Invent. math. 116, 513–530 (1994)

Inventiones mathematicae

Sur la semi-simplicité des produits tensoriels de représentations de groupes

Jean-Pierre Serre

Collège de France, 3 rue d'Ulm, F-75005 Paris, France

Oblatum 5-VII-1993

à Armand Borel

Introduction

Soit k un corps. Soit G un groupe, et soient V_1 et V_2 deux $k[G]$-modules de dimension finie sur k, autrement dit deux représentations linéaires de G. Soit $V_1 \otimes V_2$ le produit tensoriel de V_1 et V_2.

Dans [3], p. 88, Chevalley démontre:

(*) *Supposons k de caractéristique* 0. *Alors, si V_1 et V_2 sont semi-simples, il en est de même de $V_1 \otimes V_2$.*

(Autrement dit, la catégorie des représentations semi-simples de G est stable par les opérations tensorielles.)

Je me propose de montrer que ce théorème reste vrai en caractéristique $p>0$ pourvu que les dimensions des représentations soient assez petites:

(**) *Supposons que k soit de caractéristique $p>0$ et que l'on ait:*

$$\dim V_1 + \dim V_2 < p+2.$$

Alors, si V_1 et V_2 sont semi-simples, il en est de même de $V_1 \otimes V_2$.

Il y a un résultat analogue pour les produits tensoriels de m représentations, avec $p+2$ remplacé par $p+m$, cf. n° 1.2, th. 1.

La démonstration fait l'objet des §§ 1, 2, 3, 4 ci-après.

Le § 1 contient des réductions élémentaires.

Le § 2 traite le cas où G est le groupe des points d'un groupe algébrique quasi-simple simplement connexe, les représentations considérées étant algébriques et «restreintes». On utilise les propriétés des représentations dont les poids dominants appartiennent à la «petite alcôve», cf. [6]. Les principaux arguments intervenant dans la démonstration m'ont été communiqués en 1986 par J.C. Jantzen (voir aussi [7]); je l'en remercie vivement.

Let § 3 étend les résultats du § 2 au cas d'un groupe algébrique dont la composante neutre est d'indice premier à p.

Le §4 réduit le cas général au cas précédent, grâce à un procédé de «saturation» (déjà utilisé dans [8] et [9]) qui permet de remplacer les éléments d'ordre p par des groupes additifs à un paramètre.

1 Enoncé du théorème, exemples, et premières réductions

1.1. Notations

Le corps de base k est de caractéristique $p>0$; dans les §§2, 3, 4 on le suppose algébriquement clos.

On note G un groupe, et $k[G]$ l'algèbre de G sur k.

Par un *G-k-module* (ou simplement un *G-module*) on entend un $k[G]$-module de dimension finie sur k. Si V est un tel module, V est un k-espace vectoriel de dimension finie, et l'action de G sur V est définie par un homomorphisme $G \to \mathbf{GL}(V)$, autrement dit par une *représentation linéaire* de G dans V.

1.2. Enoncé du théorème

Soient $V_1, \ldots, V_m$ des G-modules, et soit $W = V_1 \otimes \ldots \otimes V_m$ leur produit tensoriel (sur k). Le groupe G opère sur W par transport de structure; on a

$$g \cdot (x_1 \otimes \ldots \otimes x_m) = (g x_1) \otimes \ldots \otimes (g x_m) \quad \text{si} \quad g \in G, \ x_i \in V_i.$$

Cette action de G fait de W un G-module.

Le théorème que nous avons en vue est:

Théorème 1 *Supposons que les G-modules V_i soient semi-simples, et que l'on ait:*

$$\sum_{i=1}^{m} (\dim V_i - 1) < p.$$

Alors le G-module $V_1 \otimes \ldots \otimes V_m$ est semi-simple.

Le cas particulier $m=2$ donne le résultat énoncé dans l'introduction:

Corollaire 1 *Si V_1 et V_2 sont semi-simples et si* $\dim V_1 + \dim V_2 < p+2$, *alors $V_1 \otimes V_2$ est semi-simple.*

On en déduit:

Corollaire 2 *Soit V un G-module semi-simple de dimension* $\leqq (p+1)/2$. *Alors les G-modules* $\mathrm{End}(V)$, $\mathrm{Sym}^2 V$ *et* $\wedge^2 V$ *sont semi-simples.*

D'après le cor. 1, $V \otimes V$ est semi-simple. Il en est donc de même de $\mathrm{Sym}^2 V$ et de $\wedge^2 V$, qui en sont des quotients. D'autre part, la semi-simplicité de V entraîne celle de son dual V^*; d'où, par le même argument, la semi-simplicité de $V \otimes V^* = \mathrm{End}(V)$.

Remarque. La majoration $\sum(\dim V_i - 1) < p$ du th. 1 est essentiellement optimale, comme le montre le cas où $G = \mathbf{SL}_2(k)$, cf. n° 1.3. Par contre, l'inégalité

$\dim V \leqq (p+1)/2$ du cor. 2 peut être améliorée d'une unité en ce qui concerne $\wedge^2 V$, cf. Appendice.

Question. Y a-t-il un énoncé analogue à celui du th. 1 pour les représentations linéaires des *k-schémas en groupes*, non nécessairement lisses (ou, ce qui revient au même, pour les comodules sur les bigèbres ayant une antipode, cf. [5], II, §2)? Le cas particulier le plus intéressant (et sans doute crucial) est celui des «groupes infinitésimaux de hauteur $\leqq 1$», qui correspondent aux *p-algèbres de Lie* ([5], II, §7, nº 4).

1.3. Exemples

Prenons $G = \mathbf{SL}_2(k)$, considéré comme groupe de transformations linéaires en deux variables x, y:

$$(x, y) \mapsto (ax+by, cx+dy), \qquad ad-bc=1.$$

Si $d \geqq 0$, notons $V(d)$ le k-espace vectoriel des polynômes homogènes de degré d en x et y. L'espace $V(d)$ a pour base:

$$\{x^d, x^{d-1}y, \ldots, y^d\}.$$

On a $\dim V(d) = d+1$. L'action naturelle de G sur $V(d)$ en fait un G-module. On sait que ce G-module est *simple* si $d < p$. Le module $V(p)$ a un sous-espace stable V' de dimension 2 stable par G, à savoir celui de base $\{x^p, y^p\}$, le quotient $V(p)/V'$ étant isomorphe à $V(p-2)$. La projection $V(p) \to V(p-2)$ est donnée par:

$$f \mapsto \frac{1}{y}\,\partial f/\partial x = -\frac{1}{x}\,\partial f/\partial y.$$

On a donc une suite exacte:

$$0 \to V' \to V(p) \to V(p-2) \to 0.$$

Lorsque le nombre d'éléments de k est >2, on vérifie que la suite exacte de G-modules ci-dessus *n'est pas scindée*; le G-module $V(p)$ n'est donc pas semi-simple.

Choisissons alors des entiers $d_1, \ldots, d_m$, compris entre 1 et $p-1$, tels que $\sum d_i = p$. L'application produit

$$(f_1, \ldots, f_m) \mapsto f_1 \ldots f_m$$

définit un homomorphisme de G-modules $V(d_1) \otimes \ldots \otimes V(d_m) \to V(p)$. Cet homomorphisme est surjectif. Comme $V(p)$ n'est pas semi-simple, le produit tensoriel $V(d_1) \otimes \ldots \otimes V(d_m)$ n'est pas semi-simple.

