Groupes algébriques affines

Matthieu Romagny

Rencontre ANR ARIVAF, 8–10 novembre 2011, Paris, IHP

Cet exposé rassemble quelques résultats de base sur la structure des groupes algébriques affines, utiles pour la suite de la rencontre. La référence principale est Milne, *Algebraic Groups, Lie Groups, and their Arithmetic Subgroups*.

On fixe un corps de base k de caractéristique 0 et une clôture séparable k^s. Tous les groupes sont des schémas en groupes affines de type fini ; on les appelle simplement des groupes algébriques ; par le théorème de Cartier, ils sont lisses. Tous les sous-groupes sont fermés. On note $\mathrm{Rep}(G)$ la catégorie des représentations de G dans des espaces vectoriels de dimension finie.

1 Généralités

1.1 Définitions et dévissage

Ici, on rappelle brièvement que tout groupe algébrique est extension de groupes des types suivants : semi-simple, unipotent, tore. Allons-y. Soit G un groupe algébrique. On note G' l'intersection des sous-groupes distingués N de G tels que G/N soit commutatif, et on l'appelle le *sous-groupe dérivé*. Si k est algébriquement clos et G connexe, on dispose de la description plus familière comme sous-groupe engendré par les commutateurs, voir Milne I.16.22. La *suite dérivée* de G est définie par $G^0 = G$ et $G^{i+1} = (G^i)'$. Si $G^n = 1$ pour un n, on dit que G est *résoluble*. Il est équivalent de dire que G s'obtient par extensions successives de groupes commutatifs.

On note « cdm » pour « connexe distingué maximal » (toujours sous-entendu : fermé).

1) Un groupe connexe affine G possède un unique sous-groupe résoluble cdm, appelé le *radical* et noté RG. Si $RG = 1$ on dit que G est *semi-simple* ; le quotient G/RG est semi-simple.

On dit qu'un groupe G est *unipotent* si chaque représentation non nulle possède un vecteur fixe non nul. Il est équivalent de dire que les objets simples de $\mathrm{Rep}(G)$ sont triviaux ; ou que G est isomorphe à un sous-groupe du groupe des matrices triangulaires supérieures unipotentes ; ou que G est composé d'éléments unipotents (au sens de Milne I.10.18) ; ou que G est extension successive de copies de $\mathbb{G}_a$.

2) Un groupe connexe affine possède un unique sous-groupe unipotent cdm, appelé le *radical unipotent* et noté R_uG ; c'est un sous-groupe de RG. Si $R_uG = 1$ on dit que G est *réductif* ; le quotient G/R_uG est réductif. Si G est résoluble, le quotient G/R_uG est un tore (voir plus loin ; en fait G est produit semi-direct de G/R_uG par R_uG).

1.2 Sous-groupes vus comme stabilisateurs

Théorème (Chevalley). *Tout sous-groupe H d'un groupe G est stabilisateur d'une droite D dans une certaine représentation fidèle E.*

Preuve. D'abord une remarque : si X est une variété affine sur laquelle G agit et $f \in k[X]$ une fonction, alors les translatées à gauche $g.f := f(g^{-1}\cdot)$ engendrent un espace de dimension finie dans $k[X]$. En effet, si on note $\alpha : k[X] \to k[G] \otimes k[X]$ la coaction et $\alpha(f) = \sum_{i=1}^m a_i \otimes b_i$ avec $a_i \in k[G]$ et $b_i \in k[X]$, alors on vérifie que $g.f = \sum a_i(g^{-1})b_i \in \mathrm{Vect}(b_1, \ldots, b_m)$.

Appliquant cela à des générateurs $f_1, \dots, f_n$ de l'idéal $I \subset k[G]$ qui définit H dans G, on obtient un sous-espace de dimension finie G-invariant $V \subset k[G]$ et tel que $W = V \cap I$ engendre I. Je dis que $H = \{g \in G,\, gW = W\}$. En effet, comme V et I sont H-invariants, alors W l'est aussi d'où l'inclusion directe. Réciproquement, si $gW = W$ alors comme W engendre I on obtient $gI = I$, donc $g \in H$.

