SUR LES REPRÉSENTATIONS DES GROUPES ALGÉBRIQUES ET DES GROUPES QUANTIQUES

SIMON RICHE, SOUS LA DIRECTION DE PATRICK POLO

Introduction

Ce texte est une introduction à la théorie des représentations des groupes algébriques semi-simples et des groupes quantiques associés, et plus particulièrement aux conjectures de Lusztig concernant les caractères des représentations irréductibles des groupes semi-simples sur un corps de caractéristique positive.

1. Les groupes algébriques

Fixons un corps $\Bbbk$ algébriquement clos. Concrètement, un groupe algébrique sur $\Bbbk$ est un sous-groupe de $\mathrm{GL}_n(\Bbbk)$ (pour un $n \geq 1$) défini par des équations polynomiales. Dans cette partie, on introduit quelques notions de base de géométrie algébrique qui permettent de donner une définition un petit peu plus abstraite (mais plus satisfaisante) des groupes algébriques, et on introduit le vocabulaire des représentations.

1.1. Notions de base de géométrie algébrique.

1.1. Notions de base de géométrie algébrique. Nous adopterons ici un point de vue très terre à terre concernant la géométrie algébrique. Nous ne parlerons par exemple que de variétés *affines*. Pour étudier plus sérieusement les groupes algébriques, nous aurions évidemment besoin de meilleures définitions (plus intrinsèques), mais elles ne sont pas nécessaires pour l'exposé de cette introduction.

Considérons un corps algébriquement clos $\Bbbk$. Si I est un idéal de $\Bbbk[X_1, \dots X_n]$, on définit $V(I) \subseteq \Bbbk^n$ comme le lieu d'annulation des polynômes de I :

$$V(I) = \{(x_1, \dots, x_n) \in \Bbbk^n \mid \forall P \in I,\, P(x_1, \dots, x_n) = 0\}.$$

La *topologie de Zariski* sur $\Bbbk^n$ est la topologie pour laquelle les fermés sont les ensembles de la forme $V(I)$ pour un idéal I de $\Bbbk[X_1, \dots X_n]$.

Une *variété algébrique affine* X (sur $\Bbbk$) est alors un fermé d'un espace $\Bbbk^n$ ($n \geq 0$), c'est-à-dire un sous-ensemble d'un espace $\Bbbk^n$ défini par une famille d'équations polynomiales. Elle est munie naturellement d'une topologie : la restriction de la topologie de Zariski à X. On l'appelle également la *topologie de Zariski* sur X.

Si $V \subseteq \Bbbk^n$ et $W \subseteq \Bbbk^m$ sont deux variétés algébriques affines, un *morphisme de variétés algébriques* de V vers W est une application $f : \Bbbk^n \to \Bbbk^m$, à coordonnées polynomiales, telle que $f(V) \subseteq W$. Si $V \subseteq \Bbbk^n$ et $W \subseteq \Bbbk^m$ sont deux variétés algébriques affines, alors $V \times W \subseteq \Bbbk^{n+m}$ est également une variété algébrique affine.

1.2. **Les groupes algébriques et leurs représentations.** Après avoir rappelé ces notions de base, on peut donner la définition d'un groupe algébrique [1].

Définition 1.2.1. *Un groupe algébrique G est une variété algébrique affine, munie d'une loi de groupe telle que la multiplication $G \times G \to G$ et l'inverse $G \to G$ soient des morphismes de variétés algébriques.*

Si G et H sont deux groupes algébriques, un morphisme de groupes algébriques de G vers H est un morphisme de groupes $G \to H$ qui est également un morphisme de variétés algébriques.

Avec cette définition, un groupe algébrique est donc un sous-ensemble d'un espace $\Bbbk^n$, défini par des équations polynomiales, muni d'une loi de groupe donnée par une formule polynomiale. L'exemple le plus simple de groupe algébrique est $(\Bbbk,+)$. Un autre exemple simple est $(\Bbbk^\times,\times)$. Pour le munir d'une structure de variété algébrique affine, on remarque qu'il est en bijection avec le fermé de $\Bbbk^2$ suivant : $\{(x,t) \in \Bbbk^2 \mid xt = 1\}$. Plus généralement, on peut considérer le groupe $\mathrm{GL}_n(\Bbbk)$, qui est en bijection avec $\{(M,t) \in \mathrm{Mat}_n(\Bbbk) \times \Bbbk \mid \det(M) \cdot t = 1\}$, ou $GL(V)$ pour un espace vectoriel de dimension finie V (la structure de variété étant définie en choisissant une base de V, ce qui permet d'identifier $\mathrm{GL}(V)$ à $\mathrm{GL}_n(\Bbbk)$ pour $n = \dim(V)$). Le groupe $\mathrm{SL}_n(\Bbbk)$ est un sous-groupe fermé de $\mathrm{GL}_n(\Bbbk)$, c'est-à-dire un sous-groupe qui est fermé pour la topologie de Zariski sur $\mathrm{GL}_n(\Bbbk)$, ce qui en fait également un groupe algébrique.

