Groupes réductifs et schémas en groupes

Guillaume Pouchin

3 avril 2006

Première partie
Groupes algébriques linéaires

Nous allons dans un premier temps définir les objets que nous allons étudier. Les groupes algébriques sont des objets munis d'une structure de variété algébrique et d'une structure de groupe compatible. Définissons donc d'abord les variétés algébriques affines (on considère uniquement des groupes algébriques linéaires, donc il suffit de présenter les variétés affines).

Dans la suite, k désignera un corps algébriquement clos. Soit $n \in \mathbb{N}$, A l'algèbre $k[X_1, \cdots, X_n]$. Si I est un idéal de A, on note $\nu(I)$ le sous-ensemble de k^n qui est le lieu des zéros des polynômes de I, c'est-à-dire :

$$\nu(I) := \{x = (x_1, \cdots, x_n) \in k^n \mid \forall P \in I, P(x) = 0\}$$

On montre que ces sous-parties de k^n vérifient les axiomes des parties fermées d'un espace topologique. On peut donc définir une topologie sur k^n, appelée topologie de Zariski, telle que les fermés sont les sous-ensembles de la forme $\nu(I)$, où I est un idéal de $A = k[X_1, \cdots, X_n]$.

Définition 1 (variété algébrique affine). Une variété algébrique affine sur k est un sous-ensemble fermé (pour la topologie de Zariski) d'un certain k^n, $n \in \mathbb{N}$, muni de la topologie induite.

Géométriquement, une variété affine est donc un sous-ensemble de k^n défini par des équations polynômiales (les polynômes de I).

A une variété affine X de la forme $\nu(I)$, où I est un idéal de $k[X_1, \cdots, X_n]$, on associe son algèbre des fonctions $k[X] := k[X_1, \cdots, X_n]/I$.

On peut remarquer que, comme l'algèbre des polynômes sur un corps est noethérienne, tout idéal I est engendré par un nombre fini de générateurs.

Cela veut donc dire concrètement qu'un nombre fini d'équations définit une variété affine.

Définissons maintenant les morphismes entre variétés :

Définition 2. Si X et Y sont respectivement des sous-variétés de k^n et k^r, un morphisme de variétés $\phi : X \to Y$ est une application polynômiale $\phi : k^n \to k^r$ telle que $\phi(X) \subseteq Y$.

Remarque 1. Si on veut définir les variétés algébriques non nécessairement affines, il faudrait introduire un objet supplémentaire, le faisceau des fonctions sur la variété. Les morphismes auront alors une condition supplémentaire pour conserver ces faisceaux.

On peut maintenant définir ce qu'est un groupe algébrique linéaire.

Définition 3. Un groupe algébrique linéaire est une variété algébrique affine munie d'une structure de groupe telle que :
- la multiplication $G \times G \to G$ est un morphisme de variétés,
- l'inverse $G \to G$ est un morphisme de variétés.

Exemples :

Les groupes de matrices classiques sont des groupes algébriques linéaires : le groupe orthogonal O_n, le groupe spécial orthogonal SO_n, le groupe spécial Sl_n, les matrices diagonales D_n, les matrices triangulaires T_n.

En fait on montre que tous les groupes algébriques linéaires peuvent se voir comme des groupes de matrices. Plus exactement on a la proposition suivante :

Proposition 1 ([Sp], thm 2.3.7). Soit G un groupe algébrique linéaire. Alors il existe un isomorphisme ϕ entre G et un sous-groupe fermé d'un certain GL_n.

Donc finalement les groupes algébriques linéaires ne sont autres que des groupes de matrices définis par un certain nombre fini d'équations algébriques.

La question qui se pose alors naturellement est celle de la classification de tous les groupes algébriques linéaires. La question étant trop générale pour avoir une réponse satisfaisante, il faut mettre en lumière une classe de groupes algébriques linéaires la plus grosse possible qui soit classifiable. La bonne notion à considérer est alors celle de groupe réductif. Rappelons d'abord qu'un groupe algébrique G est dit unipotent si tous ses éléments le sont (en plongeant G dans un groupe de matrices, dire que $x \in G$ est unipotent veut dire que $Id - x$ est nilpotent).

