermés connexes. Il en est de même de leur produit $(A_0 , B)(A , B_0)$. Or $[A : A_0]$ et $[B : B_0]$ sont finis, et un résultat de R. Baer (cf. appendice, proposition 2) montre que $AB/((A_0 , B)(A , B_0))$ est fini. Il en résulte que (A , B) est fermé et que $(A_0 , B)(A , B_0)$ est sa composante connexe.

5.- THÉORÈME 4.- Soient G et G' deux groupes algébriques, $f : G \longrightarrow G'$ un homomorphisme de groupes algébriques (i.e. un homomorphisme en tant que groupes "abstraits" et un morphisme en tant que variétés algébriques). Alors :

1) le noyau N de f est un sous-groupe fermé de G ;

2) l'image $f(G)$ est un sous-groupe fermé de G' , et sa composante connexe est l'image $f(G_0)$ de la composante connexe de G ;

3) $\dim N + \dim f(G) = \dim G$.

DÉMONSTRATION.- Le noyau N est l'image réciproque de l'élément neutre e' de G' . Il est donc fermé.

L'image $f(G_0)$ du sous-groupe connexe G_0 est un sous-groupe épais, donc fermé.

Pour démontrer le 3), nous utiliserons un résultat du séminaire 55/56 (exposé 8, théorème 2, page 3) , qui peut se traduire ainsi dans le langage des variétés que nous considérons : soient $f : V \longrightarrow W$ un morphisme de cariétés tel que $\overline{f(V)} = W$, et $e = \dim V - \dim W$. Alors, si W' est une sous-variété de W et V' une composante de $f^{-1}(W')$ telle que $W' = \overline{f(V')}$, on

a dim $V' \geqslant \dim W' + e$; de plus, la réunion des sous-variétés V' de V telles que $\dim V' > \dim \overline{f(V')} + e$ est un fermé non dense de V. Nous pouvons prendre $V = G_o$, $W = f(G_o)$, avec $\dim V = \dim G$, $\dim W = \dim f(G)$, $\dim N = \dim (N \cap V)$. La première partie du théorème donne, pour $W' = e'$, : $\dim N \geqslant \dim G - \dim f(G)$. La seconde partie donne, pour un x convenable de G, $\dim xN \leqslant \dim G - \dim f(G)$; comme $\dim xN = \dim N$, la démonstration est achevée.

Enonçons enfin un théorème qui sera démontré ultérieurement.

THEOREME 5.- Soient G un groupe algébrique, $H \subset G$ un sous-groupe fermé. Il existe une variété G/H et un morphisme $\pi : G \longrightarrow G/H$ tels que :
1) la condition $\pi(x) = \pi(y)$ soit équivalente à $x^{-1}y \in H$ $(x , y \in G)$;
2) si $f : G \longrightarrow V$ est un morphisme de G dans une variété V tel que $x^{-1}y \in H$ entraîne $f(x) = f(y)$, f se factorise sous la forme $g \circ \pi$, où $g : G/H \longrightarrow V$ est un morphisme. Si H est invariant dans G, G/H est un groupe algébrique et π un homomorphisme.

APPENDICE.

Soient G un groupe et H un sous-groupe de G. Un système de représentants des classes à gauche xH est une application de G sur une partie $\bar{G}$ de G (application notée $x \longrightarrow \bar{x}$) telle que : 1) si $x \in G$, $x^{-1}\bar{x} \in H$; 2) si $x , y \in G$, une condition nécessaire et suffisante pour que $x^{-1}y \in H$ est que $\bar{x} = \bar{y}$. Il en résulte que $\bar{\bar{x}} = \bar{x}$ et $\overline{\bar{x}\bar{y}} = \overline{xy}$. Un autre système de représentants $x \longrightarrow \bar{x}^*$ est défini d'une manière générale en posant $\bar{x}^* = \bar{x}\,\varphi(\bar{x})$, où $\varphi : \bar{G} \longrightarrow H$ est une application quelconque.