Il n'est pas très difficile de montrer que tout groupe algébrique est en fait isomorphe (comme groupe algébrique) à un sous-groupe fermé d'un $\mathrm{GL}_n(\Bbbk)$ ($n \geq 0$), ce qui justifie les propos de l'introduction.

On peut montrer que le produit de deux groupes algébriques est naturellement muni d'une structure de groupe algébrique, de même que le quotient d'un groupe algébrique par un sous-groupe distingué fermé.

Les résultats auxquels on s'intéresse dans l'étude des groupes algébriques sont de deux types : certains concernent la structure du groupe (comme variété ou comme groupe abstrait), d'autres ses représentations [2] (c'est-à-dire la façon dont il peut agir sur un espace vectoriel). Dans cet exposé on insistera surtout sur les résultats du deuxième type. Comme nous étudions ici des groupes qui ont une structure supplémentaire, nous n'étudierons que les représentations qui sont compatibles avec cette structure [3].

Définition 1.2.2. *Soit G un groupe algébrique. Si V est un espace vectoriel de dimension finie sur $\Bbbk$, une représentation de G sur V est une action linéaire de G sur V, telle que le morphisme $G \to \mathrm{GL}(V)$ correspondant soit un morphisme de groupes algébriques.*

Plus généralement, si V est un espace vectoriel de dimension quelconque sur $\Bbbk$, une représentation de G sur V est une action linéaire de G sur V, qui est localement finie (c'est-à-dire que tout point de V est inclus dans un sous-espace de dimension finie de V, stable pour l'action de G), et telle que pour tout sous espace vectoriel $W \subseteq V$ de dimension finie stable par G, l'action de G sur W induite est une représentation au sens précédent.

1. En fait, ce que nous appelons *groupe algébrique* ici devrait être appelé *groupe algébrique affine* en toute rigueur. Comme ce sont les seuls que nous considèrerons, nous avons préféré ne pas mentioner l'adjectif *affine*. Cette simplification est très courante.

2. Plus généralement, on étudie également la façon dont un groupe peut agir sur une variété. On n'en dira rien ici.

3. Ici aussi, nous simplifierons la dénomination : ce que nous appelons *représentation* devrait en toute rigueur être appelé *représentation algébrique*, ou *rationelle*.

Par exemple, l'action naturelle de $\mathrm{GL}_n(\Bbbk)$ sur $\Bbbk^n$ est une représentation de $\mathrm{GL}_n(\Bbbk)$.

Remarquons qu'avec cette définition, une représentation *irréductible* (c'est-à-dire telle que les seuls sous-espaces stables soient V et $\{0\}$) d'un groupe algébrique est nécessairement de dimension finie.

1.3. **Algèbre de Lie d'un groupe algébrique.** L'étude des groupes algébriques demande de prendre en compte deux structures différentes qui interagissent : une algébrique (celle de groupe), et une de nature géométrique et topologique (celle de variété). Dans certains cas, il est utile de se ramener à une situation totalement algébrique, en utilisant *l'algèbre de Lie* du groupe algébrique. Cette technique est efficace quand le corps $\Bbbk$ est de caractéristique nulle, mais beaucoup moins quand il est de caractéristique positive.

Définition 1.3.1. *Une algèbre de Lie L est un espace vectoriel muni d'une application bilinéaire $[\cdot,\cdot] : L \times L \to L$ qui vérifie les conditions :*
(i) $\forall X \in L, \quad [X,X] = 0.$
(ii) $\forall (X,Y,Z) \in L^3, \quad [X,[Y,Z]] + [Y,[Z,X]] + [Z,[X,Y]] = 0.$

Si G est un groupe algébrique, on peut lui associer son algèbre de Lie, notée $\mathfrak{g}$. Comme espace vectoriel, il s'agit de son espace tangent en l'unité (au sens des variétés algébriques). Si V est une représentation de G, alors $\mathfrak{g}$ agit également sur V pour en faire une représentation au sens des algèbres de Lie. Comme le cas qui nous intéresse le plus est celui où $\Bbbk$ est de caractéristique positive, nous n'entrerons pas dans ces détails. Signalons simplement que la théorie des algèbres de Lie sur un corps algébriquement clos de caractéristique nulle est très développée (voir [Hu1]). Il existe notamment un théorème de classification des algèbres de Lie semi-simples [4] très similaire au théorème 2.3.1 ci-dessous.

1.4. **Le foncteur d'induction.** Considérons un groupe algébrique G, et un sous-groupe fermé H de G. Le foncteur d'induction de H à G, noté Ind_H^G, permet d'associer, de façon fonctorielle, à toute représentation de H une représentation de G.