Définition 4. Un groupe algébrique est dit réductif s'il n'admet pas de sous-groupe fermé normal connexe unipotent.

Pour comprendre la structure de tels groupes, on étudie l'action de sous-groupes diagonalisables (appelés tores) sur son algèbre de Lie, qui est l'espace tangent à l'élément neutre. A un groupe réductif G avec un tore maximal T il est possible d'associer une donnée combinatoire appelée donnée radicielle, qui va permettre de classifier tous les groupes réductifs. En effet on a d'abord un théorème d'unicité du groupe réductif à un donnée radicielle donnée.

Théorème 1 (cf [Sp], thm 9.6.2). *Soient G et G_1 deux groupes algébriques linéaires réductifs connexes, et T et T_1 des tores maximaux respectifs, correspondant à des données radicielles $\Psi = (X, X^*, R, R^*)$ et $\Psi_1 = (X_1, X_1^*, R_1, R_1^*)$. Soit f un isomorphisme entre Ψ et Ψ_1.*
Alors il existe un isomorphisme de groupes algébriques $\phi : G \to T_1$ tel que $\phi T = T_1$ et $f = f(\phi)$.

De plus à toute donnée radicielle on peut associer un groupe algébrique réductif connexe.

Théorème 2 (cf [Sp], thm 10.1.1). *Soit $\Psi = (X, R, X^*, R^*)$ une donnée radicielle. Alors il existe un groupe algébrique linéaire connexe réductif G sur k et un tore maximal T tels que la donnée radicielle de G par rapport à T est Ψ.*

Deuxième partie

Extension à une base plus générale

Il est naturel de vouloir étendre les résultats précédents d'abord à un corps non algébriquement clos, puis à des anneaux. Dans le cas d'un corps non-algébriquement clos k, il est possible de plonger k dans une clôture algébrique et appliquer les résultats connus. Ensuite il reste à étudier le passage de la clôture algébrique au corps de départ, par des outils de cohomologie galoisienne. Par contre dans le cas d'un anneau, il est nécessaire d'utiliser les outils de géométrie algébrique, en particulier le formalisme des schémas.

Dans le cas de l'algèbre $A := k[X_1, \cdots, X_n]$ sur un corps k algébriquement clos, le théorème des zéros de Hilbert permet d'identifier les points de k^n avec les idéaux maximaux de l'algèbre A. Un morphisme de variétés affines $\phi : X \to Y$, où X et Y sont des sous-variétés respectivement de k^n et k^r, s'identifie alors avec un morphisme d'algèbre $\phi^* : k[Y] \to k[X]$ (un point de X s'identifiant à un élément $\mathfrak{m}$ de $Specmax(k[Y])$, son image par ϕ s'identifiant à $(\phi^*)^{-1}(\mathfrak{m})$). Cette correspondance n'est plus vérifiée si k n'est plus algébriquement clos (ou pire si ce n'est pas un corps mais un anneau). L'idée est alors de considérer non pas seulement les idéaux maximaux mais l'ensemble des idéaux premiers.

Lorsque A est un anneau, on munit l'ensemble $Spec(A)$ de la topologie suivante (appelée topologie de Zariski comme dans le cas des variétés algébriques) : les fermés sont les ensemble du type $\{\mathfrak{p} \in Spec(A), I \subseteq \mathfrak{p}\}$, pour I un idéal de A. On vérifie qu'ils forment bien une famille de fermés d'un espace topologique. D'où la définition suivante :

Définition 5. Un schéma affine est le spectre d'un anneau A, muni de la topologie de Zariski.

Remarque 2. Comme dans le cas des variétés, nous ne parlerons que de schémas affines, ce qui permet de simplifier les définitions. En effet dans le cas non affine, il faut ajouter un faisceau d'anneaux sur l'espace topologique, qui dans le cas affine est entièrement déterminé par l'anneau A. Le mot "schéma" désignera donc ici un schéma affine.

Définition 6. Un morphisme de schémas affines $u : X = Spec(A) \to Y = Spec(B)$ est une application correspondant à un morphisme d'anneaux $u^* : B \to A$ (si $\mathfrak{p} \in X$, $u(\mathfrak{p}) = (u^*)^{-1}(\mathfrak{p})$).