Or les $V(d_i)$ sont semi-simples (et même simples), et l'on a $\dim V(d_i) - 1 = d_i$. D'où:

$$\sum (\dim V(d_i) - 1) = p,$$

ce qui montre que l'inégalité du th. 1 ne peut pas être améliorée.

1.4. Préliminaires à la démonstration du théorème 1

1.4.1 On peut supposer que $m \geqq 2$, et que le théorème est vrai pour $m-1$ modules.

1.4.2 On peut supposer que les V_i sont $\neq 0$ (si l'un d'eux est 0, leur produit tensoriel est 0), et même que ce sont des G-modules simples.

On a donc $\dim V_i \geqq 1$ pour tout i, d'où $\dim V_i < p$ puisque la somme des $\dim V_i - 1$ est $< p$.

1.4.3 On pourrait supposer (mais nous n'en aurons pas besoin) que $\dim V_i > 1$ pour tout i. En effet, si par exemple $\dim V_1 = 1$, l'hypothèse de récurrence 1.4.1 ci-dessus montre que $V_2 \otimes \ldots \otimes V_m$ est semi-simple. Or le produit tensoriel d'un module semi-simple par un module de dimension 1 est semi-simple (les sous-modules sont les mêmes). Cela montre la semi-simplicité de $V_1 \otimes \ldots \otimes V_m$.

1.5. Extension des scalaires

Soit k' une extension de k.

Proposition 1 *Si le th. 1 est vrai pour G et k', il est vrai pour G et k.*

Soient V_i des G-k-modules satisfaisant aux hypothèses du th. 1, et soit W leur produit tensoriel. Nous devons montrer que W est semi-simple. D'après 1.4.2, on peut supposer que les V_i sont simples et que $\dim V_i < p$ pour tout i.

Par extension des scalaires, les V_i définissent des G-k'-modules V_i'. De même W définit un G-k'-module W', qui est isomorphe au produit tensoriel (sur k') des V_i'.

Lemme 1 *Les V_i' sont des G-k'-modules semi-simples.*

Soit D_i le commutant de l'image de $k[G]$ dans $\mathrm{End}(V_i)$. D'après le lemme de Schur, c'est un corps. Soit Z_i son centre, qui est une extension finie de k. Le module V_i est un Z_i-espace vectoriel, et l'on a:

$$\dim V_i = [Z_i : k] \cdot \dim_{Z_i} V_i .$$

En particulier, on a $[Z_i : k] \leqq \dim V_i < p$, ce qui montre que l'extension Z_i/k est *séparable*. D'après un critère connu (cf. e.g. [4], th. 7.5, p. 145) il en résulte que V_i est absolument semi-simple, donc que V_i' est semi-simple.

On a supposé que le th. 1 est vrai pour G et k'. On déduit de là, et du lemme 1, que $W' = V_1' \otimes \ldots \otimes V_m'$ est semi-simple. Or on sait que, si un module devient semi-simple après extension des scalaires, il est semi-simple. On en déduit donc que W est semi-simple, ce qui démontre la prop. 1.

Ainsi, on peut remplacer k par une clôture algébrique. Cela nous permettra, dans la suite de la démonstration, de supposer que k est *algébriquement clos*.

2 Le cas crucial

A partir de maintenant le corps de base k est supposé algébriquement clos.

Le but de ce § est de démontrer le th. 1 dans le cas particulier suivant: G est le groupe des k-points d'un groupe algébrique $\underline{G}$ quasi-simple; les V_i sont des G-modules simples algébriques (i.e. provenant de représentations algébriques de $\underline{G}$), de type restreint (cf. n° 2.1).

2.1. *Notations*

On note $\underline{G}$ un groupe algébrique semi-simple connexe et simplement connexe. On pose $G=\underline{G}(k)$; on se permet d'identifier G et $\underline{G}$.

Toutes les représentations linéaires de G sont supposées algébriques.

On choisit un tore maximal $\underline{T}$ de $\underline{G}$, ainsi qu'un sous-groupe de Borel $\underline{B}$ contenant $\underline{T}$. On note X le groupe $\mathrm{Hom}(\underline{T}, \mathbf{G}_m)$ des caractères de $\underline{T}$, et R le système de racines correspondant; on a $R \subset X$. Soit $Y = \mathrm{Hom}(X, \mathbf{Z})$ le $\mathbf{Z}$-dual de X; si $\alpha \in R$, on note $\alpha^\vee$ l'élément correspondant de Y («racine duale»); l'ensemble des $\alpha^\vee$ est le système de racines dual $R^\vee$ de R. Le choix du sous-groupe de Borel $\underline{B}$ définit une *base* B de R. Un élément de X est dit positif s'il est combinaison linéaire à coefficients $\geqq 0$ des éléments de B; les racines positives forment une partie R_+ de R.

Soit λ un poids (i.e. un élément de X). On dit que λ est *dominant* si $\langle \lambda, \alpha^\vee \rangle \geqq 0$ pour tout $\alpha \in R_+$ (ou pour tout $\alpha \in B$, cela revient au même). L'ensemble des poids dominants est noté X_+. Un poids dominant λ est dit *restreint* si l'on a $\langle \lambda, \alpha^\vee \rangle < p$ pour tout $\alpha \in B$.

Si λ est un poids dominant, on note $L(\lambda)$ l'unique G-module simple dont le plus haut poids est λ (cf. [6], II.2).

2.2. *La petite alcôve*

A partir de maintenant, et jusqu'à la fin du § 2, on suppose que $\underline{G}$ est *quasi-simple*, i.e. que le système de racines R est *irréductible* (cela revient à dire que le quotient de G par son centre est un groupe simple).

On note $\beta^\vee$ la *plus grande racine de* $R^\vee$, et l'on pose

$$\rho = \tfrac{1}{2} \sum_{\alpha \in R_+} \alpha.$$

On sait ([2], VI, § 1, prop. 29) que ρ est la somme des *poids fondamentaux* ω_α $(\alpha \in B)$ associés à la base B de R.

On dit qu'un poids dominant λ *appartient à la petite alcôve* si l'on a

$$\langle \lambda + \rho, \beta^\vee \rangle \leqq p. \tag{2.2.1}$$

On note C l'ensemble de ces poids.

Remarques. 1) Si $\lambda \in C$, on a $\langle \lambda + \rho, \alpha^\vee \rangle \leqq p$ pour tout $\alpha \in R$. Cela résulte du fait que $\langle \lambda, \alpha^\vee \rangle \leqq \langle \lambda, \beta^\vee \rangle$ puisque $\beta^\vee - \alpha^\vee$ est combinaison linéaire à coefficients $\geqq 0$ d'éléments de $R_+^\vee$. L'ensemble C coïncide donc avec l'ensemble $X_+ \cap \bar{C}_{\mathbf{Z}}$ de [6], p. 247–248.

2) Soit h le nombre de Coxeter de R (ou de $R^\vee$: c'est le même). On a $\langle \rho, \beta^\vee \rangle = h - 1$, cf. [2], VI, § 1, prop. 31. Cela permet de récrire (2.2.1) sous la forme:

$$\langle \lambda, \beta^\vee \rangle \leqq p - h + 1. \tag{2.2.2}$$

3) Tout élément λ de C est un poids dominant *restreint*, au sens du n° 2.1.