Soit V un $\Bbbk$-espace vectoriel. On note $\mathrm{Mor}(G,V)$ l'ensemble des applications $\phi : G \to V$ telles que $\phi(G)$ soit inclus dans un sous-espace vectoriel W de V de dimension finie, et telles que $\phi : G \to W$ soit un morphisme de variétés algébriques. Si V est une représentation de H, on définit alors

$$\mathrm{Ind}_H^G(V) := \{\phi \in \mathrm{Mor}(G,V) \mid \forall h \in H, \forall g \in G, \, \phi(gh) = h^{-1} \cdot \phi(g)\}.$$

On définit une action de G sur cet espace vectoriel en posant $(g \cdot \phi)(g') = \phi(g^{-1}g')$. On peut vérifier que ceci définit un foncteur de la catégorie des représentations de H dans celle des représentations de G, qui est adjoint à droite du foncteur naturel de restriction de G à H, noté Res_H^G, c'est-à-dire qu'on a

$$\mathrm{Hom}_G(V, \mathrm{Ind}_H^G(W)) = \mathrm{Hom}_H(\mathrm{Res}_H^G(V), W)$$

pour toute représentation V de G et toute représentation W de H.

L'étude de ces foncteurs (et de leurs foncteurs dérivés) est extrêment importante dans la théorie des représentations des groupes algébriques.

4. On ne rappellera pas ici la définition de la semi-simplicité pour les algèbres de Lie. Elle est évidemment similaire à la définition pour les groupes algébriques.

2. Les groupes algébriques réductifs et semi-simples

L'étude des représentations des groupes algébriques se ramène essentiellement à celle des représentations d'une classe particulière de groupes algébriques, les groupes *réductifs*. On introduira également une sous-famille des groupes réductifs, pour laquelle les résultats sont parfois plus simples à énoncer, les groupes *semi-simples*.

2.1. **Groupes algébriques réductifs et semi-simples : définitions.** Pour définir les groupes algébriques réductifs ou semi-simples, il faut introduire tout d'abord une définition. Un groupe algébrique est dit *unipotent* si son seul module simple est le module trivial $\Bbbk$. Rappelons également qu'un groupe (abstrait) G est dit *résoluble* si $\mathcal{D}^i(G) = \{1\}$ pour i assez grand, où $\mathcal{D}^1(G) = \mathcal{D}(G)$ est le sous-groupe de G engendré par les commutateurs $ghg^{-1}h^{-1}$, $(g,h) \in G^2$, et $\mathcal{D}^{n+1}(G) = \mathcal{D}(\mathcal{D}^n(G))$. On peut vérifier qu'un groupe algébrique unipotent est résoluble.

Définition 2.1.1. *Un groupe algébrique G est dit réductif s'il ne possède pas de sous-groupe fermé, connexe, unipotent, et distingué autre que $\{1\}$.*

Il est dit semi-simple s'il ne possède pas de sous-groupe fermé, connexe, résoluble, et distingué autre que $\{1\}$.

Par exemple, on peut montrer que le groupe $\mathrm{GL}_n(\Bbbk)$ est réductif, et que le groupe $\mathrm{SL}_n(\Bbbk)$ est semi-simple.

Pour motiver cette définition, considérons un groupe algébrique G quelconque. Il possède un unique sous-groupe fermé, connexe, unipotent (respectivement résoluble), distingué, et maximal pour cette propriété ([Hu2, 19.5]). On le note $\mathcal{R}_u(G)$ (respectivement $\mathcal{R}(G)$). Si V est une représentation irréductible de G, $\mathcal{R}_u(G)$ agit trivialement sur V (en effet, V contient un sous-espace qui est une représentation irréductible de $\mathcal{R}_u(G)$, c'est-à-dire une droite sur laquelle $\mathcal{R}_u(G)$ agit trivialement ; comme la représentation est irréductible, cette droite engendre V comme représentation de G ; et comme $\mathcal{R}_u(G)$ est distingué dans G, on en déduit qu'il agit trivialement sur V). La représentation se factorise donc par le quotient $G/\mathcal{R}_u(G)$, qui est un groupe réductif. On fera assez souvent l'hypothèse supplémentaire que G est un groupe connexe. Mais si G est un groupe algébrique quelconque, sa composante connexe qui contient 1_G est un sous-groupe fermé, distingué, d'indice fini, noté G^0. L'étude de G se ramène donc à celle de G^0, qui est un groupe algébrique connexe, et celle de G/G^0, qui est un groupe fini.

Il existe de très nombreux résultats de structure pour les groupes algébriques réductifs connexes, qui généralisent des résultats classiques sur $\mathrm{GL}_n(\Bbbk)$, comme par exemple la décomposition de Bruhat (voir [Hu2]). On peut également classer les groupes algébriques réductifs connexes à isomorphisme près, en leur faisant correspondre une *donnée radicielle*. Le résultat de classification des groupes semi-simples est un petit peu plus facile à énoncer, et essentiellement équivalent. Il fait intervenir la notion très importante de *système de racines*.

2.2. **Systèmes de racines.** La notion de système de racines est de nature combinatoire. Elle est extrêmement importante dans toutes les théories de Lie.

Considérons un espace vectoriel V sur $\mathbb{R}$, de dimension finie. Si $v \in V$, une *réflexion de vecteur v* est un endomorphisme s de V qui laisse fixe un hyperplan de V, et qui vérifie $s(v) = -v$.