Supposons maintenant H abélien et d'indice $[G : H]$ fini. On définit une application $T : G \longrightarrow H$ (transfert de G dans H) en posant, pour $x \in G$,

$$(1) \qquad T(x) = \prod_{\bar{y} \in \bar{G}} (\overline{x\bar{y}})^{-1} x\bar{y} \quad .$$

Le transfert ne dépend pas du choix du système de représentants. En effet $\bar{y} \longrightarrow \overline{x\bar{y}}$ est, pour tout $x \in G$, une permutation de $\bar{G}$. Si on remplace $\bar{y}$ par $\bar{y}\,\varphi(\bar{y})$, comme plus haut, $T(x)$ est remplacé par

$$\prod_{\bar{y} \in \bar{G}} \varphi(\overline{x\bar{y}})^{-1} (\overline{x\bar{y}})^{-1} x\bar{y}\ \varphi(\bar{y}) = \left(\prod_{\bar{y} \in \bar{G}} \varphi(\overline{x\bar{y}})^{-1}\, \varphi(\bar{y})\right) T(x) = T(x) \quad .$$

De plus, T est un homomorphisme. En effet, si $x , x' \in G$,

$$T(xx') = \prod_{\bar{y} \in \bar{G}} \overline{(xx'y)}^{-1} xx'\bar{y} = \prod_{\bar{y} \in \bar{G}} (\overline{(xx'y)}^{-1} x\, \overline{x'y})(\overline{(x'y)}^{-1} x'\bar{y}) = T(x)T(x') .$$

Supposons maintenant que H soit le centre Z de G et que $[G : Z] = n$. Soient x un élément de G et j l'ordre de x modulo Z. Nous choisirons un système de représentants des classes suivant Z composé de n/j familles de la forme $(\bar{y} , x\bar{y} , \ldots , x^{j-1}\bar{y})$. Le produit des facteurs correspondants dans $T(x)$ est alors $\bar{y}^{-1}x^j\bar{y} = x^j$ puisque $x^j \in Z$; donc $T(x) = (x^j)^{n/j} = x^n$. On en conclut que, si $[G : Z] = n < \infty$, l'application $T : x \longrightarrow x^n$ est un homomorphisme de G dans Z ; comme Z est abélien, $T(x) = 1$ pour x dans le groupe des commutateurs de G.

Revenons au cas d'un groupe G et d'un sous-groupe H d'indice $n = [G : H]$ fini. Supposons que G possède p générateurs $s_1 , \ldots , s_p$ et choisissons un système de représentants $\bar{y}$ de G modulo H tel que $\bar{1} = 1$. Alors les np éléments $(\overline{s_i y})^{-1} s_i \bar{y}$ $(1 \leq i \leq p , \bar{y} \in \bar{G})$ engendrent H. En effet, soit $x = s_{i_1}^{e(1)} \ldots s_{i_r}^{e(r)}$ un élément de H $(1 \leq i_1 , \ldots , i_r \leq p , e(k) = \pm 1)$. Posons $x_k = s_{i_k}^{e(k)} \ldots s_{i_r}^{e(r)}$, d'où $x_1 = x$, $x_{r+1} = 1$. Posons $u_k = \bar{x}_k^{-1} s_{i_k}^{e(k)} \bar{x}_{k+1}$; on a alors $x = u_1 \ldots u_r$, car $\bar{x}_{r+1} = \bar{1} = 1$. Suivant que $e(k)$ est $+1$ ou -1, u_k ou son inverse est de la forme $(\overline{s_i y})^{-1} s_i \bar{y}$, ce qui démontre l'assertion. On en conclut que tout sous-groupe d'indice fini d'un groupe de type fini est lui-même de type fini.

PROPOSITION 1.- Soient G un groupe, et Z son centre, qui est supposé d'indice $n = [G : Z]$ fini. Alors le groupe des commutateurs $(G , G) = G'$ est fini.