En effet, d'après la Remarque 1) ci-dessus, on a $\langle \lambda+\rho, \alpha^\vee \rangle \leqq p$ pour tout $\alpha \in B$. Comme $\langle \rho, \alpha^\vee \rangle = 1$ (cf. [2], VI, § 1, prop. 29), cela entraîne bien $\langle \lambda, \alpha^\vee \rangle < p$.

L'intérêt de la petite alcôve C provient (entre autres) du résultat suivant, dû essentiellement à Verma et Humphreys:

Proposition 2 *Soit V une représentation linéaire de $\underline{G}$, et soit $X(V)$ l'ensemble des poids de $\underline{T}$ dans V. Supposons que $X_+ \cap X(V)$ soit contenu dans C. Alors V est semi-simple.*

Le module V admet une suite de composition dont les quotients sont des modules simples $L(\lambda_i)$, avec $\lambda_i \in X(V) \cap X_+$, donc $\lambda_i \in C$. Tout revient à voir que les extensions successives qui interviennent dans V sont triviales. Avec les notations de [6], I.4.2, on est donc ramené à prouver:

Lemme 2 *Si λ et μ appartiennent à C, on a* $\mathrm{Ext}^1_{\underline{G}}(L(\lambda), L(\mu)) = 0$.

Si $\lambda = \mu$, la nullité de $\mathrm{Ext}^1_{\underline{G}}(L(\lambda), L(\mu))$ est un fait général ([6], II.2.12). Si $\lambda \neq \mu$, λ et μ ne sont pas conjugués par le groupe de Weyl affine W_p ([6], II.6.2.(5)); la nullité de $\mathrm{Ext}^1_{\underline{G}}(L(\lambda)), L(\mu))$ résulte du «linkage principle» ([6], II.6.17).

(*Variante* – Avec les notations de [6], II.5.6, on a $L(\mu) = H^0(\mu)$ et $L(\lambda) = H^0(\lambda) = L(-w_0\lambda)^* = V(\lambda)$. On peut alors récrire $\mathrm{Ext}^1_{\underline{G}}(L(\lambda), L(\mu))$ sous la forme $\mathrm{Ext}^1_{\underline{G}}(V(\lambda), H^0(\mu))$ et l'on applique le fait que ce groupe est 0 quels que soient $\lambda, \mu \in X_+$, cf. [6], II.4.13.)

Remarque. La démonstration montre en outre que V est somme directe de modules du type $H^0(\lambda)$, $\lambda \in C$, donc que V «se relève» en caractéristique 0.

2.3. Modules simples restreints de dimension $\leqq p$

Le résultat suivant est dû à Jantzen ([7], 2.1):

Proposition 3 *Soit λ un poids dominant restreint* (cf. n° 2.1), *et soit $L(\lambda)$ le $\underline{G}$-module simple correspondant. Supposons que* $\dim L(\lambda) \leqq p$. *Alors:*

(i) *On a $\langle \lambda, \alpha^\vee \rangle < p$ pour tout $\alpha \in R_+$.*

(ii) *On a* $\sum_{\alpha \in R_+} \langle \lambda, \alpha^\vee \rangle < \dim L(\lambda)$.

Rappelons la démonstration. On utilise le lemme suivant (où aucune hypothèse sur λ n'est nécessaire):

Lemme 3 *Soit $\alpha \in R_+$ tel que l'entier $n = \langle \lambda, \alpha^\vee \rangle$ soit $< p$. Alors*

$$\lambda, \lambda - \alpha, \ldots, \lambda - n\alpha$$

sont des poids de $L(\lambda)$ (i.e. appartiennent à $X(L(\lambda))$).

Cela résulte facilement des propriétés des représentations du groupe $\mathbf{SL}_2$.

Soit alors R_λ l'ensemble des $\alpha \in R_+$ tels que l'inégalité (i) de la prop. 3 soit vraie. L'hypothèse que λ est restreint montre que R_λ contient la base B de R. D'autre part, si $\alpha \in R_\lambda$, et si $m_\alpha = \langle \lambda, \alpha^\vee \rangle$, le lemme 3 montre que λ,

$\lambda-\alpha, \ldots, \lambda-m_\alpha\alpha$ sont des poids de $L(\lambda)$. Lorsque α varie dans R_λ, le nombre total de ces poids est

$$1+\sum_{\alpha\in R_\lambda} m_\alpha = 1+\sum_{\alpha\in R_\lambda}\langle\lambda,\alpha^\vee\rangle.$$

On en conclut:

$$\sum_{\alpha\in R_\lambda}\langle\lambda,\alpha^\vee\rangle \leqq \dim L(\lambda)-1. \tag{2.3.1}$$

Lemme 4 *L'ensemble* $R_\lambda^\vee$ *est une partie close de* $R^\vee$ (au sens de [2], VI, §1, déf. 4).

Il faut voir que, si $\alpha_1^\vee\in R_\lambda^\vee$, $\alpha_2^\vee\in R_\lambda^\vee$ et $\alpha_1^\vee+\alpha_2^\vee\in R^\vee$, on a $\alpha_1^\vee+\alpha_2^\vee\in R_\lambda^\vee$. Or (2.3.1) montre que

$$\langle\lambda,\alpha_1^\vee\rangle+\langle\lambda,\alpha_2^\vee\rangle\leqq\dim L(\lambda)-1,$$

d'où

$$\langle\lambda,\alpha_1^\vee+\alpha_2^\vee\rangle\leqq\dim L(\lambda)-1<p,$$

ce qui démontre le lemme.

Le lemme 4 montre que $R_\lambda^\vee$ est une partie close de $R^\vee$ contenant la base $B^\vee$. D'après [2], VI, §1, prop. 19, ceci entraîne $R_\lambda^\vee\supset R_+^\vee$, d'où $R_\lambda=R_+$. Cela démontre (i). Quant à (ii), il résulte de (2.3.1) combiné avec l'égalité $R_\lambda=R_+$.

Remarque. La prop. 3 pourrait aussi se déduire du lemme énoncé dans [8], n° 4.6. Malheureusement, la démonstration donnée dans [8] est insuffisante.

2.4. *Une inégalité*

Le résultat suivant n'a rien à voir avec la caractéristique p:

Proposition 5 *Soit* $\lambda\in X_+$, $\lambda\neq 0$. *On a:*

$$\langle\lambda+\rho,\beta^\vee\rangle\leqq 1+\sum_{\alpha\in R_+}\langle\lambda,\alpha^\vee\rangle. \tag{2.4.1}$$

(Rappelons que ρ est la demi-somme des racines >0, et que $\beta^\vee$ est la plus grande racine de $R^\vee$, cf. n° 2.2.)

Observons d'abord que, si l'inégalité (2.4.1) est vraie pour deux poids dominants λ et μ, elle est aussi vraie pour $\lambda+\mu$. On a en effet:

$$\begin{aligned}\langle\lambda+\mu+\rho,\beta^\vee\rangle &= \langle\lambda+\rho,\beta^\vee\rangle+\langle\mu+\rho,\beta^\vee\rangle-\langle\rho,\beta^\vee\rangle\\ &\leqq 2+\sum_{\alpha\in R_+}\langle\lambda,\alpha^\vee\rangle+\sum_{\alpha\in R_+}\langle\mu,\alpha^\vee\rangle-\langle\rho,\beta^\vee\rangle\\ &\leqq 1+\sum_{\alpha\in R_+}\langle\lambda+\mu,\alpha^\vee\rangle+1-\langle\rho,\beta^\vee\rangle\\ &\leqq 1+\sum_{\alpha\in R_+}\langle\lambda+\mu,\alpha^\vee\rangle,\end{aligned}$$

car $\langle\rho,\beta^\vee\rangle=h-1$ est $\geqq 1$.