Définition 2.2.1. *Un sous-ensemble R de V est appelé un système de racines*[5] *s'il vérifie les axiomes suivants :*

(i) *R est fini, engendre V et ne contient pas 0.*

5. Ici encore, on simplifie la terminologie : pour être exact, ce qu'on définit ici est un système de racines *réduit*.

(ii) *Pour tout* $\alpha \in R$*, il existe une réflexion* s_α *de* V*, de vecteur* α*, laissant stable* R *(grâce à l'axiome* (i)*, elle est alors unique).*

(iii) *Si* $\alpha,\beta \in R$*, alors* $s_\alpha(\beta) - \beta$ *est un multiple entier de* α*.*

(iv) *Si* $\alpha \in R$*, les seuls multiples de* α *dans* R *sont* $\pm\alpha$*.*

Si R est un système de racines, on note W le sous-groupe de $\mathrm{GL}(V)$ engendré par les s_α, $\alpha \in R$. C'est un groupe fini, appelé le *groupe de Weyl* de R. Comme W est fini, il existe un produit scalaire sur V invariant par W, qu'on note $(\cdot,\cdot)$. On a alors $s_\alpha(\lambda) = \lambda - \langle\lambda,\alpha\rangle\alpha$, où $\langle\lambda,\alpha\rangle = 2(\lambda,\alpha)/(\alpha,\alpha)$.

Classer les systèmes de racines à isomorphisme [6] près ne pose aucune difficulté. Chaque système est (de façon unique) somme directe de systèmes *irréductibles*. Il existe quatre familles infinies de systèmes irréductibles, appelées $\mathbf{A}_n$ ($n \geq 1$), $\mathbf{B}_n$ ($n \geq 2$), $\mathbf{C}_n$ ($n \geq 3$) et $\mathbf{D}_n$ ($n \geq 4$), et cinq types exceptionnels, appelés $\mathbf{E}_6$, $\mathbf{E}_7$, $\mathbf{E}_8$, $\mathbf{F}_4$ et $\mathbf{G}_2$.

Si R est un système de racines, notons $\Lambda(R)$ l'ensemble de ses *poids*, c'est-à-dire les éléments $\lambda \in V$ tels que pour tout $\alpha \in R$, $\langle\lambda,\alpha\rangle \in \mathbb{Z}$. Il s'agit d'un groupe abélien libre, de rang $\dim(V)$. Il contient le réseau des racines $\mathbb{Z}R$ (c'est-à-dire le sous-groupe de V engendré par R), mais est généralement plus gros. Le groupe $\Lambda(R)/\mathbb{Z}R$ est appelé le *groupe fondamental* de R. Il s'agit d'un groupe fini, donné par le tableau suivant :

$\mathbf{A}_n$	$\mathbf{B}_n$, $\mathbf{C}_n$, $\mathbf{E}_7$	$\mathbf{D}_n$ (n pair)	$\mathbf{D}_n$ (n impair)	$\mathbf{E}_6$	$\mathbf{E}_8$, $\mathbf{F}_4$, $\mathbf{G}_2$
$\mathbb{Z}/(n+1)\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	0

Choisissons un hyperplan de V qui ne contient aucune racine. Choisissons un des demi-espaces délimités par cet hyperplan, et notons R^+ les racines contenues dans ce demi-espace, qu'on appelle *racines positives*. Un poids λ est dit *dominant* si pour tout $\alpha \in R^+$, $\langle\lambda,\alpha\rangle \geq 0$. Ces poids joueront un rôle très important dans l'étude des représentations d'un groupe algébrique semi-simple. On la notera $\Lambda(R)^+$.

On définit également une relation d'ordre sur $\Lambda(R)$ par $\lambda \leq \mu$ si et seulement si $\mu - \lambda$ est une somme de racines positives. Notons que ces deux définitions dépendent du choix d'une famille de racines positives.

2.3. **Groupes algébriques semi-simples : classification.** Commençons par remarquer qu'un groupe algébrique G est résoluble connexe si et seulement si toute représentation irréductible de G est de dimension 1 ([Hu2, 17]). Si G est résoluble connexe et si de plus toute représentation de G est somme directe de représentations irréductibles, on dira que G est un *tore* (cite[16]Hu2).

Soit G un groupe algébrique semi-simple connexe. Notons T un tore maximal de G. Pour $G = \mathrm{SL}_n(\Bbbk)$, on peut prendre pour T le sous-groupe des matrices diagonales. On note $X(T)$ les *caractères* de T, c'est-à-dire le groupe abélien des morphismes de groupes algébriques $T \to \Bbbk^\times$. Alors T agit par conjugaison sur l'algèbre de Lie $\mathfrak{g}$ de G, et on a une décomposition

$$\mathfrak{g} = \bigoplus_{\lambda \in X(T)} \mathfrak{g}_\lambda$$

où $\mathfrak{g}_\lambda := \{x \in \mathfrak{g} \mid \forall t \in T,\ t \cdot x = \lambda(t)x\}$. Pour $G = \mathrm{SL}_n(\Bbbk)$, on a $\mathfrak{g} = \mathrm{Ker}(\mathrm{Tr})$, et la décomposition précédente est donnée par

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{i \neq j} \Bbbk E_{i,j},$$

où $\mathfrak{h}$ désigne le sous-espace des matrices diagonales de trace nulle.