Remarque 3. Un tel morphisme peut avoir beaucoup de propriétés. On dit par exemple qu'il est :
- de type fini si via u^* l'algèbre A est de type fini sur B,
- fini si via u^* l'algèbre A est finie sur B (i.e. est un B-module de type fini).
Il y a ensuite diverses propriétés de régularité : la platitude ou la lissité (plus forte que la platitude).

Comme dans le cas des variétés où on disposait d'un corps sous-jacent k, il est utile de définir des schémas par rapport à un schéma de base.

Définition 7. Un schéma X sur un schéma S (dit schéma de base) est un morphisme de schémas $X \to S$. Un morphisme de S-schémas entre X et Y est un morphisme de schémas faisant commuter le diagramme :

$$\begin{tikzcd} X \arrow[rr] \arrow[dr] & & Y \arrow[dl] \\ & S & \end{tikzcd}$$

Remarque 4. Concrètement, si le schéma de base S est le spectre d'un anneau R, un S-schéma $X = Spec(A)$ est le spectre d'un anneau A qui est aussi une R-algèbre.

La méthode que l'on va suivre est alors la suivante. Soit $X = Spec(A)$ un S-schéma, $S = Spec(R)$. Pour tout point s du schéma de base on va considérer sa fibre dans X. Cette fibre sera alors un schéma sur le spectre d'un corps. On pourra alors travailler comme dans la section précédente sur un corps sous-jacent.

Rappelons tout d'abord ce qu'est la localisation d'un anneau par rapport à une partie multiplicative (on rappelle qu'une partie multiplicative d'un anneau est une partie stable par multiplication) :

Définition 8 (localisé d'un anneau). Le localisé $S^{-1}A$ d'un anneau A en une partie multiplicative S est l'ensemble des classes d'équivalence de $A \times A$ pour la relation d'équivalence suivante :

$$(a, b) \sim (c, d) \Leftrightarrow \exists s \in S, s(ad - bc) = 0$$

C'est un ensemble muni d'une structure d'anneau canonique, et on a un morphisme canonique $A \to S^{-1}A$ qui à $a \in A$ associe la classe de $(a, 1)$.

L'exemple le plus important de partie multiplicative est l'ensemble $A - \mathfrak{p}$, où $\mathfrak{p}$ est un idéal premier de A. On note alors le localisé $A_\mathfrak{p}$. C'est alors un anneau local d'idéal maximal $\mathfrak{p}A_\mathfrak{p}$. Le corps résiduel $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ est noté $k(\mathfrak{p})$. On a donc associé à tout point s du schéma $X = Spec(A)$ un corps $k(s)$, avec un morphisme canonique $Spec(k(s)) \to A$. Nous allons maintenant expliquer dans le cas d'un schéma X sur un schéma S ce qu'est la fibre de X en un point $s \in S$. Nous verront alors que celle-ci est un schéma sur $Spec(k(s))$, ce qui permet de se ramener au cas d'une algèbre sur un corps.

Définition 9 (produit fibré). Soient X et Y deux S-schémas. Le produit fibré de X et Y (au-dessus de S) est un schéma sur S noté $X \times_S Y$, qui a la propriété suivante : pour tout S-schéma muni de deux morphismes $Z \to X$ et $Z \to Y$ au-dessus de S, le diagramme suivant commute :

$$\begin{tikzcd}
Z \arrow[dr] \arrow[drr] \arrow[ddr] & & \\
& X \times_S Y \arrow[r] \arrow[d] & Y \arrow[d] \\
& X \arrow[r] & S
\end{tikzcd}$$

On peut remarquer que cette notion est la même que le produit ensembliste. La notion de produit fibré permet alors de définir la fibre d'un S-schéma X en un point $S \in S$. En effet on a vu que pour s un point de S, on avait un morphisme $Spec(k(s)) \to S$. On peut alors considérer le produit fibré $X \times_S Spec(k(s))$, qui est alors aussi un $Spec(k(s))$-schéma. Comme dans la notion ensembliste de produit fibré, les éléments de $X \times Spec(k(s))$ correspondent aux éléments de X qui s'envoient sur s. Cela explique donc l'appellation fibre.

