Agrégation – Mathématiques générales 1994

Corrigé - Michel Coste

PARTIE I – PRÉLIMINAIRES

1-1 Par récurrence sur n. Pour $n = 1$, si $P \in k[X_1]$ a une infinité de zéros, alors P est le polynôme nul. Supposons $n > 1$, et le résultat montré pour $n - 1$. Soit

$$P = P_0(X_1, \dots, X_{n-1}) + \cdots + P_d(X_1, \dots, X_{n-1})X_n^d.$$

Pour tout $x = (x_1, \dots, x_{n-1}) \in A_1 \times \cdots \times A_{n-1}$, le polynôme $P(x, X_n)$, en une variable X_n, a une infinité de zéros, donc tous les coefficients $P_i(x)$ sont nuls. Puisque les P_i sont nuls sur $A_1 \times \cdots \times A_{n-1}$, par hypothèse de récurrence les P_i sont tous le polynôme nul, et P est le polynôme nul.

1-2 Soit $a = (a_1, \dots, a_n) \in U$. Puisque U est ouvert, il existe $\epsilon > 0$ tel que tout $x = (x_1, \dots, x_n)$ qui vérifie $|x_i - a_i| < \epsilon$ pour $i = 1, \dots, n$ est encore dans U. En posant $A_i = \{x_i;\ |x_i - a_i| < \epsilon\}$, on est ramené à la question 1-1.

1-3

1-3-1 La linéarité de $f \mapsto g \cdot f$ est claire. Si e est l'élément neutre de G, on a $e \cdot f = f$. La seule vérification à écrire est pour $g' \cdot (g \cdot f) = (g'g) \cdot f$. Pour tout $v \in V$,

$$\begin{aligned}\big(g' \cdot (g \cdot f)\big)(v) &= (g \cdot f)(g'^{-1} \cdot v) = f\big(g^{-1} \cdot (g'^{-1} \cdot v)\big) = f\big((g^{-1}g'^{-1}) \cdot v\big) \\ &= f\big((g'g)^{-1} \cdot v\big) = \big((g'g) \cdot f\big)(v).\end{aligned}$$

1-3-2 Si $h \in F(V)^G$, alors $h(g \cdot v) = (g^{-1} \cdot h)(v) = h(v)$ et h est constant sur $\mathcal{O}_v$. Réciproquement, si f est constante sur chaque G-orbite, alors pour tout $v \in V$ et tout $g \in G$ on a $(g \cdot f)(v) = f(g^{-1} \cdot v) = f(v)$ et $f \in F(V)^G$.

1-4

1-4-1 Comme G est engendré par ω, il suffit de vérifier pour $g = \omega$. Par linéarité, il suffit de vérifier pour $P = X^m$ et $Q = X^n$, et alors c'est évident.

1-4-2 Comme G est engendré par ω, on a $k[X]^G = \{P \in k[X];\ \rho(\omega)(P) = P\}$. Si $P = a_0 + a_1X + \cdots + a_dX^d$, on a $\rho(\omega)(P) = a_0 + a_1\omega X + \cdots + a_d\omega^d X^d$, et $P \in k[X]^G$ si et seulement si pour tout i, $a_i = a_i\omega^i$. Comme $\omega^i = 1$ si et seulement si r divise i, on a $P \in k[X]^G$ si et seulement si $a_i = 0$ pour tout i non divisible par r, c.-à-d. si et seulement si $P \in k[X^r]$.

1-5

1-5-1 Soit $g^{-1} = (a_{i,j})$. Alors $g \cdot P$ est la fonction associée au polynôme

$$P(\sum_j a_{1,j}X_j, \dots, \sum_j a_{n,j}X_j).$$

1-5-2 L'orbite de v est $k^n \setminus \{0\}$. D'une part, pour tout $g \in Gl_n(k)$, on a $g \cdot v \neq 0$. D'autrepart, si w est un élément non nul de k^n, il existe $g \in Gl_n(k)$ tel que $g \cdot v = w$: il suffit de compléter en des bases $\epsilon_0 = v, \epsilon_1, \dots, \epsilon_n$ et $\varphi_0 = w, \varphi_1, \dots, \varphi_n$ de k^n et de définir g par $g(\epsilon_i) = \varphi_i$ pour $i = 1, \dots, n$.