Il suffit donc de démontrer (2.4.1) lorsque λ est *indécomposable*, autrement dit lorsque λ est le *poids fondamental* ω_γ associé à une racine simple $\gamma \in B$. On a alors $\langle \omega_\gamma, \gamma^\vee \rangle = 1$ et $\langle \omega_\gamma, \alpha^\vee \rangle = 0$ pour $\alpha \in B$, $\alpha \neq \gamma$. Si l'on écrit $\beta^\vee$ sous la forme $\beta^\vee = \sum_{\alpha \in B} q_\alpha \alpha^\vee$, et si l'on pose:

$$2\rho^\vee = \sum_{\alpha \in R_+} \alpha^\vee = \sum_{\alpha \in B} c_\alpha \alpha^\vee,$$

on a $\langle \omega_\gamma, \beta^\vee \rangle = q_\gamma$ et $\sum_{\alpha \in R_+} \langle \omega_\gamma, \alpha^\vee \rangle = \langle \omega_\gamma, 2\rho^\vee \rangle = c_\gamma$. L'inégalité à démontrer s'écrit alors

$$q_\gamma + h - 1 \leqq 1 + c_\gamma.$$

En remplaçant R par $R^\vee$, on voit que l'on est ramené à prouver le résultat suivant:

Proposition 6 *Soit r le rang de R, et soient $\alpha_1, \ldots, \alpha_r$ les éléments de B. Soit $\sum q_i \alpha_i$ la plus grande racine de R, et soit $2\rho = \sum c_i \alpha_i$ la somme des racines >0. On a:*

(2.4.2) $$c_i \geqq q_i + h - 2,$$

où h est le nombre de Coxeter de R.

Cela se vérifie cas par cas, en utilisant les tables de [2], VI, §4, qui donnent les valeurs des c_i, des q_i et de h:
Type A_r $(r \geqq 1)$: $h = r+1$; $c_i = i(r-i+1)$; $q_i = 1$. L'inégalité (2.4.2) est stricte, sauf si $i = 1$ ou r, auquel cas c'est une égalité.
Type B_r $(r \geqq 2)$: $h = 2r$; $c_i = i(2r-i)$; $q_i = 2$ pour $i > 1$ et $q_1 = 1$. L'inégalité (2.4.2) est stricte, sauf si $i = 1$ ou si $r = 2$ et $i = 2$.
Type C_r $(r \geqq 3)$: $h = 2r$; $c_i = i(2r-i+1)$ pour $i < r$ et $c_r = r(r+1)/2$; $q_i = 2$ pour $i < r$ et $q_r = 1$. L'inégalité (2.4.2) est stricte, sauf si $i = 1$.
Type D_r $(r \geqq 4)$: $h = 2r-2$; $c_i = i(2r-i-1)$ si $i \leqq r-2$, et $c_{r-1} = c_r = r(r-1)/2$; $q_i = 1$ pour $i = 1, r-1, r$ et $q_i = 2$ pour $2 \leqq i \leqq r-2$. L'inégalité (2.4.2) est stricte.
Type E_6: $h = 12$; $(c_i) = 16, 22, 30, 42, 30, 16$; $(q_i) = 1, 2, 2, 3, 2, 1$.
Type E_7: $h = 18$; $(c_i) = 34, 49, 66, 96, 75, 52, 27$; $(q_i) = 2, 2, 3, 4, 3, 2, 1$.
Type E_8: $h = 30$; $(c_i) = 92, 136, 182, 270, 220, 168, 114, 58$; $(q_i) = 2, 3, 4, 6, 5, 4, 3, 2$.
Type F_4: $h = 12$; $(c_i) = 16, 30, 42, 22$; $(q_i) = 2, 3, 4, 2$.
Type G_2: $h = 6$; $(c_i) = 10, 6$; $(q_i) = 3, 2$.

Pour chacun des types exceptionnels E_6, E_7, E_8, F_4, G_2, l'inégalité (2.4.2) est stricte, à la seule exception du cas de G_2 où il y a égalité pour $i = 2$.

Note. Les prop. 5 et 6 m'ont été suggérées par des inégalités que Jantzen m'avait signalées en 1986.

Remarque (ajoutée à la correction des épreuves).

G. Lusztig m'a signalé que la prop. 6 peut se démontrer sans utiliser la classification des systèmes de racines:

Si l'on note $c_i(\alpha)$ le coefficient de α_i dans la racine α, il s'agit de montrer que

$$\sum_{\alpha > 0} c_i(\alpha) \geqq h - 2 + c_i(\tilde{\alpha}) \qquad \text{pour tout } i,$$

où $\tilde{\alpha}$ est la plus grande racine de R. Or on sait (cf. J. Tits, Invent Math. **17** (1972), p. 174, lemme A.2) que, pour tout $\alpha \in R_+$, $\alpha \neq \tilde{\alpha}$, il existe $\alpha' \in R_+$ tel que $\alpha' - \alpha \in B$. On déduit de là qu'il existe une suite de racines $\{\gamma_1, \ldots, \gamma_N\}$ «reliant» α_i à $\tilde{\alpha}$, i.e. telles que:

$$\gamma_1 = \alpha_i, \quad \gamma_N = \tilde{\alpha}, \quad \text{et} \quad \gamma_j - \gamma_{j-1} \in B \qquad \text{pour } 1 < j \leqq N.$$

On a $N = h-1$ d'après [2], VI, §1, prop. 31. Les γ_j sont >0, et l'on a $c_i(\gamma_j) \geqq 1$ pour tout j. La somme des $c_i(\gamma_j)$ est donc $\geqq h-2+c_i(\tilde{\alpha})$; il en est *a fortiori* de même de la somme des $c_i(\alpha)$ pour $\alpha \in R_+$.

Une démonstration analogue m'a été communiquée par G. Seligman.

2.5. *Démonstration du th. 1 dans le cas restreint*

Nous allons maintenant démontrer le th. 1 dans le cas particulier où les V_i sont des G-modules simples de type $L(\lambda_i)$, avec λ_i restreint. De façon plus précise:

Proposition 7 *Soient $\lambda_1, \ldots, \lambda_m$ des poids dominants restreints* (cf. n° 2.1) *tels que $\sum(\dim L(\lambda_i) - 1) < p$, et soit W le produit tensoriel des $L(\lambda_i)$. Alors:*

(i) *W est somme directe de modules simples du type $L(\lambda)$, avec λ restreint.*

(ii) *Si l'un des λ_i est $\neq 0$, W est somme directe de modules simples du type $L(\lambda)$, avec $\lambda \in C$* (cf. n° 2.2).

(En particulier, W est semi-simple.)