Définition 10. La fibre du S-schéma X en un point $s \in S$ est le $Spec(k(s))$-schéma $X \times_S Spec(k(s))$.

On peut regarder à quoi cela correspond algébriquement. On note $X = Spec(A)$ et $S = Spec(R)$, avec un idéal premier $\mathfrak{p}$ de R. Le produit fibré correspond à un produit tensoriel, et la fibre en $\mathfrak{p}$ est donc $Spec(A \otimes_R k(\mathfrak{p}))$.

Pour se ramener comme dans la partie précédente à des algèbres sur un corps algébriquement clos, on peut plonger $k(s)$ dans une clôture algébrique $\bar{k}(s)$. Le produit fibré obtenu alors est appelé fibre géométrique en s.

La définition de schéma en groupes est du même type que celle des groupes algébriques :

Définition 11. Un S-schéma X est un schéma en groupes s'il existe des morphismes de S-schémas :
- une multiplication $m : X \times_S X \to X$,
- une inversion $i : X \to X$,
- une unité $\epsilon : S \to X$,

vérifiant les axiomes usuels de loi de groupe.

On peut donc étudier chacune des fibres géométriques d'un schéma en groupes, qui sera, sous certaines hypothèses supplémentaires, un groupe algébrique sur un corps algébriquement clos. Pour que les fibres se comportent de façon régulière en faisant varier le point $s \in S$, il faut donner à notre schéma une hypothèse de régularité telle que la lissité.

Ces observations justifient la définition d'un schéma en groupes réductif :

Définition 12 (schéma en groupes réductif). Un schéma en groupes sur un schéma S est dit réductif si c'est un schéma affine lisse sur S dont toutes les fibres géométriques sont des groupes algébriques réductifs.

L'étude des schémas en groupes réductifs est moins aisée que celle des groupes réductifs, notamment parce que la topologie de Zariski est trop grosse. Par exemple on peut définir ce qu'est un tore dans le cas des schémas en groupes, mais l'existence d'un tore maximal n'est pas assurée. Il faut pour avoir un tore maximal changer de base (en fait faire un changement de base "étale", i.e. le morphisme de changement de base doit être étale, qui est une condition de régularité plus forte que lisse).

Les schémas en groupes réductif sont alors, comme dans le cas des groupes réductifs, classifiés suivant une donnée combinatoire, toujours appelée donnée radicielle. Les théorèmes d'existence et d'unicité sont donnés dans [SGA3], tome 3.

Troisième partie

L'exemple de l'isomorphisme de Satake

On peut illustrer les différentes techniques expliquées précédemment par le texte de Mirkovic et Vilonen ([MV]). Le point de départ est le suivant : on sait qu'étant donné un goupe algébrique réductif G sur $\mathbb{C}$, on a une équivalence de catégories entre les représentations du dual de G et une certaine catégorie de faisceaux pervers (démontré par Ginzburg, [Gi], d'après des idées et résultats de Drinfeld et Lusztig, [Lu]). L'idée est alors d'étendre le résultat à des bases plus générales que $\mathbb{C}$.

Un des points importants de cette correspondance est de prouver qu'un schéma en groupes quasi-réductif (qui est d'apparence plus faible que réductif) est en fait réductif. C'est le but de l'article de Prasad et Yu ([PY]). Les réductions classiques de géométrie algébrique sont utilisées dans cet article : par exemple on se ramène à un schéma de base qui est le spectre d'un anneau de valuation discrète R. Rappelons qu'un anneau de valuation discrète est un anneau principal de dimension 1 et local. Concrètement, si on appelle π un générateur de l'idéal non nul, tous les éléments sont de la forme $c\pi^n$, pour $n \in \mathbb{N}$ et c inversible. D'autre part, on évite les divers changements de base étale en se ramenant à l' "hensélisé" de l'anneau R (cf [Ray]), qui en quelque sorte prend en compte tous les changements de base étale possibles.