Considérons maintenant $d = \dim(W)$ et l'action induite sur $E = \wedge^d V$. Si $D = \wedge^d W$, je dis que $H = \{g \in G,\, gD = D\}$. En effet, si $gD = D$, complétons une base de $W \cap gW$ en une base $\{e_i\}$ de V de sorte que $W = \mathrm{Vect}(e_1, \dots, e_d)$ et $gW = \mathrm{Vect}(e_n, \dots, e_{n+d-1})$ pour un certain $n \geq 1$. Alors $g(e_1 \wedge \cdots \wedge e_d)$ est un multiple de $e_n \wedge \cdots \wedge e_{n+d-1}$, donc $gD = D$ impose $n = 1$ i.e. $gW = W$ puis $g \in H$. L'autre inclusion est évidente.

On a donc réalisé H comme stabilisateur de la droite D. Si l'action de H sur E n'est pas fidèle, on remplace E par $E \oplus F$ pour une certaine représentation fidèle F et c'est gagné.

2 Groupes de type multiplicatif

Soit M un groupe commutatif, et $k[M]$ l'algèbre de groupe. Si M est noté multiplicativement (resp. additivement), les éléments de $k[M]$ sont les sommes $\sum a_m m$ (resp. $\sum a_m X^m$) indicées par un ensemble fini $I \subset M$. C'est une algèbre de Hopf avec la counité $\epsilon(m) = 1$, le coproduit $\Delta(m) = m \otimes m$ et le coinverse $i(m) = m^{-1}$.

Proposition. *Le foncteur défini sur les k-algèbres A par $D(M)(A) = \mathrm{Hom}_{Gp}(M, A^\times)$ est représentable par le schéma en groupes $Spec(k[M])$. Le schéma en groupes $D(M)$ est algébrique si et seulement si M est de type fini; dans ce cas $D(M)$ est produit de copies de $\mathbb{G}_m$ par un nombre fini de μ_n.*

En effet, un morphisme de groupes $\varphi : M \to A^\times$ s'étend par linéarité de manière unique en un morphisme d'algèbres $k[M] \to A$, $\sum a_m m \mapsto \sum a_m \varphi(m)$. L'assertion sur l'algébricité est claire. La description de $D(M)$ pour M de type fini découle du théorème de structure des groupes abéliens de type fini et des deux exemples $D(\mathbb{Z}) = \mathbb{G}_m$ et $D(\mathbb{Z}/n\mathbb{Z}) = \mu_n$.

On dit qu'un schéma en groupes est *diagonalisable* s'il est de la forme $D(M)$.

Proposition. *Si $G = D(M)$, alors le groupe des caractères $X(G) = \mathrm{Hom}(G, \mathbb{G}_m)$ est isomorphe à M. Ainsi D et X établissent des équivalences de catégories inverses l'une de l'autre entre la catégorie des groupes commutatifs et la catégorie des groupes diagonalisables.*

En effet, un caractère est donné par un morphisme d'algèbres de Hopf $k[z, z^{-1}] \to k[M]$. Un tel morphisme est déterminé par l'image de z, qui est un élément $\sum a_m m$ tel que $\sum a_m = 1$ (compatibilité à la counité) et $\sum a_m m \otimes m = \sum a_m a_n m \otimes n$ (compatibilité à la comultiplication). On trouve que tous les a_m sont nuls sauf l'un d'entre eux qui vaut 1, cqfd.

Proposition. *Soit G un groupe diagonalisable et V une représentation de dimension finie. Alors $V = \oplus_{\chi \in X(G)} V_\chi$ où V_χ est le sous-espace de V sur lequel G agit par le caractère χ.*

Se démontre par un calcul explicite sembable à celui de la preuve de la proposition précédente.

On dit qu'un schéma en groupes G est *de type multiplicatif* si $G \otimes k^s$ est diagonalisable ; un *tore* si $G \otimes k^s$ est un produit de $\mathbb{G}_{m,k^s}$; un *tore déployé* si G est un produit de $\mathbb{G}_{m,k}$.