1-5-3 Si $P \in k[X_1, \dots, X_n]$ est invariant par $Gl_n(k)$ alors, d'après 1-5-2 et 1-3-2, P est constant sur $k^n \setminus \{0\}$, et vaut disons a. Alors $P - a$ s'annule sur $k^\times \times \dots \times k^\times$, et donc d'après 1-1 $P - a$ est le polynôme nul. Le polynôme P est une constante.

PARTIE II – POLYNÔMES ET ACTION SUR DES ALGÈBRES

2-1

2-1-1 Soient Y_i^0 pour $i = 1, \dots, n$ les formes linéaires coordonnées dans une autre base de V. Il suffit de voir que $Y_i^0 \in k[X_1^0, \dots, X_n^0]$, ceci donnera

$$k[Y_1^0, \dots, Y_n^0] \subset k[X_1^0, \dots, X_n^0],$$

et on aura l'autre inclusion par symétrie. Or on a $Y^0 = M^{-1}X^0$, où M est la matrice de changement de base.

2-1-2 Le morphisme est clairement surjectif, il reste à vérifier que son noyau est nul. Ceci est vrai, parce qu'un polynôme nul sur k^n est le polynôme nul, comme k est infini (voir 1-1).

2-1-3 $S(V)_d$ est caractérisé par

$$f \in S(V)_d \iff f \in S(V) \text{ et } \forall \lambda \in k \ \forall v \in k^n,\ f(\lambda v) = \lambda^d f(v).$$

Cette caractérisation est indépendante du choix de la base.

2-2

2-2-1 Il reste à vérifier que $g \cdot 1 = 1$, ce qui est évident, et que $g \cdot (f_1 \times f_2) = (g \cdot f_1) \times (g \cdot f_2)$, ce qui se calcule ainsi :

$$\begin{aligned}\big(g \cdot (f_1 \times f_2)\big)(v) &= (f_1 \times f_2)(g^{-1} \cdot v) = f_1(g^{-1} \cdot v) \times f_2(g^{-1} \cdot v) \\ &= (g \cdot f_1)(v) \times (g \cdot f_2)(v) = \big((g \cdot f_1) \times (g \cdot f_2)\big)(v).\end{aligned}$$

2-2-2 On utilise la caractérisation de 2-1-3. Soit $f \in S(V)_d$; il vérifie $f(\lambda v) = \lambda^d f(v)$ pour tout $\lambda \in k$ et tout $v \in k^n$. Calculons, pour $g \in G$,

$$(g \cdot f)(\lambda v) = f\big(g^{-1} \cdot (\lambda v)\big) = f\big(\lambda(g^{-1} \cdot v)\big) = \lambda^d f(g^{-1} \cdot v) = \lambda^d (g \cdot f)(v).$$

Ce calcul montre que $g \cdot f$ appartient à $S(V)_d$.

2-2-3 Rappelons que $S(V) = \bigoplus_{d \geq 0} S(V)_d$. Puisque $S(V)^G$ est un sous-espace vectoriel de $S(V)$, l'inclusion

$$S(V)^G \supset \bigoplus_{d \geq 0} \big(S(V)^G \cap S(V)_d\big)$$

est claire. Pour montrer l'inclusion dans l'autre sens, il suffit de voir que si $f \in S(V)^G$ et si $f = f_0 + f_1 + \dots + f_k$ est sa décomposition en polynômes homogènes ($f_d \in S(V)_d$), alors $f_d \in S(V)^G$ pour tout d. D'après 2-2-2, on a $g \cdot f_d \in S(V)_d$ pour tout $g \in G$, et donc

$$g \cdot f = (g \cdot f_0) + \dots + (g \cdot f_k)$$

est la décomposition de $g \cdot f$ en polynômes homogènes. Comme $f = g \cdot f$, on a $f_d = g \cdot f_d$ pour tout d et pour tout $g \in G$.

PARTIE III – EXEMPLES

3 *Groupe spécial linéaire*

3-1 On choisit une base de V. Soit $M(v_1, \ldots, v_r)$ la matrice dont la i-ème colonne est formée des coordonnées de v_i dans cette base. On identifie de cette manière V à $k^{n\times r}$. La famille $(v_1, \ldots, v_r)$ est libre si et seulement si un des déterminants de taille $r \times r$ extraits de $M(v_1, \ldots, v_r)$ est non nul. Un tel déterminant est un polynôme en les coefficients de la matrice, et donc l'endroit où il est différent de zéro est un ouvert de $k^{n\times r}$.

