Armand Borel

Groupes algébriques

Séminaire N. Bourbaki, 1956, exp. nº 121, p. 229-238
<http://www.numdam.org/item?id=SB_1954-1956__3__229_0>

Séminaire BOURBAKI
(Décembre 1955)

GROUPES ALGÉBRIQUES.

par Armand BOREL

Un groupe algébrique sera dans cet exposé un groupe de matrices à coefficients dans un corps universel (i.e. algébriquement fermé et de degré de transcendance infini sur son corps premier) Ω, qui est là totalité des éléments inversibles d'un ensemble algébrique de l'espace $M(n, \Omega)$ des matrices carrées d'ordre n. On se propose ici de discuter ces groupes d'un point de vue "global" qui ne fait pas intervenir l'algèbre de Lie. Les résultats valent en caractéristique p quelconque ; pour simplifiér, on laissera de côté leur extension aux groupes à coefficients dans un corps algébriquement fermé quelconque et celle de certains d'entre eux aux variétés de groupe.

1. Généralités.

Dans le groupe linéaire général $GL(n, \Omega)$, on utilise la topologie de Zariski un fermé étant donc l'intersection de $GL(n, \Omega)$ avec un ensemble algébrique de $M(n, \Omega)$. On démontre que l'ensemble algébrique sous-jacent à un groupe algébrique G est irréductible si et seulement s'il est connexe ; la composante connexe de e dans G sera notée G_o ; c'est un sous-groupe invariant fermé d'indice fini dans G.

Une représentation rationnelle $f : G \to GL(m, \Omega)$ est un homomorphisme (de groupes abstraits) dont la restriction à chaque composante connexe de e est une application rationnelle partout définie (en fait on peut (cf. [5], [8] et [9]) postuler moins, mais c'est sans importance ici). L'image de f est un sous-groupe fermé de $GL(m, \Omega)$, connexe si G l'est. Le noyau N de f est un sous-groupe invariant fermé de dimension égale à $\dim G - \dim f(G)$. Inversement ([2b], p. 119) :

1.1. - Soient G un groupe algébrique et N un sous-groupe invariant fermé de G. Alors il existe une représentation rationnelle de G ayant le noyau N.

La démonstration s'appuie principalement sur le fait ([2a], p. 85) qu'un groupe algébrique peut être caractérisé par un nombre fini de semi-invariants (que l'on peut supposer de même poids, comme le montre la démonstration). Un semi-invariant d'un sous-ensemble $M \subset M(n, \Omega)$ est un polynôme sur $M(n, \Omega)$ vérifiant $P(x.m) = \chi(m) P(x)$, $(x \in M(n, \Omega)$, $m \in M$; $\chi(m) \in \Omega)$; la fonction χ

est le poids de P.

2. Tores.

$D(n)$ dénote le sous-groupe des matrices diagonales de $GL(n, \Omega)$. Un groupe linéaire est diagonal (resp. diagonalisable), s'il est contenu dans $D(n)$ (resp. conjugué à un sous-groupe de $D(n)$). Un groupe algébrique connexe diagonalisable sera appelé tore.

PROPOSITION 2.1. - Soient G un groupe algébrique diagonal. Alors G peut être défini par un nombre fini d'équations monomiales $x_1^{m_1} \cdots x_n^{m_n} = 1$, ($m_i$ entiers). S'il est connexe de dimension d, il est isomorphe à $(\Omega^*)^d$.