Proposition. *Soit Γ le groupe de Galois de k^s/k. Alors les foncteurs $G \mapsto X(G \otimes k^s)$ et $M \mapsto D_{k^s}(M)/\Gamma = \mathrm{Spec}(k^s[M]^\Gamma)$ établissent des équivalences de catégories inverses entre les*

groupes de type multiplicatif et les groupes commutatifs avec action continue de Γ. *Ces équivalences préservent les suites exactes.*

Ceci se déduit des résultats précédents par descente.

Exemple. Prenons $k = \mathbb{R}$. Sur le groupe $M = \mathbb{Z}$, il y a deux actions de $\Gamma = \mathbb{Z}/2\mathbb{Z}$. L'action triviale donne $G = \mathbb{G}_m$, et et l'action non triviale donne la $\mathbb{R}$-algèbre

$$\mathbb{C}[z, z^{-1}]^{\mathbb{Z}/2\mathbb{Z}} = \big\{P \in \mathbb{C}[z, z^{-1}],\ \overline{P}(z^{-1}) = P(z)\big\}.$$

Cette algèbre est engendrée par les éléments $x = \frac{1}{2}(z + z^{-1})$ et $y = \frac{1}{2}(iz - iz^{-1})$, avec la relation $x^2 + y^2 = 1$, donc $G = \mathrm{Spec}(\mathbb{R}[x, y]/(x^2 + y^2 - 1))$. On peut le voir aussi en décrivant les points. Avec les notations de la proposition, si $K \subset k^{\mathrm{s}}$ est une sous-extension et $\Gamma_K = \mathrm{Gal}(k^{\mathrm{s}}/K)$ on a

$$G(K) = \mathrm{Hom}(\mathrm{Spec}(K), G_K) = \mathrm{Hom}(\mathrm{Spec}(k^{\mathrm{s}}), G \otimes k^{\mathrm{s}})^{\Gamma_K} = \mathrm{Hom}_{Gp}(M, (k^{\mathrm{s}})^{\times})^{\Gamma_K}.$$

Dans l'exemple, on trouve $G(\mathbb{R}) = \mathrm{Hom}(\mathbb{Z}, \mathbb{C}^{\times})^{\mathbb{Z}/2\mathbb{Z}} = \{z \in \mathbb{C}^{\times}, z^{-1} = \overline{z}\} = S^1$.

Remarque : rigidité des groupes de type multiplicatif. Via l'équivalence de catégories ci-dessus, le schéma en groupes des automorphismes d'un groupe diagonalisable $G = D(M)$ est isomorphe au schéma en groupes constant (discret) des automorphismes du groupe commutatif M. De même, le schéma en groupes des automorphismes d'un groupe de type multiplicatif est étale (non quasi-compact en général).

3 Groupes semi-simples

Les algèbres de Lie des groupes de Lie reflètent une très large part de leur structure, et sont inévitables pour bien des questions. Il ne faut cependant pas tout leur faire dire : par exemple $\mathbb{G}_m$ et $\mathbb{G}_a$ ont même algèbre de Lie.

3.1 Algèbres de Lie

Pour une algèbre de Lie $\mathfrak{g}$, on définit la *suite dérivée* par $\mathfrak{g}^0 = \mathfrak{g}$ et $\mathfrak{g}^{i+1} = [\mathfrak{g}^i, \mathfrak{g}^i]$. On dit que $\mathfrak{g}$ est *résoluble* si $\mathfrak{g}^n = 0$ pour un n. Il existe une plus grande sous-algèbre de Lie résoluble de $\mathfrak{g}$, appelée le *radical* et notée $\mathrm{Rad}\,\mathfrak{g}$. On dit que $\mathfrak{g}$ est *semi-simple* si $\mathrm{Rad}\,\mathfrak{g} = 0$. La *représentation adjointe* $\mathrm{ad} : \mathfrak{g} \to \mathrm{Der}\,\mathfrak{g}$ envoie x sur $\mathrm{ad}(x) = [x, -]$.

Théorème (critère de Cartan-Killing). *L'algèbre de Lie* $\mathfrak{g}$ *est semi-simple si et seulement si la forme de Killing* $\kappa(x, y) = \mathrm{tr}(\mathrm{ad}\,x\,\mathrm{ad}\,y)$ *est non-dégénérée.*

Voir Milne II.5.13.