3-2 Etant donné $(v_1, \ldots, v_r)$ et $(w_1, \ldots, w_r)$ dans U_r, on peut compléter en des bases $(v_1, \ldots, v_n)$ et $(w_1, \ldots, w_n)$ de V. Soit $h \in GL(V)$ tel que $h(v_i) = w_i$ pour $i = 1, \ldots, n$. On définit $g \in SL(V)$ par $g(v_i) = w_i$ pour $i < n$ et $g(v_n) = (1/\det h)w_n$; on a bien $\det g = 1$, et $g \cdot (v_1, \ldots, v_r) = (w_1, \ldots, w_r)$. Ceci montre que U_r est contenu dans une orbite de $SL(V)$. Par ailleurs, on a $g \cdot U_r \subset U_r$ pour tout $g \in SL(V)$ (et même $GL(V)$), donc U_r est bien une orbite de $SL(V)$.

Soit $f \in S(V^r)^{SL(V)}$. Alors f est constant et vaut disons $a \in k$ sur U_r puisque U_r est une orbite de $SL(V)$ (1-3-2). Comme $f - a$ est nul sur U_r qui est un ouvert de V^r (3-1), le polynôme $f - a$ est nul (1-2) et donc f est une constante.

3-3

3-3-1 Soit $g \in SL(V)$. On a

$$\det_e\big(g^{-1} \cdot (v_1, \ldots, v_n)\big) = \det(g^{-1}) \times \det_e(v_1, \ldots, v_n) = \det_e(v_1, \ldots, v_n),$$

ce qui veut dire que $g \cdot f = f$. Donc f appartient à $S(V^n)^{SL(V)}$.

3-3-2 Soit $v = (v_1, \ldots, v_n) \in U_n$ (c.-à-d. une base de V). Si $(e_1, \ldots, e_{n-1}, \alpha e_n)$ est dans l'orbite de v sous $SL(V)$, on doit avoir par 3-3-1

$$\det_e(v) = \det_e(e_1, \ldots, e_{n-1}, \alpha e_n) = \alpha,$$

ce qui montre déjà l'unicité, et donne $\alpha = f(v)$. Par ailleurs, l'automorphisme linéaire g défini par $g(v_i) = e_i$ pour $i < n$ et $g(e_n) = f(v)\, e_n$ est bien dans $SL(V)$, ce qui montre que $(e_1, \ldots, e_{n-1}, f(v)\, e_n)$ est dans l'orbite de v sous $SL(V)$.

D'après 3-3-1 on a $k[f] \subset S(V^n)^{SL(V)}$. Soit maintenant $\varphi \in S(V^n)$. Il existe un polynôme P en une variable tel que $\varphi(e_1, \ldots, e_{n-1}, \alpha e_n) = P(\alpha)$. Si φ est invariant par $SL(V)$, il est constant sur les orbites de $SL(V)$ (1-3-2), et on a d'après ce qui précède, pour tout $v = (v_1, \ldots, v_n) \in U_n$,

$$\varphi(v) = \varphi(e_1, \ldots, e_{n-1}, f(v)\, e_n) = P(f(v)).$$

Puisque $\varphi - P(f)$ est nul sur U_n, c'est le polynôme nul (3-1 et 1-2). On a donc $\varphi \in k[f]$, et ceci montre l'égalité $S(V^n)^{SL(V)} = k[f]$.