Soit V l'espace des semi-invariants de G de poids χ et de degré $\leq m$, χ et m étant tels que G soit caractérisé par ces semi-invariants. Il est invariant par $D(n)$ et est l'espace d'une représentation diagonale η de ce dernier, dont les coefficients sont des monômes en les coeffcients x_i, à exposants entiers $\geqslant 0$. Soit ζ la représentation de $D(n)$ dans l'espace des endomorphismes de V définie par $\zeta(X) = \eta(x).X.\eta(x^{-1})$. Elle se met sous forme diagonale et a alors des coefficients monômes à exposants entiers, et $\zeta(x) = 1$ si et seulement si $x \in G$. Soit maintenant G connexe. Alors, si g est générique, toute puissance g^m (m entier $\neq 0$) de g l'est aussi ; par suite, si G vérifie une équation monomiale, il en vérifie aussi une dont les exposants m_i sont premiers dans leur ensemble ; il existe alors une matrice unimodulaire dont la première ligne est formée des m_i, d'où l'on déduit un automorphisme de $D(n)$ qui envoie G sur un sous-groupe G' du groupe défini par $x_1 = 1$, et les équations monomiales de G et G' se correspondent. Après un nombre fini de pas, on arrive à un sous-groupe de $D(k)$ ne satisfaisant à aucune équation monomiale, donc égal à $D(k)$ vu la première assertion.

COROLLAIRE 2.2. - Soient G et H des groupes algébriques diagonaux. Si tout élément d'ordre fini de H est dans G, alors $H \subset G$.

On utilise le fait que H est engendré par H_o et par ses éléments d'ordre fini et le fait qu'un tore de dimension d contient m^d éléments d'ordre diviseur de m pour tout m premier à p, qui résultent de 2.1.

COROLLAIRE 2.3. - Tout tore invariant dans un groupe algébrique connexe y est central. Dans un tore, un élément générique engendre un sous-groupe partout dense.

3. Groupe adhérent à une matrice. Groupes nilpotents.

On appelle groupe adhérent à un sous-ensemble $N \subset GL(n, \Omega)$ et l'on note $A(M)$

le plus petit groupe algébrique contenant M ; c'est aussi l'adhérence du sous-groupe engendré par M ; il est connexe si M est fermé irréductible. D^iG désigne le i-ième groupe-dérivé de G ; si G est algébrique, on introduit encore $\mathcal{D}^iG = A([\mathcal{D}^{i-1}G , \mathcal{D}^{i-1}G])$, $(\mathcal{D}^0G = G)$. Soient M et N des sous-groupes de $GL(n , \Omega)$. Alors $A([A(M) , A(N)]) = A([M , N])$, d'où il résulte que $\mathcal{D}^iA(M) = A(D^iM)$ donc que si M est commutatif (resp. résoluble) $A(M)$ est commutatif (resp. résoluble, et même résoluble comme groupe algébrique, i.e. $\mathcal{D}^iA(M) = \{e\}$ pour i assez grand). Remarque analogue pour la série centrale descendante et la nilpotence. Si M est invariant dans N , $A(M)$ est invariant dans $A(N)$; si de plus N/M est commutatif, ou nilpotent ou résoluble, $A(N)/A(M)$ l'est aussi.

Une matrice est <u>unipotente</u> (resp. semi-simple) si ses valeurs propres sont égales à 1 (resp. ses diviseurs élémentaires sont simples). Tout $x \in GL(n , \Omega)$ s'écrit d'une et d'une seule façon comme produit $x = x_s . x_u$ avec x_s semi-simple, x_u unipotent, $x_s x_u = x_u x_s$.

Soit x unipotente. Alors $x = 1 + n$, où n est nilpotente ; si $p \neq 0$, x est donc d'ordre fini égal à une puissance de p et $A(x)$ est le groupe cyclique engendré par x ; si $p = 0$ et $n \neq 0$, alors x est d'ordre infini et l'on voit aisément que $A(x)$ est le groupe à un paramètre $\exp(t \log x)$, $(t \in \Omega)$. Si x est semi-simple, $A(x)$ est diagonalisable et de l'unicité des racines p^n-ièmes en caractéristique p on déduit aisément que pour $p \neq 0$, $A(x)$ contient l'unique racine p^m-ième semi-simple de x .

THÉORÈME 3.1 (KOLCHIN [4]). - <u>Soit</u> x <u>une matrice inversible</u>. <u>Alors</u> x_s , $x_u \in A(x)$.