Le cas où tous les λ_i sont 0 est trivial: le G-module W est isomorphe au G-module unité $L(0)$. Ce cas étant écarté, posons $\mu = \sum \lambda_i$. On a $\mu \in X_+$ et $\mu \neq 0$, d'où:

$$\begin{aligned}
\langle \mu + \rho, \beta^\vee \rangle &\leqq 1 + \sum_{\alpha \in R_+} \langle \mu, \alpha^\vee \rangle && \text{(prop. 5)} \\
&\leqq 1 + \sum_i \sum_{\alpha \in R_+} \langle \lambda_i, \alpha^\vee \rangle \\
&\leqq 1 + \sum_i (\dim L(\lambda_i) - 1) && \text{(prop. 3)} \\
&\leqq p \quad \text{(par hypothèse).}
\end{aligned}$$

Cela montre que le poids dominant μ appartient à la petite alcôve C. Or tous les poids de $W = \bigotimes L(\lambda_i)$ sont de la forme $\lambda = \mu - \sum_{\alpha \in B} n_\alpha \alpha$, avec $n_\alpha \geqq 0$. Comme $\langle \alpha, \beta^\vee \rangle \geqq 0$ pour tout $\alpha \in B$ ([2], VI, §1, prop. 25), on a

$$\langle \lambda + \rho, \beta^\vee \rangle \leqq \langle \mu + \rho, \beta^\vee \rangle \leqq p.$$

Ainsi, les poids de $W = \bigotimes L(\lambda_i)$ qui sont dominants appartiennent à C. Les assertions (i) et (ii) en résultent, grâce à la prop. 2.

3 Le cas où $(G : G^0)$ est premier à p

On rappelle que le corps de base k est algébriquement clos.

3.1. *Enoncé*

Dans ce §, G désigne un groupe algébrique linéaire (lisse), que l'on identifie au groupe $G(k)$ de ses points rationnels. La composante neutre de G est notée

G^0. On se donne des G-modules simples (algébriques) V_i satisfaisant à la condition du th. 1:

$$\sum(\dim V_i - 1) < p.$$

On se propose de démontrer le th. 1 pour ces modules, sous l'hypothèse supplémentaire que $(G : G^0)$ est premier à p. Autrement dit:

Proposition 8 *Supposons que le groupe fini G/G^0 soit d'ordre premier à p. Alors le produit tensoriel des V_i est semi-simple.*

La démonstration se fera en trois étapes:
(i) G est quasi-simple simplement connexe (n° 3.2);
(ii) G est connexe (n° 3.3);
(iii) cas général (n° 3.4).

Remarque. L'hypothèse «G/G^0 est d'ordre premier à p» est très restrictive: elle exclut le cas, *a priori* le plus intéressant, où G est un groupe fini d'ordre divisible par p. C'est pour traiter ce cas que la technique de «saturation» du §4 sera nécessaire.

3.2. Le cas quasi-simple simplement connexe

On suppose G quasi-simple simplement connexe, comme au §2. D'après le *théorème de décomposition de Steinberg* ([6], II.3.17, p. 224) chacun des G-modules simples V_i s'écrit comme produit tensoriel:

$$V_i = V_{i,0}^{[0]} \otimes V_{i,1}^{[1]} \otimes V_{i,2}^{[2]} \otimes \ldots$$

où les $V_{i,n}$ sont des G-modules simples à poids dominant restreint (cf. n° 2.1), et l'exposant $[n]$ représente une *torsion de Frobenius* d'exposant p^n, cf. [6], p. 153 et p. 223.

On déduit de là une décomposition de $W = \bigotimes V_i$ en:

$$W = W_0^{[0]} \otimes W_1^{[1]} \otimes W_2^{[2]} \otimes \ldots,$$

avec $W_n = \bigotimes_i V_{i,n}$. Comme $\dim V_{i,n} \leqq \dim V_i$ pour tout n, on a

$$\sum_i (\dim V_{i,n} - 1) < p,$$

et la prop. 7 du n° 2.5 montre que W_n est somme directe de modules simples de la forme $L(\lambda)$, avec λ restreint. Il résulte de là que W est somme directe de produits tensoriels de la forme:

$$L(\lambda_0)^{[0]} \otimes L(\lambda_1)^{[1]} \otimes \ldots,$$

où les λ_n sont restreints. Or un tel produit tensoriel est un module simple d'après le théorème de Steinberg déjà cité. Il en résulte bien que W est semi-simple.

3.3. Le cas connexe

On suppose G connexe. Soit N le noyau de la représentation linéaire de G fournie par la somme directe des V_i. D'après un résultat connu ([1], lemme 2.2), G/N est réductif. Quitte à remplacer G par G/N, on peut donc supposer que G est *réductif connexe.*

On peut alors écrire G comme un quotient d'un produit direct

$$G' = G_1 \times \ldots \times G_n,$$

où les G_j sont, soit des tores, soit des groupes quasi-simples simplement connexes. Quitte à remplacer G par G', on peut supposer que $G = G'$. Chacun des V_i s'écrit alors comme un produit tensoriel $V_i = \bigotimes_j V_{i,j}$, où les $V_{i,j}$ sont des G_j-modules simples (algébriques, bien sûr). Le produit tensoriel W des V_i s'écrit donc

$$W = \bigotimes_j W_j, \quad \text{où} \quad W_j = \bigotimes_i V_{i,j}.$$

On a $\dim V_{i,j} \leqq \dim V_i$ pour tout j. *Les W_j sont des G_j-modules semi-simples*: lorsque G_j est un tore, c'est évident, et lorsque G_j est quasi-simple simplement connexe, cela résulte de ce qui a été fait au n° 3.2.

On en déduit que W est somme directe de produits tensoriels de la forme $\bigotimes_j E_j$, où E_j est un G_j-module simple; comme un tel produit est un G-module simple, cela montre bien que W est semi-simple.

Variante. La semi-simplicité de W peut aussi se démontrer en utilisant le fait qu'un $(G_1 \times \ldots \times G_n)$-module est semi-simple si et seulement si c'est un G_j-module semi-simple pour tout j, cf. [7], § 3.

3.4. Le cas où $(G : G^0)$ est premier à p

La semi-simplicité de W résulte alors du résultat suivant, appliqué à $H = G$ et $N = G^0$:

Lemme 5 *Soient H un groupe, N un sous-groupe normal de H, et V un H-module.*
(a) *Si V est semi-simple comme H-module, il est semi-simple comme N-module.*
(b) *Si V est semi-simple comme N-module, et si $(H : N)$ est fini et premier à la caractéristique de k, alors V est semi-simple comme H-module.*

Rappelons la démonstration (cf. [7], § 3):

Pour (a), on peut supposer que V est un H-module simple. Soit V' le plus grand sous-N-module de V qui soit N-semi-simple. Du fait que N est normal dans H, V' est stable par H. Comme $V \neq 0$, on a $V' \neq 0$. D'où $V' = V$, ce qui démontre (a).

Pour (b), soit W un sous-H-module de V. Comme V est N-semi-simple, il existe un projecteur q: $V \to W$ qui commute à l'action de N. Soit s l'indice de N dans H, et soient $h_1, \ldots, h_s$ un système de représentants de H/N dans H. Posons

$$\bar{q} = \frac{1}{s} \sum h_i q h_i^{-1} \quad \text{(moyenne des transformés de } q\text{).}$$

On vérifie facilement que $\bar{q}$ commute à l'action de H, et que c'est un projecteur de V sur W. Ainsi, W est facteur direct dans V comme H-module. Cela prouve que V est H-semi-simple.

Ceci achève la démonstration de la prop. 8.