Corollaire. *Toute algèbre de Lie semi-simple est la somme directe finie de ses idéaux simples.*

Pour le voir, on prend pour $\mathfrak{g}_1$ un idéal non nul de dimension minimale (donc simple), et on itère avec l'orthogonal de $\mathfrak{g}_1$ pour κ.

Théorème (Weyl). *Une algèbre de Lie* $\mathfrak{g}$ *est semi-simple si et seulement si toutes ses représentations de dimension finie sont semi-simples, i.e.* $\mathrm{Rep}(\mathfrak{g})$ *est semi-simple.*

Voir Milne II.6.10.

3.2 Groupes simples et semi-simples

Théorème. *Soit G un groupe algébrique connexe et $\mathfrak{g}$ son algèbre de Lie. Alors G est semi-simple si et seulement si $\mathfrak{g}$ est semi-simple.*

Ceci se démontre en utilisant la caractérisation de la semi-simplicité par la non-existence de sous-groupes connexes distingués abéliens $\neq 1$ (côté groupe) et d'idéaux abéliens $\neq 0$ (côté algèbre). Voir Milne II.5.23 pour les détails.

Corollaire. *Si G est semi-simple, alors* $\mathrm{Rep}(G)$ *est semi-simple.*

Immédiat sachant qu'un sous-espace $W \subset V$ d'une représentation de G est G-stable si et seulement si elle est $\mathfrak{g}$-stable, Milne II.2.16.

Un groupe algébrique G est dit *simple* (on trouve aussi la terminologie *presque simple*) s'il est connexe, non commutatif, et si ses seuls sous-groupes distingués stricts sont finis (i.e. G n'a pas de sous-groupe distingué *connexe* non trivial). Exemples : SL_n et $\mathrm{PSL}_n = \mathrm{SL}_n / \mu_n$.

Théorème. *Soit G un groupe algébrique semi-simple. Alors G possède un nombre fini de sous-groupes distingués simples $G_1, \ldots, G_r$, qui commutent entre eux, et le morphisme de produit $G_1 \times \cdots \times G_r \to G$ est surjectif à noyau fini.*

En effet, l'algèbre de Lie $\mathfrak{g}$ est semi-simple donc produit de ses idéaux simples $\mathfrak{g}_i$. Toutes les sous-algèbres de Lie de $\mathfrak{g}$ ne sont pas l'algèbre de Lie d'un sous-groupe en général, mais c'est le cas pour les $\mathfrak{g}_i$. Précisément, soit $C_i = \{g \in G, \mathrm{Ad}(g)x = x,\ \forall x \in \mathfrak{g}_j, \forall j \neq i\}$ le centralisateur de la somme des $\mathfrak{g}_j$, $j \neq i$, et $G_i = C_i^\circ$ sa composante neutre. On a $\mathrm{Lie}(G_i) = \mathrm{Lie}(C_i) = \mathfrak{g}_i$ et on en déduit toutes les propriétés annoncées. Voir Milne II.5.31 pour les détails.

Exemple : Le quotient de $\mathrm{SL}_n \times \mathrm{SL}_n$ par μ_n diagonal.

Corollaire. *Si G est semi-simple, alors $G = G'$.*

C'est clair si G est simple, et on en déduit le résultat en utilisant la surjection du théorème.

4 Groupes réductifs

Théorème. *Un groupe connexe G est réductif ssi* $\mathrm{Rep}(G)$ *est semi-simple.*

Preuve. Supposons G réductif, soient R le radical, Z° le centre connexe, G' le groupe dérivé.

Lemme. $R = Z^\circ$.

En effet, comme G est réductif, R est un tore. Par rigidité des tores, l'action $G \to \mathrm{Aut}(R)$ de G sur R par conjugaison est triviale donc $R \subset Z^\circ$. La réciproque provient de la définition de R.