Soit $p \neq 0$. Il existe $k = p^m$ tel que $x^k = x_s^k$ d'où $x_s^k \in A(x)$, et $x_s \in A(x)$ par la remarque précédant (3.1). Si $p = 0$, on met $A(x)$ sous une forme triangulaire telle que la partie semi-simple y_s d'un élément $y \in A(x)$ soit sa partie diagonale ; alors $y \to y_s$ est une représentation rationnelle de $A(x)$ dans $D(n)$ et il suffit de faire voir que son image est contenue dans $A(x) \cap D(n)$. Vu (2.2), on peut se borner à le faire pour les éléments d'ordre fini, ce qui est aisé.

De ce qui précède on déduit sans grandes difficultés, surtout par considération des éléments d'ordre fini, le

THÉORÈME 3.2. - <u>Soient</u> G , G' <u>des groupes algébriques et</u> f <u>une représentation rationnelle de</u> G <u>sur</u> G' . <u>Alors si</u> x <u>est semi-simple</u> (<u>resp</u>. <u>unipotente</u>), $f(x)$ <u>l'est aussi</u>. <u>Toute matrice semi-simple</u> (<u>resp</u>. <u>unipotente</u>) <u>de</u> G' <u>est image d'une matrice semi-simple</u> (<u>resp</u>. <u>unipotente</u>) <u>de</u> G .

(3.1) implique évidemment qu'un groupe algébrique commutatif est le produit direct des sous-groupes formés par les éléments semi-simples et par les éléments unipotents (c'est du reste l'énoncé de Kolchin). Plus généralement, à l'aide de (1.1), (3.1), (3.2) on établit par récurrence sur la dimension, le

THÉORÈME 3.3. - *Soit* G *un groupe algébrique nilpotent connexe et soit* G_s *(resp.* G_u*) l'ensemble des matrices semi-simples (resp. unipotentes) de* G *. Alors* G_s *et* G_u *sont des sous-groupes invariants fermés connexes dont* G *est le produit direct.* G_s *est central dans* G *, et est l'unique tore maximal de* G *.*

Enfin, mentionnons encore le lemme suivant, bien qu'il soit plus technique, car il joue un rôle important dans certaines démonstrations de la suite.

LEMME 3.4. - *Soient* G *un groupe algébrique et* N *un sous-groupe invariant fermé connexe commutatif de* G *. Pour* $g \in G$ *, notons* F_g *, (resp.* M_g*), le centralisateur de* g *dans* N *, (resp. l'image de* N *par l'endomorphisme* $n \to [g, n]$*). Si* g *est semi-simple (resp. unipotent) et si* N *est formé de matrices unipotentes (resp. semi-simples), alors* $F_g \cap M_g = \{e\}$ *,* $N = F_g . M_g$ *et* F_g *est connexe.*

Le point essentiel est l'égalité $F_g \cap M_g = \{e\}$. Pour l'établir on considère un élément $a \in N$ tel que $[g, a] = b \in F_g$ et l'on montre que $x \to [x, a]$ définit une représentation rationnelle de $A(g)$ dans N . Cette représentation est alors triviale par (3.2), d'où $b = e$.

4. Espaces de transformations.

Bien que les lemmes de ce paragraphe ne soient appliqués dans cet exposé qu'à des groupes algébriques et à des variétés affines ou projectives, il est plus naturel de les formuler dans le cadre des variétés abstraites. Une *variété de groupe* G est une variété abstraite munie d'une loi de composition de groupe $f : G \times G \to G$ qui est une application rationnelle partout définie et telle que $x \to x^{-1}$ soit birationnelle birégulière. Une variété V est un *espace de transformations* de G si l'on a une application rationnelle partout définie de $G \times V$ dans V telle que $e(v) = v$, $g(g'(v)) = (g , g')(v)$, $(g , g' \in G , v \in V)$ et que pour tout $g \in G$, l'application $v \to g(v)$ de V dans V soit birationnelle birégulière.