4 Saturation

4.1. Sous-groupe à un paramètre défini par un élément d'ordre p

Soit V un k-espace vectoriel de dimension finie, et soit $s \in \mathbf{GL}(V)$ tel que $s^p = 1$. On a $s = 1 + u$, avec $u^p = 0$. Si $t \in k$, on peut définir un élément s^t de $\mathbf{GL}(V)$ par la formule du binôme tronqué:

$$s^t = \sum_{i<p} \binom{t}{i} u^i = 1 + tu + t(t-1)u^2/2 + \ldots \tag{4.1.1}$$

L'application $t \mapsto s^t$ définit un homomorphisme de groupes algébriques

$$\varphi_s\colon\ \mathbf{G}_a \to \mathbf{GL}_V,$$

où $\mathbf{G}_a$ désigne le groupe additif. Cet homomorphisme possède les deux propriétés suivantes, qui le caractérisent (cf. [8, 9], ainsi que [5], II, §2, n° 2.6):

$$\varphi_s(1) = s. \tag{4.1.2}$$

(4.1.3) *φ_s est de degré $<p$*, i.e. l'application $t \mapsto \varphi_s(t)$ est une application polynomiale de degré $<p$.

Remarques. (1) On sait ([5], *loc. cit.*) que tout homomorphisme $\mathbf{G}_a \to \mathbf{GL}_V$ s'écrit de façon unique comme produit

$$t \mapsto \varphi_{s_0}(t)\, \varphi_{s_1}(t^p)\, \varphi_{s_2}(t^{p^2}) \ldots,$$

où les s_i sont des éléments de $\mathbf{GL}(V)$, commutant entre eux, tels que $s_i^p = 1$ pour tout i, et $s_i = 1$ pour i assez grand.
(2) Une autre façon de décrire les s^t consiste à utiliser *l'exponentielle tronquée* $x \mapsto e(x)$, définie si $x^p = 0$, par:

$$e(x) = \sum_{i<p} x^i/i! = 1 + x + x^2/2 + \ldots + x^{p-1}/(p-1)!\,. \tag{4.1.4}$$

L'élément $s = 1 + u$ s'écrit de façon unique sous la forme $e(x)$, avec

$$x = \sum_{0<i<p} (-1)^{i+1} u^i/i = u - u^2/2 + \ldots - u^{p-1}/(p-1),$$

et l'on a

(4.1.5) $$s^t = e(tx) \quad \text{pour tout} \quad t \in k.$$

Multiplicativité des s^t.

Soient $s_i = 1 + u_i$ $(1 \leqq i \leqq m)$ des éléments de $\mathbf{GL}(V)$, commutant deux à deux, et tels que $s_i^p = 1$ pour tout i. Le produit $s = s_1 \ldots s_m$ est alors tel que $s^p = 1$. On désire comparer s^t au produit des s_i^t:

Proposition 9 *Supposons que l'on ait $\prod u_i^{n_i} = 0$ pour toutes les familles d'entiers $n_i \geqq 0$ telles que $\sum n_i \geqq p$. On a alors:*

(4.1.6) $$s^t = s_1^t \ldots s_m^t \quad \textit{pour tout} \quad t \in k.$$

En effet, il est clair que l'homomorphisme $t \mapsto s_1^t \ldots s_m^t$ satisfait aux conditions (4.1.2) et (4.1.3).

Corollaire. *La formule* (4.1.6) *est valable s'il existe des entiers $v_i \geqq 0$ tels que $\sum (v_i - 1) < p$, et que $u_i^{v_i} = 0$ pour tout i.*

En effet, si les (n_i) sont tels que $\sum n_i \geqq p$, on a $n_i \geqq v_i$ pour au moins un i, et le produit des $u_i^{n_i}$ est 0.

Remarque. Il est essentiel de faire une hypothèse restrictive sur les u_i. En termes d'exponentielles tronquées, cela tient à ce que la formule naïve

(4.1.7?) $$e(x)\, e(y) = e(x+y) \quad \text{si} \quad x^p = 0, \ y^p = 0, \ xy = yx,$$

n'est pas valable en général. La formule correcte est:

(4.1.7) $$e(x)\, e(y) = e(x + y - W_p(x, y)),$$

où W_p est le *polynôme de Witt*, réduction (mod p) de $\dfrac{1}{p}((x+y)^p - x^p - y^p)$. Par exemple:

$$W_2 = xy, \qquad W_3 = xy(x+y), \qquad W_5 = xy(x+y)(x^2 + xy + y^2),$$
$$W_7 = xy(x+y)(x+3y)^2(x+5y)^2.$$

On appliquera ce qui précède à la situation suivante:

L'espace vectoriel V est somme directe de sous-espaces $V_1, \ldots, V_m$. Pour tout i, on se donne $s_i \in \mathbf{GL}(V_i)$ tel que $s_i^p = 1$. Si $W = V_1 \otimes \ldots \otimes V_m$, l'automorphisme

$$s = s_1 \otimes \ldots \otimes s_m$$

de W est tel que $s^p = 1$.

Proposition 10 *Supposons que $\sum (\dim V_i - 1) < p$. On a alors*

(4.1.8) $$s^t = s_1^t \otimes \ldots \otimes s_m^t \quad \textit{pour tout} \quad t \in k.$$

Si $v_i = \dim V_i$, on a $\sum (v_i - 1) < p$, et $(s_i - 1)^{v_i} = 0$ pour tout i (Hamilton-Cayley). On en déduit que

$$(s_1 - 1)^{v_1} \otimes 1 \otimes \ldots \otimes 1 = 0, \ \ldots, \ 1 \otimes 1 \otimes \ldots \otimes (s_m - 1)^{v_m} = 0,$$

et l'on applique le cor. à la prop. 9.

Corollaire. *Tout sous-espace vectoriel de $V_1 \otimes \ldots \otimes V_m$ qui est stable (*resp. *fixé) par $s = s_1 \otimes \ldots \otimes s_m$ est stable (*resp. *fixé) par les $s_1^t \otimes \ldots \otimes s_m^t$.*

En effet, il est clair qu'un tel sous-espace est stable (resp. fixé) par les s^t.

Remarque. Pour $m = 2$, on peut montrer (sans faire d'hypothèses sur les $\dim V_i$) que tout élément de $V_1 \otimes V_2$ fixé par $s_1 \otimes s_2$ est fixé par les $s_1^t \otimes s_2^t$. Ce résultat ne s'étend pas à $m \geqq 3$.

4.2. Sous-groupes saturés de $\mathbf{GL}(V)$

Soit H un sous-groupe de $\mathbf{GL}(V)$. Nous dirons que H est *saturé* si tout élément unipotent s de H possède les deux propriétés suivantes:

(4.2.1) $$s^p = 1.$$

(4.2.2) *On a $s^t \in H$ pour tout $t \in k$.*

Remarque. Lorsque $\dim V \leqq p$, la condition (4.2.1) est automatiquement satisfaite. On déduit de là qu'il existe un plus petit sous-groupe saturé de $\mathbf{GL}(V)$ contenant H; on l'appelle *le saturé de H.*

Exemples. (a) Si $n \leqq p$, le groupe symplectique $\mathbf{Sp}_n$ et le groupe spécial orthogonal $\mathbf{SO}_n$ sont saturés. Il en est de même, plus généralement, de tout groupe défini par des invariants tensoriels de degré 2: cela résulte de la dernière remarque du n° 4.1.
(b) En caractéristique 7, le groupe alterné A_7 a une représentation simple de dimension 5. Son saturé dans cette représentation est le groupe orthogonal $\mathbf{SO}_5$.
(c) En caractéristique 11, le groupe de Janko J_1 a une représentation simple de dimension 7. Le saturé correspondant est le groupe exceptionnel G_2.