Lemme. *G' est semi-simple.*

Comme G/R est semi-simple, il est égal à son groupe dérivé ; la surjection $f : G \to G/R$ induit une surjection $f' : G' \to G/R$ entre groupes dérivés. Le radical de G' s'envoie par f' sur celui de G/R qui est trivial, donc il est inclus dans $\ker(f')$ et il suffit de montrer que ce dernier est fini. Or $\ker(f') = G' \cap R = G' \cap Z^\circ$ où Z° est le centre connexe, d'après le lemme. Maintenant soit $\rho : G \to \mathrm{GL}(V)$ une représentation fidèle de G. Soit $V = \oplus V_\chi$ sa décomposition

comme représentation du tore Z°. Le groupe G commute avec Z° donc son image dans $\mathrm{GL}(V)$ est incluse dans le centralisateur de Z° qui est $\prod \mathrm{GL}(V_\chi)$. Ainsi $G' \subset \prod \mathrm{SL}(V_\chi)$. Or Z° agit sur V_χ par homothéties et donc intersecte $\mathrm{SL}(V_\chi)$ selon un groupe fini.

Revenons à notre preuve. On a $G = Z^\circ G'$ car $Z^\circ = R$ et G' se surjecte sur G/R. Soit V une G-représentation et $V = \oplus V_\chi$ sa décomposition comme représentation du tore Z°. Comme Z° et G' commutent, chaque V_χ est G'-stable. Comme G' est semi-simple, alors $\mathrm{Rep}(G')$ est semi-simple, et V_χ se décompose en somme directe de G'-modules simples qui sont en fait des G-modules simples, cqfd.

Réciproquement, supposons $\mathrm{Rep}(G)$ semi-simple. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation fidèle. Soit N le radical unipotent. Alors ρ est semi-simple par hypothèse et $\rho|_N$ l'est (comme représentation de N bien sûr) d'après :

Lemme. *Soit N un sous-groupe distingué de G. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation semi-simple de G. Alors $\rho|_N : N \to \mathrm{GL}(V)$ est une représentation semi-simple de N.*

En effet, pour voir cela on peut supposer que X est simple. Soit Y un sous-N-module simple de X. Comme N est distingué, pour tout $g \in G(k)$ le sous-espace gY est un encore un sous-N-module simple de X. Par ailleurs la somme $\sum_{g\in G} gY$ est un sous-G-module non nul de X, donc égal à X. Alors X est somme de N-modules simples, donc il est semi-simple.

D'après ce lemme l'espace V est donc somme directe de N-modules simples V_i. Comme N est unipotent, ses modules simples sont de dimension 1 avec action triviale. Il s'ensuit que N agit trivialement sur V, donc $N = 1$ puisque V est fidèle. Ceci montre que G est réductif.

Exemple. Les sous-groupes réductifs de SL_2 sont 1, SL_2 et les tores maximaux. En effet, on sait que le *rang* (la dimension d'un tore maximal) de SL_2 est 1. Soit $G \neq 1, \mathrm{SL}_2$ un sous-groupe réductif. Si $\dim(G) = 1$, alors $G \otimes \overline{k}$ est isomorphe à $\mathbb{G}_a$ ou $\mathbb{G}_m$, donc $\mathbb{G}_m$ car il est réductif, donc G est un tore maximal. Si $\dim(G) = 2$, son radical R est un tore de dimension 0 ou 1. Alors G/R (donc aussi son algèbre de Lie) est semi-simple de dimension 2 ou 1. Mais les algèbres de Lie de dimension ≤ 2 sont résolubles, impossible.

Remarque. Soit $G = \mathbb{G}_m$ et $\mathfrak{g} = \mathfrak{gl}_1$ son algèbre de Lie. On vient de voir que $\mathrm{Rep}(G)$ est semi-simple, mais $\mathrm{Rep}(\mathfrak{g})$ ne l'est pas car $\mathfrak{g}$ n'est pas semi-simple. En effet, la représentation de dimension 2 donnée par $x.\binom{a}{b} = \binom{0}{xa}$ a pour seul sous-module non trivial le sous-espace vectoriel d'équation $a = 0$.

Remarque. Résumons les liens entre G et $\mathrm{Rep}(G)$:

G est réductif	ssi	$\mathrm{Rep}(G)$ est semi-simple,
G est résoluble	ssi	$\mathrm{Rep}(G)$ a tous ses objets simples de dimension 1,
G est unipotent	ssi	$\mathrm{Rep}(G)$ a tous ses objets simples de dimension 1 triviaux,
G est un tore	ssi	$\mathrm{Rep}(G)$ est semi-simple et a tous ses objets simples de dimension 1.