Les commutateurs (x , y) sont définis par $(x , y) = xyx^{-1}y^{-1}$; G' est engendré par les éléments (x , y) pour $x , y \in G$. Les identités

$$(2) \qquad \begin{aligned} (x , yy') &= (x , y)(y , (x , y'))(x , y') \\ (xx' , y) &= (x , (x' , y))(x' , y)(x , y) \end{aligned}$$

montrent que (x , y) ne dépend que des classes de x et de y modulo Z ; G' est donc de type fini. L'indice de $G' \cap Z$ dans G' est $[G' : G' \cap Z] = [G'Z : Z]$ et est donc fini. Le groupe $G' \cap Z$ est alors un groupe abélien de type fini dont tout élément x vérifie $x^n = 1$ (d'après le transfert de G

dans Z) ; donc $G' \cap Z$ est fini. Comme $[G' : G' \cap Z]$ est fini, il en résulte que G' est fini.

Si M et N sont deux sous-groupes invariants d'un groupe G , nous désignerons par (M , N) leur groupe des commutateurs, engendré par les (m , n) où $m \in M$, $n \in N$. On a $(M , N) \subset M \cap N$.

PROPOSITION 2.- Soient M , N , M_o et N_o des sous-groupes invariants d'un groupe G . Si $M_o \subset M$, $N_o \subset N$ et si les groupes $M/(M_o(M , N_o))$ et $N/(N_o(N , M_o))$ sont finis, le groupe $(M , N)/((M , N_o)(N , M_o))$ est fini.

Passons d'abord au quotient modulo $(M , N_o)(N , M_o)$, i.e. supposons que $(M , N_o) = (N , M_o) = \{1\}$; soit $[M : M_o] = i$, $[N : N_o] = j$. Il faut montrer que le groupe $H = (M , N)$ est fini.

Le groupe H est de type fini. En effet les identités (2) montrent que, pour $m \in M$ et $n \in N$, (m , n) ne dépend que des classes de m et n modulo M_o et N_o respectivement.

Comme $H = (M , N) \subset M \cap N$, tout élément de H commute avec tout élément de M_o et tout élément de N_o ; les groupes $H \cap M_o$ et $H \cap N_o$ sont donc dans le centre de H ; comme $H/(H \cap M_o)$ est isomorphe au sous-groupe HM_o/M_o de M/M_o , il est fini, et on voit de même que $H \cap N_o$ est d'indice fini dans H . Le centre de H est donc d'indice fini dans H , d'où il résulte (proposition 1) que le groupe des commutateurs $H' = (H , H)$ est fini. Comme H/H' est abélien de type fini, il ne reste plus qu'à majorer les ordres des éléments de H/H' . Soient $m \in M$, $h \in H$. Montrons que $(m , h)^j \in H'$. On a $h^j \in N_o$, d'où $mh^j m^{-1} = h^j$. Or on a

$$mhm^{-1} = (m , h)m \qquad h^j = mh^j m^{-1} \equiv (m , h)^j h^j \pmod{H'}$$

Ainsi $(m , h)^j \in H'$ et de même, pour $n \in N$, $(n , h)^i \in H'$. La relation

$$(m , n^k) = (m , n^{k-1})(n^{k-1} , (m , n))(m , n)$$

montre par récurrence que

$$(3) \qquad (m , n^k) \equiv (m , n)^k \prod_{r=1}^{k-1} (n^r , (m , n)) \pmod{H'} .$$

Pour $k = j$, $(m , n^k) = 1$ puisque $n^j \in N_o$. Faisons $k = j$ dans (3) , puis élevons à la puissance i . Compte tenu des relations $(n^r , (m , n))^i \in H'$, il vient $(m , n)^{ij} \in H'$, ce qui prouve que (m , n) est d'ordre fini modulo H' .