Proposition 11 *Soit H un sous-groupe algébrique de $\mathbf{GL}(V)$ et soit H^0 sa composante neutre. Supposons que H soit saturé. Alors $(H : H^0)$ est premier à p.*

On utilise le lemme bien connu suivant:

Lemme 6 *Soit H un groupe algébrique linéaire et soit γ un élément de H/H^0 d'ordre une puissance de p. Il existe alors un élément unipotent de H dont l'image dans H/H^0 est égale à γ.*

Rappelons la démonstration. Soit x un représentant de γ dans H, et décomposons x en $x = s u$, avec s semi-simple, u unipotent, $s u = u s$. En utilisant la structure des groupes de type multiplicatif, on voit qu'il existe un entier N premier à p tel que $s^N \in H^0$; d'autre part, u est d'ordre une puissance de p. Soient $\bar{s}$ et $\bar{u}$ les images de s et u dans H/H^0. On a $\bar{s}\bar{u} = \bar{u}\bar{s} = \gamma$. Comme $\bar{u}$ et γ sont des p-éléments et que $\bar{s}$ est d'ordre premier à p, on a $\bar{s} = 1$, d'où $\bar{u} = \gamma$, cqfd.

Si maintenant $(H : H^0)$ était divisible par p, le groupe fini H/H^0 contiendrait un élément γ d'ordre p. D'après le lemme 6, on pourrait représenter γ par un élément unipotent s de H. Mais, comme H est saturé, s est contenu dans l'image du sous-groupe à un paramètre $t \mapsto s^t$, qui est connexe. On a donc $s \in H^0$, d'où $\gamma = 1$, ce qui contredit le fait que γ est d'ordre p.

4.3. Fin de la démonstration du théorème 1

Nous revenons à la situation du th. 1. Soient donc V_i $(1 \leqq i \leqq m)$ des G-modules simples, avec

$$\sum (\dim V_i - 1) < p. \tag{4.3.1}$$

Comme au n° 4.1, soit $V = V_1 \oplus \ldots \oplus V_m$ la somme directe des V_i, et soit $W = V_1 \otimes \ldots \otimes V_m$ leur produit tensoriel.

Considérons le sous-groupe H de $\mathbf{GL}(V)$ formé des éléments x ayant les deux propriétés (4.3.2) et (4.3.3) ci-après:

(4.3.2) *x laisse stables les V_i.*

Notons x_i la restriction de x à V_i. Le produit tensoriel $x_W = x_1 \otimes \ldots \otimes x_m$ opère sur W. La seconde propriété imposée à x est:

(4.3.3) *x_W laisse stable tout sous-espace vectoriel de W stable par G.*

Le groupe H est un sous-groupe de $\mathbf{GL}(V)$ contenu dans $\mathbf{GL}(V_1) \times \ldots \times \mathbf{GL}(V_m)$ et contenant l'image de G dans $\mathbf{GL}(V)$. Par construction, les sous-espaces vectoriels de W stables par H sont les mêmes que ceux qui sont stables par G.

Proposition 12 *Le groupe H est un sous-groupe algébrique et saturé de* $\mathbf{GL}(V)$.

Que H soit un sous-groupe algébrique de $\mathbf{GL}(V)$ est évident: la condition «laisser stable un sous-espace» est algébrique.

D'autre part, si $s = (s_1, \ldots, s_m)$ est un élément unipotent de H, on a $s_i^p = 1$ pour tout i, puisque $\dim V_i \leqq p$. D'où $s^p = 1$. Il reste à vérifier que les s^t, $t \in k$, appartiennent à H, i.e. satisfont aux conditions (4.3.2) et (4.3.3). C'est immédiat pour (4.3.2): tout sous-espace vectoriel de V stable par s est stable par les s^t. Pour (4.3.3), cela résulte du corollaire à la prop. 10.

Nous pouvons maintenant achever la *démonstration du théorème 1*. Tout d'abord, les V_i sont des H-modules algébriques *simples* (puisqu'ils sont simples comme G-modules). D'après la prop. 12, et le corollaire à la prop. 11, l'indice $(H : H^0)$ est premier à p. On peut donc appliquer à H la prop. 8 du n° 3.1. On en déduit que W est semi-simple comme H-module. Mais les sous-espaces vectoriels de W stables par G sont les mêmes que ceux stables par H. Il en résulte bien que W est semi-simple comme G-module.

Remarques. (1) A la place du groupe H, on aurait pu utiliser le plus petit sous-groupe algébrique saturé de $\mathbf{GL}(V)$ contenant l'image de G.

(2) Dans la démonstration du th. 1 donnée ci-dessus, l'hypothèse sur les $\dim V_i$ est intervenue *deux fois* de façon essentielle: d'abord dans les calculs de poids de la prop. 7 (pour assurer que W ne fait intervenir que la petite alcôve), et ensuite dans la prop. 10, pour la formule $s^t = s_1^t \otimes \ldots \otimes s_m^t$.

Appendice – Semi-simplicité de $\wedge^2 V$

Il s'agit d'améliorer d'une unité la borne donnée dans le cor. 2 au th. 1. Autrement dit:

Théorème 2 *Soit V un G-module semi-simple de dimension $\leqq (p+3)/2$. Alors le G-module $W = \wedge^2 V$ est semi-simple.*

La démonstration est analogue à celle du th. 1. Je me borne à en indiquer les grandes lignes.

Tout d'abord, l'énoncé est évident si $p=2$, car alors $\dim V \leqq 2$. Il est facile si $p=3$ car, si $\dim V=3$, on a $\wedge^2 V \simeq L \otimes V^*$, où V^* est le dual de V et $L = \det(V) = \wedge^3 V$; la semi-simplicité de V entraîne celle de V^*, donc aussi celle de $L \otimes V^*$, puisque $\dim L = 1$. On peut donc supposer $p \geqq 5$, d'où $\dim V < p$. Cela permet, comme au n° 1.4, de supposer que k est algébriquement clos, et que V est un G-module simple. Les arguments des §§2, 3 et 4 se transposent alors de la manière suivante:

– §2 – Ici, on suppose que G est quasi-simple connexe, et que $V = L(\lambda)$, où λ est un poids dominant restreint, que l'on peut supposer $\neq 0$. D'après les prop. 3 et 4, on a:

$$\langle \lambda + \rho, \beta^\vee \rangle \leqq 1 + \sum_{\alpha \in R_+} \langle \lambda, \alpha^\vee \rangle \leqq \dim L(\lambda) \leqq (p+3)/2.$$

Or tous les poids de $\wedge^2 V$ sont de la forme $\mu = 2\lambda - \gamma$, où γ est une combinaison linéaire à coefficients $\geqq 0$, non tous nuls, des éléments de la base B. On a alors:

$$\begin{aligned} \langle \mu + \rho, \beta^\vee \rangle &= 2\langle \lambda + \rho, \beta^\vee \rangle - \langle \rho, \beta^\vee \rangle - \langle \gamma, \beta^\vee \rangle \\ &\leqq p + 3 - (h-1) - \langle \gamma, \beta^\vee \rangle. \end{aligned}$$

On a $h - 1 + \langle \gamma, \beta^\vee \rangle \geqq 3$, car:
ou bien G est de type A_1, et $h=2$, $\langle \gamma, \beta^\vee \rangle \geqq 2$;
ou bien G est de type A_2, et $h=3$, $\langle \gamma, \beta^\vee \rangle \geqq 1$;
ou bien G n'est ni de type A_1 ni de type A_2, et $h \geqq 4$, $\langle \gamma, \beta^\vee \rangle \geqq 0$.