Soit H un sous-groupe fermé de G . Alors ([5], [8] et [9]) l'espace des classes à gauche G/H peut être muni canoniquement d'une structure de variété abstraite, espace de transformations relativement aux translations à gauche, telle que la projection canonique τ_H de G sur G/H soit rationnelle partout définie. Si f est une application rationnelle de G dans une variété V , constante sur les classes gH , alors elle passe au quotient c'est-à-dire se factorise en $\bar{f} \circ \tau_H$, où $\bar{f}$ est une application rationnelle de G/H dans V , partout définie si f l'est. Lorsque H est invariant, G/H est une variété de groupe et τ_H est homomorphique ; si de plus G est linéaire, G/H l'est aussi (cf. [6] ; en caractéristique 0 , cela résulte déjà de (1.1), en caractéristique $p \neq 0$, il faut encore exorciser l'inséparabilité pure).

LEMME 4.1. - <u>Soit V un espace de transformations pour la variété de groupe G . Alors il existe une orbite fermée.</u>

Une orbite $G(v)$ est l'image de G par l'application rationnelle $g \to g(v)$. Elle contient donc un sous-ensemble relativement ouvert non vide de son adhérence $\overline{G(v)}$; cette dernière est évidemment invariante par G , par conséquent si $G(v) \neq \overline{G(v)}$, l'orbite d'un point de $\overline{G(v)}' - G(v)$ y sera contenue, donc aura une adhérence de dimension $< \dim \overline{G(v)}$. L'orbite d'un point v tel que $\dim \overline{G(v)}$ soit minimum est donc fermée.

4.2. - Une variété abstraite V est <u>complète</u> (au sens de Weil), si toute spécialisation d'un point de V est dans V . Nous aurons besoin des propriétés suivantes de cette notion : une variété affine complète se réduit à un point. L'image d'une variété complète par une application rationnelle partout définie est fermée et complète. Toute variété projective est complète. Enfin, tout "revêtement fini" non singulier d'une variété complète non singulière est complet ; plus précisément (WEIL) : Soient U , V des variétés non singulières et f une application rationnelle partout définie de U sur V . On suppose que l'image réciproque de chaque point de V se compose de m points distincts. Alors si V est complète (resp. projective), U est complète (resp. projective).

LEMME 4.3. - <u>Soit G un groupe algébrique (donc linéaire d'après nos conventions) connexe résoluble opérant sur une variété complète. Alors G admet un point fixe.</u>

Par récurrence, on se ramène au cas où G est commutatif. Soit alors W une orbite fermée (4.1) et soit H le groupe d'isotropie d'un point $w \in W$. L'application $g \to g(w)$ induit une application rationnelle bijective de G/H , qui est une variété affine (car c'est un groupe algébrique), sur W qui est complète ; par conséquent (4.2), G/H est complète et $G = H$.

5. <u>Le théorème fondamental.</u>

<u>Notation</u> : Dans toute la suite, G désigne un groupe algébrique connexe.

5.1. - Un drapeau de Ω^n est le système formé par n sous-espaces de dimensions $1, 2, \ldots, n$ emboîtés. L'ensemble $F(n)$ des drapeaux admet une structure de variété projective non singulière, espace homogène de $GL(n, \Omega)$. Un sous-groupe de $GL(n, \Omega)$ laisse un drapeau fixe si et seulement s'il peut être mis sous forme triangulaire ; il est alors résoluble. Appliqué à G opérant sur $F(n)$, (4.3) montre donc que tout groupe algébrique résolube connexe peut être mis sous forme triangulaire ; c'est la généralisation de KOLCHIN [3] du théorème de Lie. Il en résulte que l'ensemble G_u des matrices unipotentes d'un tel groupe est un sous-groupe invariant fermé (nilpotent) contenant $\mathcal{D}^1 G$.

THÉORÈME 5.2. - Les sous-groupes fermés résolubles connexes maximaux de G sont conjugués par automorphismes intérieurs. Le quotient de G par l'un d'entre eux est une variété projective.

Soit W une orbite fermée de G opérant sur $F(n)$ et soit H le groupe d'isotropie d'un drapeau $w \in W$; le groupe H est fermé résoluble ; G/H_o est un revêtement fini de W, (d'ordre égal à l'indice de H_o dans H), donc (4.2) est une variété projective. Si M est un sous-groupe fermé résoluble connexe de G, alors (4.3) il admet un point fixe sur G/H_o, donc est conjugué à un sous-groupe de H_o, d'où aisément le théorème.