En tant qu'espace topologique, $S = Spec(R)$ est alors simple : il n'a que deux points. Le premier est fermé (l'idéal πR) et est appelé point spécial, l'autre est ouvert et dense, il est appelé point générique.

Définition 13. Un schéma en groupes $\mathcal{G}$ sur S est dit quasi-réductif s'il vérifie les conditions suivantes :
- $\mathcal{G}$ est affine et plat sur R,

- la fibre générique $\mathcal{G}_K$ est connexe et lisse sur K,
- la fibre spéciale réduite $(\mathcal{G}_{\bar{k}})_{red}$ est de type fini sur $\bar{k}$ et sa composante neutre $(\mathcal{G}_{\bar{k}})^{\circ}_{red}$ est un groupe algébrique réductif de même dimension que $\mathcal{G}_K$.

Le théorème démontré par Prasad et Yu est alors le suivant :

Théorème 3. *Soit $\mathcal{G}$ un schéma en groupes quasi-réductif. Si l'une des conditions suivantes est vérifiées :*
- la caractéristique de $R/\pi R$ est différente de 2,
- le type de $\mathcal{G}_{\bar{K}}$ (i.e. sa donnée radicielle) est le même que celui de $(\mathcal{G}_{\bar{k}})^{\circ}_{red}$,
- il n'y a pas de sous-groupe fermé normal de $\mathcal{G}_{\bar{K}}$ isomorphe à SO_{2n+1}, $n \in \mathbb{N}$.
alors $\mathcal{G}$ est un schéma en groupes réductif.

On voit que les hypothèses de départ sont beaucoup plus faibles que les conditions requises pour être réductif. On ne suppose pas que le schéma est de type fini sur R, et la condition de régularité est uniquement une hypothèse de platitude.

L'idée de Prasad et Yu est de considérer un "modèle" lisse du schéma $\mathcal{G}$. Ce modèle $\hat{\mathcal{G}}$ est un schéma en groupes lisse sur $Spec(R)$ (et non plus plat), muni d'un morphisme $\hat{\mathcal{G}} \to \mathcal{G}$, ayant la même fibre générique que $\mathcal{G}$. L'idée de modèle lisse est exposé dans [BLR].

Les hypothèses de régularité permettent de prouver que le modèle $\hat{\mathcal{G}}$ est un schéma en groupes réductif. Ensuite il reste à montrer qu'il est en fait isomorphe à $\mathcal{G}$.

Références

[Bo] A.Borel, Linear algebraic groups, Springer, 1991.

[BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, Néron models, Springer Verlag, 1990.

[BT1] F. Bruhat, J. Tits, Groupes réductifs sur un corps local I, Publ. Math. IHES 41 (1972), 5-251.

[BT2] F. Bruhat, J. Tits, Groupes réductifs sur un corps local II, Publ. Math. IHES 60 (1984), 5-184.

[Gi] V. Ginzburg, Perverse sheaves on a loop group and Langland duality, Preprint Alg-geom/9551107, 1996.

[Hu] J.E. Humphreys, Linear algebraic groups, Springer, 1975.

[Ja] J.C.Jantzen, Representations of algebraic groups, Academic Press, 1987.

[Lu] G. Lusztig, Singularities, character formulas, and a q-analogue for weight multiplicities, in "Analyse et topologie sur les espaces singuliers", Astérisque 101-102, 1982.

[MV] I.Mirkovic K.Vilonen, Geometric Langlands duality and representations of algebraic groups over commutative rings, 2004.

[PY] G. Prasad, J.-K. Yu, On quasi-reductive group schemes, J.Alg.Geom 2005.

[Ray] M. Raynaud, Anneaux locaux henséliens, Lecture Notes in Mathematics 169, Springer, 1970.

[Sp] T.A. Springer, Linear Algebraic Groups, Birkhäuser, 1981.

[SGA3] Schémas en groupes (SGA3), 3 tomes (Exp. I à VII, VIII à XVIII, et XIX à XXVI), Lect.Notes Math. 151, 152, 153, Springer-Verlag, 1970.

[WA] W.C. Waterhouse, Introduction to affine group schemes, Springer-Verlag, 1979.