6. On laisse au lecteur le soin de deviner quelle est la notion d'isomorphisme à considérer ici, ou de consulter [Hu1] ou [BLie].

Notons $R = \{\lambda \in X(T) - \{0\} \mid \mathfrak{g}_\lambda \neq 0\}$. Alors on peut vérifier que R est un système de racines dans l'espace $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$, et que

$$\mathbb{Z}R \subseteq X(T) \subseteq \Lambda(R).$$

On a alors le résultat de classification suivant ([Hu2, 32]) :

Théorème 2.3.1. (i) *Un groupe algébrique semi-simple est quasi-simple (c'est-à-dire ne possède pas de sous-groupe distingué connexe non trivial) si et seulement si son système de racines est irréductible.*

(ii) *Tout groupe algébrique semi-simple connexe est de façon unique un quotient par un sous-groupe fini d'un produit de groupes algébriques connexes quasi-simples.*

(iii) *De plus, un groupe algébrique connexe quasi-simple est déterminé de façon unique par son système de racines et son groupe fondamental $\Lambda(R)/X(T)$. Pour chaque système irréductible R et chaque sous-groupe de $\Lambda(R)/\mathbb{Z}R$, il existe un (unique) groupe correspondant.*

Un groupe algébrique semi-simple connexe est dit *simplement connexe* si $X(T) = \Lambda(R)$, et *de type adjoint* si $X(T) = \mathbb{Z}R$.

Donnons quelques exemples : le groupe $\mathrm{SL}_n(\Bbbk)$ est simplement connexe, de type $\mathbf{A}_{n+1}$; $\mathrm{SO}_{2n+1}(\Bbbk)$ est de type adjoint, de type $\mathbf{B}_n$; $\mathrm{Sp}_{2n}(\Bbbk)$ est simplement connexe, de type $\mathbf{C}_n$; $\mathrm{SO}_{2n}(\Bbbk)$ est de type $\mathbf{D}_n$, et n'est ni simplement connexe, ni de type adjoint.

Cette classification est indépendante du choix du corps $\Bbbk$ (et en particulier de sa caractéristique). On pourra donc parler du “même” groupe G pour différents corps.

2.4. **Groupes algébriques réductifs : représentations.** Dans la suite, on s'intéresse aux représentations d'un groupe algébrique réductif connexe G. Remarquons que, comme précédemment, on peut lui associer un système de racines R (la différence est que ce n'est pas un système de racines dans $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$, mais dans un sous-espace de cet espace).

Soit T un tore maximal de G. Si V est une représentation de G, elle est somme d'espaces de poids pour T, c'est-à-dire que

$$V = \bigoplus_{\lambda \in X(T)} V_\lambda$$

où, pour $\lambda \in X(T)$, on a noté $V_\lambda = \{x \in V \mid \forall t \in T,\ t \cdot v = \lambda(t)v\}$. Si V est de dimension finie, on définit son *caractère* comme l'élément suivant de l'algèbre de groupe $\mathbb{Z}[X(T)]$:

$$\mathrm{ch}(V) := \sum_{\lambda \in X(T)} \dim(V_\lambda) e(\lambda).$$

On appelle *sous-groupe de Borel* de G un sous-groupe fermé résoluble connexe maximal (tous les tels sous-groupes de G sont conjugués : [Hu2, 21.3]). Comme on l'a vu plus haut, les groupes résolubles connexes sont ceux qui ont leurs représentations irréductibles de dimension 1. Il est donc naturel, dans l'étude des représentations de G, de considérer un tel sous-groupe le gros possible, et d'induire les représentations simples de ce sous-groupe jusqu'à G. On considère donc un tore maximal T de G, et un sous-groupe de Borel B de G contenant T. A ce choix est alors associé une famille de racines positives R^+ (celles qui apparaissent dans la décomposition en poids pour T de $\mathfrak{g}/\mathfrak{b}$, pour les algèbres de Lie $\mathfrak{b}$ de B et $\mathfrak{g}$ de G). La notion de poids dominant ainsi que la relation d'ordre considérées dans la suite sont toujours prises relativement à ce choix. On peut montrer que $X(B) = X(T)$. Si $\lambda \in \Lambda(R)^+ \cap X(T)$, on note $\Bbbk_B(\lambda)$ la représentation de B de dimension 1 associée à λ, et

$$H^0(\lambda) = \mathrm{Ind}_B^G(\Bbbk_B(\lambda)).$$

Cette représentation est de dimension finie. Elle possède une unique sous-représentation irréductible, qu'on note $L(\lambda)$. Les $L(\lambda)$ sont alors toutes les représentations irréductibles de G, et sont non isomorphes deux à deux ([Hu2, 31.3, 31.4]).