COROLLAIRE 5.3. (KOLCHIN [4]). - Un groupe linéaire formé de matrices unipotentes peut être mis sous forme triangulaire et est nilpotent.

On se ramène sans grandes difficultés au cas où le groupe envisagé est algébrique connexe. Le corollaire résulte alors de l'énoncé suivant plus précis (dont on a besoin ultérieurement) :

5.4. - Si les matrices semi-simples de G sont toutes d'ordre fini, alors G est formé de matrices unipotentes et peut être mis sous forme triangulaire.

Soit R un sous-groupe fermé résoluble connexe maximal de G, supposé mis sous forme triangulaire. L'application $x \longrightarrow$ partie diagonale de x est une représentation rationnelle de R, dont l'image est d'une part un tore et d'autre part formée d'éléments d'ordre fini ; cette représentation est donc triviale et R ne contient que des matrices unipotentes. Soit alors (e_i) une base de Ω^n dont les j premiers éléments sous-tendent un sous-espace invariant par $R (j = 1, \ldots, n)$. L'application $g \longrightarrow g(e_1 \wedge \ldots \wedge e_j)$ de G dans $\Lambda^j(\Omega^n)$ passe alors au quotient par R et son image est une variété affine complète, donc un point. Ainsi le drapeau fixe par R l'est aussi par G, d'où $G = R$.

COROLLAIRE 5.5. - Le centralisateur connexe C d'un tore maximal Q de G est nilpotent, égal à son normalisateur connexe.

Soit f une représentation rationnelle de C, de noyau Q. Si $s \in C$ est semi-simple, alors $s^m \in Q$ pour m convenable (car sinon $A(s)_o$ et Q engendreraient un tore $\neq Q$), donc (3.2), $f(C)$ vérifie l'hypothèse de (5.4) et est nilpotent. Ainsi C est nilpotent et la dernière assertion se déduit de (3.3) et (2.3).

6. Les conjugués de certains sous-groupes.

LEMME 6.1. - a. Soit H un sous-groupe fermé de G, égal à son normalisateur connexe. Suposons que pour tout point générique h de H, (sur un corps de définition pour G, H), la condition $ghg^{-1} \in H$, $(g \in G)$, soit équivalente à $gHg^{-1} = H$. Alors l'ensemble des conjugués de H contient un ouvert non vide de G.

b. Soit H un groupe fermé de G tel que G/H soit complète. Si l'ensemble des conjugués de H contient un ouvert non vide de G, alors il est égal à G.

On ne reproduit pas la démonstration de a., qui consiste à calculer les dimensions de certaines extensions du corps de base. En ce qui concerne b., il suffit de remarquer que tout point générique (donc par spécialisation tout point) de G admet un point fixe sur G/H.

THÉORÈME 6.2. - Les conjugués du centralisateur connexe C d'un tore maximal Q de G contiennent un ouvert non vide de G. Par suite, les tores maximaux de G sont conjugués par automorphismes intérieurs et tout élément de G fait partie d'un sous-groupe fermé résoluble connexe maximal.

Il suffit essentiellement de voir que C vérifie les hypothèses de 6.1 a., ce qui résulte de (5,5), (2.3), (3.3).

De (6.2) et (4.3), on tire aisément que si $g \in G$ centralise un sous-groupe résoluble connexe H, alors il existe un sous-groupe résoluble connexe contenant g et H. Cela permet de ramener la démonstration de (6.3) au cas G résoluble, dans lequel elle se rattache directement au paragraphe 3.

PROPOSITION 6.3. - Tout élément semi-simple de G fait partie d'un tore. Le centralisateur d'un tore est connexe. Si s semi-simple centralise un tore T, il existe un tore contenant s et T.