On déduit de là $\langle \mu + \rho, \beta^\vee \rangle \leqq p$. Les poids dominants de W appartiennent donc à la petite alcôve C, et il en résulte que W est semi-simple de type restreint, cf. prop. 2.

– §3 – On suppose que G est algébrique linéaire, avec $(G:G^0)$ premier à p, et que V est un G-module algébrique. Les démonstrations du §3 se transposent sans grand changement. L'une des façons de procéder consiste à remarquer que, si V se décompose en $V = V' \otimes V''$, avec $\dim V' > 1$, $\dim V'' > 1$, alors $\wedge^2 V$ est quotient de $V' \otimes V'' \otimes V' \otimes V''$, qui est semi-simple d'après le th. 1. Cela permet de supposer que V est «indécomposable» (comme produit tensoriel), ce qui facilite beaucoup les arguments.

(Une autre possibilité est d'utiliser les formules:

$$\wedge^2(V' \otimes V'') = \wedge^2 V' \otimes \mathrm{Sym}^2 V'' \oplus \mathrm{Sym}^2 V' \otimes \wedge^2 V''$$

et

$$\mathrm{Sym}^2(V' \otimes V'') = \mathrm{Sym}^2 V' \otimes \mathrm{Sym}^2 V'' \oplus \wedge^2 V' \otimes \wedge^2 V''.)$$

– § 4 – Ici, le point essentiel consiste à prouver que, si $s \in \mathbf{GL}(V)$ est tel que $s^p = 1$, et si $\dim V \leqq (p+3)/2$, on a:

$$(\wedge^2 s)^t = \wedge^2 s^t \quad \text{pour tout} \quad t \in k,$$

ce qui se fait en vérifiant que l'application $t \mapsto \wedge^2 s^t$ est polynomiale de degré $< p$. On introduit ensuite, comme au n° 4.3, le sous-groupe H de $\mathbf{GL}(V)$ formé des éléments x tels que $\wedge^2 x$ laisse stable tout sous-espace vectoriel de $\wedge^2 V$ stable par G. Le groupe H est algébrique saturé; d'après la prop. 11, $(H : H^0)$ est premier à p. En appliquant à H les résultats du § 3, on en déduit que $\wedge^2 V$ est semi-simple comme H-module, donc aussi comme G-module.

Remarques. (1) Pour $p \geqq 5$, la borne $\dim V \leqq (p+3)/2$ est *optimale.* Cela se voit, comme au n° 1.3, en prenant pour G le groupe $\mathbf{SL}_2(k)$ et pour V le G-module $V(d)$, avec $d = (p+3)/2$. On a $\dim V(d) = 1 + (p+3)/2$, et $V(d)$ est simple. D'autre part, on définit un morphisme surjectif

$$\theta\colon \wedge^2 V(d) \to V(p+1)$$

par

$$\theta(f \wedge g) = \mathrm{Jac}(f, g) = \partial f/\partial x \cdot \partial g/\partial y - \partial f/\partial y \cdot \partial g/\partial x.$$

Comme $V(p+1)$ n'est pas semi-simple, $\wedge^2 V(d)$ ne l'est pas non plus.
(2) Pour $p = 2$, la borne $\dim V \leqq 5/2$ du th. 2 *n'est pas optimale.* On peut la remplacer par $\dim V \leqq 3$. En effet, si $\dim V = 3$, on a $\wedge^2 V \simeq L \otimes V^*$ où V^* est le dual de V, et $L = \wedge^3 V$, cf. ci-dessus; la semi-simplicité de V entraîne celle de $L \otimes V^*$. La borne $\dim V \leqq 3$, elle, est optimale. Cela se voit en prenant $G = \mathbf{SL}_2(k)$, avec $|k| \geqq 4$, et $V = V(3)$; le G-module V est simple de dimension 4, et l'on peut vérifier que $\wedge^2 V$ n'est pas semi-simple.
(3) Pour $p = 3$, la borne $\dim V \leqq 3$ du th. 2 *n'est pas optimale.* On peut la remplacer par $\dim V \leqq 4$. Pour le voir, il suffit de traiter le cas où V est un G-module simple de dimension 4, de sorte que $W = \wedge^2 V$ est de dimension 6. Si l'on choisit une base de $\wedge^4 V$, le produit extérieur

$$W \otimes W \to \wedge^4 V$$

définit sur W une *forme bilinéaire symétrique non dégénérée*, qui est quasi-invariante par G (i.e. invariante à un facteur près). (L'application $s \mapsto \wedge^2 s$ définit un isomorphisme de $\mathbf{SL}(V)/\mu_2$ sur $\mathbf{SO}(W)$; cela traduit l'identité des systèmes de racines de types A_3 et D_3.) On vérifie (par exemple en comparant les sous-groupes paraboliques de $\mathbf{SL}(V)$ et de $\mathbf{SO}(W)$) que les sous-espaces totalement isotropes de W stables par G correspondent aux sous-espaces de V stables par G. Comme on a supposé V simple, il n'y a pas de tels sous-espaces (à part 0 et V). On déduit de là que, si H est un sous-espace vectoriel de W stable par G, et H' son orthogonal, on a $H \cap H' = 0$. D'où $W = H \oplus H'$, ce qui montre que H a un supplémentaire stable par G. Donc W est semi-simple.

La borne $\dim V \leqq 4$, elle, est optimale. Cela se voit en prenant $G = \mathbf{SL}_2(k)$ et $V = V(1) \oplus V(2)$, qui est semi-simple de dimension 5. Le G-module $W = \wedge^2 V$ contient alors $V(1) \otimes V(2)$, qui n'est pas semi-simple, cf. n° 1.3.

Question. Peut-on étendre le th. 2 aux autres puissances extérieures? De façon plus précise, soit V un G-module semi-simple de dimension n, et soit m un entier $\geqq 2$. *Est-il vrai que* $\wedge^m V$ *est semi-simple si* $p > m(n-m)$? C'est vrai pour $m = 2$ d'après le th. 2, et aussi si $p > m(n-1)$ d'après le th. 1.

Bibliographie

1. Borel, A., Tits, J.: Groupes réductifs. Publ. Math. I.H.E.S. **27**, 55–150 (1965) (= Borel, A.: Oe. 66)
2. Bourbaki, N.: Groupes et Algèbres de Lie. Chap. 4–5–6, Paris: Masson et CCLS 1981
3. Chevalley, C.: Théorie des groupes de Lie, tome III, Paris: Hermann 1954
4. Curtis, C.W., Reiner, I.: Methods of Representation Theory. Vol. I, New York: John Wiley and Sons 1981
5. Demazure, M., Gabriel, P.: Groupes algébriques. Paris et Amsterdam: Masson et North-Holland 1970
6. Jantzen, J.C.: Representations of Algebraic Groups. Orlando: Academic Press, Pure and Applied Mathematics (vol. 131) 1987
7. Jantzen, J.C.: Low dimensional representations of reductive groups are semisimple. University of Oregon, Eugene 1993
8. Matthews, C.R., Vaserstein, L.N., Weisfeiler, B.: Congruence properties of Zariski-dense subgroups I. Proc. London Math. Soc. **48**, 514–532 (1984)
9. Nori, M.V.: On subgroups of $\mathbf{GL}_n(\mathbf{F}_q)$. Invent. Math. **88**, 257–275 (1987)