Les représentations $H^0(\lambda)$ sont bien connues. Il existe notamment une formule (la *formule des caractères de Weyl*) qui donne explicitement le caractère de cette représentation. Les caractères qui apparaissent dans cette représentation sont λ (avec multiplicité 1), et d'autres poids qui sont tous inférieurs à λ pour l'ordre considéré sur les poids. Pour cette raison, λ est appelé le *plus haut poids* de $H^0(\lambda)$. Si le corps $\Bbbk$ est de caractéristique 0, la représentation $H^0(\lambda)$ est irréductible : on a donc $L(\lambda) = H^0(\lambda)$. Dans ce cas, on connait donc très bien les représentations irréductibles. De plus, on peut montrer que toute représentation de G est somme directe de représentations irréductibles.

Si la caractéristique de $\Bbbk$ est positive, la situation est beaucoup plus compliquée. Les représentations de G ne sont pas nécessairement sommes directes de représentations irréductibles. Et le problème de la détermination des caractères des représentations irréductibles est beaucoup plus difficile. Dans la suite, on s'intéresse au problème du calcul de ces caractères, dans le cas où G est semi-simple. Remarquons tout d'abord que supposer G semi-simple ne restreint pas la généralité : en effet, si G est un groupe réductif, alors $\mathcal{R}(G)$ est un sous-groupe central ; si V une représentation irréductible de G, $\mathcal{R}(G)$ agit donc sur V par un caractère ; quitte à tensoriser par l'opposé de ce caractère, on peut supposer qu'il est trivial ; la représentation se factorise alors en une représentation de $G/\mathcal{R}(G)$, qui est semi-simple.

Pour comprendre l'intérêt de ce problème, il faut signaler que les poids de $L(\lambda)$ vérifient la même propriété que celle des poids de $H^0(\lambda)$ signalée ci-dessus, à savoir que λ apparaît avec multiplicité 1, et que tous les autres poids qui apparaissent sont inférieurs à λ. En particulier, les $\mathrm{ch}(L(\lambda))$ sont linéairement indépendants. Si V est une représentation de G de dimension finie, il existe une suite de sous-représentations

$$(*) \qquad V = V^0 \subset V^1 \subset \ldots \subset V^{r-1} \subset V^r = V$$

telle que pour tout $i = 1 \ldots r$, V^i/V^{i-1} est une représentation irréductible, donc est isomorphe à $L(\lambda_i)$ pour un certain poids dominant λ_i. On a alors

$$\mathrm{ch}(V) = \sum_{i=1}^{r} \mathrm{ch}(L(\lambda_i)).$$

Comme les $\mathrm{ch}(L(\lambda))$ sont linéairement indépendants, cette écriture est unique. Ceci démontre d'une part que les $L(\lambda_i)$ qui apparaissent dans $(*)$ sont uniques[7] (on les appelle les *facteurs de composition* de V), et d'autre part que pour les déterminer, il suffit de décomposer $\mathrm{ch}(V)$ en une somme de termes de la forme $\mathrm{ch}(L(\lambda))$ (ce qui est possible, de façon unique).

Si on connaît les caractères des $L(\lambda)$ pour tout poids dominant λ, on peut donc déterminer les facteurs de composition d'un module uniquement en calculant son caractère.

3. Les groupes quantiques de Lusztig

Comme on l'a dit plus haut, si le corps $\Bbbk$ est de caractéristique nulle, il existe une assez bonne correspondance entre les propriétés et les représentations d'un groupe algébrique et de son algèbre de Lie. Ce n'est plus le cas en caractéristique positive. Par exemple, si le groupe $G = \Bbbk^\times$ agit sur $\Bbbk$ par $(t \cdot x) = t^p x$, cette représentation

7. En fait, cette unicité est un fait très général : c'est le théorème de Jordan-Hölder.

est non triviale, alors que la dérivée de cette représentation est la représentation triviale de l'algèbre de Lie $\mathfrak{g} = \Bbbk$ sur $\Bbbk$.

Il faut donc introduire d'autres objets algébriques, qui vivent en caractéristique 0, et qui donnent de bonnes informations sur les représentations des groupes. Il s'agit des groupes quantiques, introduits par G. Lusztig en 1988 [8]. Pour les définir, on considère une $\mathbb{C}(q)$-algèbre (où q est une indéterminée), définie par générateurs et relations, ces dernières étant des déformations des relations de Serre donnant une présentation de l'algèbre de Lie $\mathfrak{g}$ de G (voir [Hu1, 18.1]), puis on “spécialise” ce paramètre q.