7. Sous-groupes de Cartan. Eléments réguliers.

Un sous-groupe de Cartan d'un groupe (quelconque) M est un sous-groupe nilpotent maximal, dont tout sous-groupe d'indice fini est d'indice fini dans son normalisateur (définition de CHEVALLEY [2 b]). Dans le cas d'un groupe algébrique, un sous-groupe de Cartan C est fermé et la deuxième condition équivaut à : "C_o est égal à son normalisateur connexe".

THÉORÈME 7.1. - Les sous-groupes de Cartan de G sont les centralisateurs de ses tores maximaux. Ils sont donc connexes et conjugués par automorphismes intérieurs.

a. Soit C le centralisateur d'un tore maximal Q. Il est connexe (6.3), égal à son normalisateur connexe (5.5) ; pour voir qu'il est nilpotent maximal, on montre (à l'aide du paragraphe 3) qu'un groupe nilpotent algébrique centralise la partie semi-simple de sa composante connexe de e.

b. Soit C un sous-groupe de Cartan. Vu ce qui précède, il suffira de faire voir que C_o est le centralisateur connexe d'un tore maximal de G, donc que si H est un sous-groupe fermé nilpotent de G, égal à son normalisateur connexe, alors H est le centralisateur connexe d'un tore maximal de G. Pour cela on s'appuie sur le lemme suivant (élémentaire) : Dans un groupe algébrique nilpotent connexe, le normalisateur connexe d'un sous-groupe fermé connexe propre H est $\neq H$. Soit alors S le tore maximal de H, R un sous-groupe résoluble connexe maximal de G contenant H, Q un tore maximal de R contenant S, et soit $M = Q.M_u$ où M_u est le centralisateur (connexe par 3.4) de Q dans R_u. On tire du lemme précité que $M_u = H_u$ donc que H est invariant dans M, d'où $M = H$ et $Q = S$; et enfin que H est le centralisateur connexe de Q dans G.

7.2. - Un élément $g \in G$ est régulier si le centralisateur connexe $C(g_s)_o$ de sa partie semi-simple est de dimension minimum. Il est immédiat que g est régulier si et seulement si $C(g_s)_o$ est un sous-groupe de Cartan ; ou, ce qui revient au même comme on le voit aisément, si $C(g_s)_o$ est nilpotent. Remarquons que d'après (6.3) tout élément semi-simple est contenu dans son centralisateur connexe.

THÉORÈME 7.3. - Un élément $g \in G$ est régulier si et seulement s'il fait partie d'exactement un sous-groupe de Cartan de G. L'ensemble des éléments réguliers de G contient un ouvert non vide de G.

On ne détaillera pas la démonstration, qui s'appuie sur les résultats déjà acquis sans faire intervenir d'idée nouvelle. Signalons cependant que l'unicité du sous-groupe de Cartan contenant un élément régulier résulte principalement du lemme suivant, trivial pour $p = 0$ et dont la démonstration en caractéristique $p \neq 0$ s'appuie surtout sur (3.4) : Si l'élément unipotent u et l'élement semi-simple s de G commutent, alors $u \in C(s)_0$.

REMARQUES.

1° En caractéristique 0 , les résultats des paragraphes 2 et 7, le théorème 3, sont démontrés dans [2]. Il est élémentaire que les éléments réguliers forment un ouvert, mais je regrette de ne pas savoir s'il en est ainsi pour $p \neq 0$.

2° Toutes les propriétés des groupes résolubles établies ci-dessus peuvent être obtenues directement comme conséquences du paragraphe 3 ; c'est la méthode suivie dans [1]. On démontre alors en outre que G est produit semi-direct d'un tore maximal par sa partie unipotente, que les tores maximaux sont conjugués par des éléments de $\mathfrak{C}^{\infty} G$, (intersection des termes de la série centrale descendante), et enfin que si $\mathfrak{C}^{\infty}G$ est commutatif et si C est un sous-groupe de Cartan, alors $C \cap \mathfrak{C}^{\infty}G = \{e\}$ et $G = C . \mathfrak{C}^{\infty}G$.

3° Les notions de sous-groupe fermé résoluble connexe maximal, tore maximal, sous-groupe de Cartan, élément régulier se conservent par représentation rationnelle surjective.