3.1. **Définition.** Soit R le système de racines du groupe semi-simple G. Soit I une base de ce système de racines [9]. Le groupe quantique $U_q(\mathfrak{g})$ associé à G est la $\mathbb{C}(q)$-algèbre définie par les générateurs

$$E_i,\ F_i,\ K_i,\ K_i^{-1}\ (i \in I)$$

et les relations, pour i et j dans I :

(R1): $K_iK_j = K_jK_i$; $K_iK_i^{-1} = 1$

(R2): $K_iE_jK_i^{-1} = q^{(i,j)}E_j$; $K_iF_jK_i^{-1} = q^{-(i,j)}F_j$

(R3): $E_iF_j - F_jE_i = \delta_{ij}\frac{K_i - K_i^{-1}}{q^{d_i} - q^{-d_i}}$

(R4): $\sum_{s=0}^{1-a_{ij}} (-1)^s \begin{bmatrix} 1-a_{ij} \\ s \end{bmatrix}_{d_i} E_i^{1-a_{ij}-s}E_jE_i^s = 0$

(R5): $\sum_{s=0}^{1-a_{ij}} (-1)^s \begin{bmatrix} 1-a_{ij} \\ s \end{bmatrix}_{d_i} F_i^{1-a_{ij}-s}F_jF_i^s = 0$

où on a noté $[N]_d! = \prod_{s=1}^{N} \frac{q^{ds}-q^{-ds}}{q^d - q^{-d}}$, $\begin{bmatrix} N \\ M \end{bmatrix}_d = \frac{[N]_d!}{[M]_d![N-M]_d!}$ $(d \in \mathbb{N})$, $a_{i,j} = \frac{(i,j)}{(j,j)}$ (les d_i, choisis dans $\{1,2,3\}$, sont tels que la matrice $(d_ia_{i,j})$ est symétrique).

On peut ensuite définir des *spécialisations* de $U_q(\mathfrak{g})$. Fixons un entier $l \in \mathbb{N} - \{0\}$. Notons $\mathcal{A} := \mathbb{C}[q,q^{-1}]$. Notons maintenant $U_{\mathcal{A}}$ la sous-$\mathcal{A}$-algèbre de $U_q(\mathfrak{g})$ engendrée par les éléments

$$E_i^{(N)} = \frac{E_i^N}{[N]_{d_i}!},\ F_i^{(N)} = \frac{F_i^N}{[N]_{d_i}!},\ K_i,\ K_i^{-1},\ i \in I,\ N \geq 1.$$

Notons enfin $\mathcal{M}$ l'idéal de $\mathcal{A}$ engendré par $(q - e^{2i\pi/l})$. Le groupe quantique de Lusztig U est alors défini par :

$$\mathsf{U} := \mathsf{U}_{\mathcal{A}}/(\mathcal{M} \cdot \mathsf{U}_{\mathcal{A}} + \sum_{i \in I}(K_i^l - 1)\mathsf{U}_{\mathcal{A}}).$$

C'est une algèbre sur $\mathbb{C}$, c'est-à-dire définie en caractéristique 0 (ce qui facilite les calculs). Mais, grâce à l'utilisation des puissances divisées, quand $l = p$, elle va en fait se comporter comme le groupe G en caractéristique p.

3.2. **Représentations du groupe quantique U.** On peut développer pour le groupe quantique U une théorie tout à fait similaire à celle des groupes algébriques semi-simples. En particulier, on peut définir une sous-algèbre B de U qui joue un rôle similaire à celui joué par le sous-groupe de Borel B. On a alors un foncteur d'induction $\mathrm{Ind}_{\mathsf{B}}^{\mathsf{U}}$, et on peut définir là aussi le U-module $H_q^0(\lambda) = \mathrm{Ind}_{\mathsf{B}}^{\mathsf{U}}(\Bbbk_{\mathsf{B}}(\lambda))$ et son unique sous-module simple $L_q(\lambda)$ pour tout poids dominant λ. Les $L_q(\lambda)$ sont alors tous les U-modules simples *de type 1* (ce ne sont pas tous les modules simples de U, mais il suffit de connaître ceux-ci pour les connaître tous). Il existe également

8. En fait, les groupes quantiques ont été “inventés” par Drinfeld et Jimbo (indépendamment). Lusztig a été le premier à les utiliser dans l'étude des représentations des groupes algébriques semi-simples.

9. On n'a pas défini cette notion ici. On laisse au lecteur le soin de deviner de quoi il s'agit, ou de consulter [Hu1] ou [BLie] ...

une notion de caractère pour un U-module de dimension finie, analogue à la notion précédente.

4. Les conjectures de Kazhdan-Lusztig et Lusztig

Dans cette partie on introduit la conjecture à laquelle on s'intéresse. On rappelle auparavant une autre conjecture, énoncée un petit peu plus tôt (et totalement résolue depuis), qui en est en quelque sorte l'origine. On ne considèrera que des groupes semi-simples simplement connexes (c'est-à-dire tels que $X(T) = \Lambda(R)$), mais ceci ne restreint pas la généralité, étant donné que tout groupe semi-simple est quotient d'un groupe simplement connexe.

4.1. **La conjecture de Kazhdan-Lusztig pour les algèbres de Lie semi-simples.** Soit L une algèbre de Lie semi-simple de dimension finie sur un corps $\Bbbk$ algébriquement clos de caractéristique nulle. Il existe un groupe semi-simple simplement connexe G tel que L soit l'algèbre de Lie de G. Les représentations irréductibles de dimension finie de L sont les $H^0(\lambda)$ introduites plus haut. Elles sont donc bien connues. Il existe cependant d'autres représentations irréductibles de L dans la catégorie $\mathcal{O}$, qui sont de dimension infinie, mais qui sont une somme d'espaces de poids (pour la sous-algèbre de Cartan de L) de dimension finie, ce qui permet de définir leur caractère. Elle sont paramétrées par les poids non dominants de R.

En 1979, Kazhdan et Lusztig ont proposé une conjecture donnant ces caractères [10] (en tout cas pour certains poids). Cette conjecture a été prouvée en 1981 indépendamment par Beilinson-Bernstein et Brylinski-Kashiwara. L'idée de cette preuve est de construire une équivalence de catégories entre une sous-catégorie $\mathcal{O}_0$ de $\mathcal{O}$ et une catégorie de faisceaux pervers sur la variété algébrique G/B, de traduire le problème du calcul des caractères en termes de faisceaux pervers, et enfin de résoudre ce problème grâce aux outils très puissants que l'on possède pour étudier ces objets (qui généralisent la théorie des poids pour la cohomologie des variétés algébriques).

4.2. **La conjecture de Lusztig pour les groupes algébriques.** Une conjecture similaire a été proposée en 1980 par Lusztig, qui donne les caractères des représentations irréductibles d'un groupe algébrique semi-simple simplement connexe sur un corps de caractéristique positive p, toujours en terme de valeurs en 1 de polynômes de Kazhdan-Lusztig (voir [Lu1]). La formule donnée par cette conjecture n'est pas vérifiée pour tous les poids dominants si la caractéristique du corps est trop petite. Cependant, la conjecture affirme qu'il existe une borne explicite, ne dépendant que du système de racines du groupe G (plus précisément, de son *nombre de Coxeter* h : $2h-2$ semble être un bon candidat), telle que pour tout groupe G et tout nombre premier p au-delà de cette borne, les caractères des représentations irréductibles de G sont donnés par cette formule.

Cette conjecture a été vérifiée par le calcul pour les "petits" groupes, par exemple $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$, $\mathbf{B}_2$, $\mathbf{G}_2$.

4.3. **La preuve actuelle de cette conjecture.** Quelques années plus tard, en 1990, Lusztig a proposé une méthode de résolution de sa conjecture (voir [Lu2]) :

(i) Tout d'abord, prouver un résultat analogue pour le groupe quantique U associé à G (pour $l = p$).

10. En fait, la conjecture porte sur les multiplicités des représentations irréductibles dans les modules de Verma. Mais ce problème est tout à fait équivalent à celui du calcul des caractères des représentations irréductibles. Ces multiplicités sont données comme des valeurs en 1 de certains polynômes définis de façon combinatoire, les *polynômes de Kazhdan-Lusztig*.

(ii) Puis démontrer que les caractères des représentations irréductibles pour G et pour U sont identiques[11] (pour p supérieur à la borne mentionnée).

Le point (i) a été démontré en toute généralité (c'est-à-dire pour p supérieur à une borne explicite, et très petite), grâce aux travaux de D. Kazhdan, G. Lusztig, M. Kashiwara et T. Tanisaki, en se ramenant à un problème concernant les algèbres de Lie de Kac-Moody, qui est une généralisation de la conjecture évoquée en 4.1, et donc finalement à un problème concernant la *variété grassmannienne affine*.

Cependant, le point (ii) est plus délicat. H. H. Andersen, J. C. Jantzen et W. Soergel se sont attelés à cette preuve, mais ils n'ont pu prouver (en 1994) qu'un résultat plus faible : pour chaque groupe G, il existe une borne (mais qu'on ne sait pas calculer, même pour le type $\mathbf{A}_n$) au-delà de laquelle l'égalité des caractères est vraie. Ce résultat est déjà intéressant, mais pas vraiment satisfaisant : si on prend un groupe G et un premier p, on ne sait pas si la conjecture est vraie !

Références

[BLie] N. Bourbaki, *Groupes et Algèbres de Lie, chapitres 4,5 et 6*, Hermann, 1968.

[Hu1] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer, 1972.

[Hu2] J. E. Humphreys, *Linear Algebraic Groups*, Springer, 1975.

[Ja1] J. C. Jantzen, *Representations of Algebraic Groups, second edition*, American Mathematical Society, 2003.

[Ja2] J. C. Jantzen, *Lectures on Quantum Groups*, American Mathematical Society, 1996.

[Lu1] G. Lusztig, *Some Problems in the Representation Theory of Finite Chevalley Groups*, in B. Cooperstein, G. Mason, *The Santa Cruz Conference on Finite Groups*, Proc. Symp. Pure Math. 37 (1980) p. 313-317.

[Lu2] G. Lusztig, *On Quantum Groups*, J. of Algebra 131 (1990) p. 466-475.

11. En fait, cette conjecture n'affirme l'égalité des caractères que pour les représentations irréductibles dont le poids dominant est *restreint*. Mais la connaissance des caractères de ces représentations suffit à les connaître tous, grâce à un théorème classique de Steinberg.