4 *Quelques groupes finis*

4-1 L'algèbre $k[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ est l'algèbre des polynômes symétriques (c'est en fait la définition des polynômes symétriques). Soient $\varphi_1, \ldots, \varphi_n$ les polynômes symétriques élémentaires : $\varphi_1 = \sum_{i=1}^n X_i$, $\varphi_2 = \sum_{1 \leq i < j \leq n} X_i X_j, \ldots,\ \varphi_n = X_1 X_2 \cdots X_n$. On sait que tout polynôme symétrique peut s'écrire comme polynôme à coefficients dans k en les $\varphi_1, \ldots, \varphi_n$. Ceci veut dire que l'algèbre des polynômes élémentaires est égale à la sous-algèbre $k[\varphi_1, \ldots, \varphi_n]$ de $k[X_1, \ldots, X_n]$. On sait que le morphisme π de l'algèbre de polynômes en n indéterminées $k[S_1, \ldots, S_n]$ dans $k[X_1, \ldots, X_n]$ défini par $\pi(S_i) = \varphi_i$ est injectif. Ceci s'exprime par le fait que si un polynôme P à n indéterminées vérifie $P(\varphi_1, \ldots, \varphi_n) = 0$, alors P est le polynôme nul (on dit aussi que les φ_i sont algébriquement indépendants sur k). Donc π induit un isomorphisme de $k[S_1, \ldots, S_n]$ sur $k[\varphi_1, \ldots, \varphi_n]$. L'algèbre des polynômes symétriques est une algèbre de polynômes.

4-2

4-2-1 Pour $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n$, notons $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ et $|\alpha| = \alpha_1 + \cdots + \alpha_n$. Soit $f = \sum_{\alpha \in \mathbf{N}^n} a_\alpha X^\alpha$ un polynôme (les $a_\alpha \in k$ sont nuls, sauf un nombre fini d'entre eux). Alors $\epsilon \cdot f = \sum_\alpha (-1)^\alpha a_\alpha X^\alpha$, et donc $f = \epsilon \cdot f$ si et seulement si $a_\alpha = 0$ pour tout α tel que $|\alpha|$ est impair (c'est ici que joue l'hypothèse que la caractéristique de k est différente de 2). Il est immédiat que si $|\alpha|$ est pair, alors X^α est produit de monômes X_i^2 ou $X_i X_j$. Ceci montre que

$$k[X_1, \ldots, X_n]^G \subset k[X_1^2, \ldots, X_i X_j, \ldots, X_n^2].$$

L'inclusion dans l'autre sens vient de $\epsilon \cdot X_i^2 = X_i^2$ et $\epsilon \cdot X_i X_j = X_i X_j$.

4-2-2 Tout monôme M du second degré est irréductible dans $k[X_1, \ldots, X_n]^G$. En effet, si $M = PQ$ avec P et Q dans $k[X_1, \ldots, X_n]^G$, alors les degrés totaux de P et Q sont forcément pairs (4-2-1) et donc un de ces deux facteurs doit être une constante (c.-à-d. un élément inversible de $k[X_1, \ldots, X_n]^G$). Supposons maintenant $n \geq 2$. Les trois monômes X_1^2, X_2^2 et $X_1 X_2$ sont irréductibles, et bien sûr aucun n'est multiple d'un autre par une constante. L'égalité

$$(X_1 X_2)^2 = X_1^2 X_2^2$$

est donc un contre-exemple à l'unicité de la décomposition en produit de facteurs irréductibles dans $k[X_1, \ldots, X_n]^G$. Cet anneau n'est pas factoriel.

Une algèbre de polynômes est factorielle. Donc $k[X_1, \ldots, X_n]^G$ ne peut pas être une algèbre de polynômes pour $n \geq 2$. Pour $n = 1$, l'algèbre $k[X_1]^G = k[X_1^2]$ est bien une algèbre de polynômes.

4-2-3 Puisque $V^2 - UW$ est unitaire par rapport à V, on peut faire la division euclidienne de P par rapport à V. Le reste va être de degré au plus 1 en V, et la division s'écrit :

$$P = (V^2 - UW)Q(U, V, W) + R_1(U, W)V + R_0(U, W).$$

Dans cette égalité, quand on fait $U = X^2$, $V = XY$ et $W = Y^2$, on obtient

$$0 = R_1(X^2, Y^2)XY + R_0(X^2, Y^2).$$

Posons $R_1 = \sum_{k,l} r_{k,l} U^k W^l$ et $R_0 = \sum_{k,l} s_{k,l} U^k W^l$. Dans $R_1(X^2, Y^2)XY + R_0(X^2, Y^2)$, le coefficient de $X^{2k}Y^{2l}$ est $s_{k,l}$, et celui de $X^{2k+1}Y^{2l+1}$ est $r_{k,l}$. L'égalité ci-dessus montre donc que R_1 et R_0 sont tous les deux le polynôme nul. Ainsi $V^2 - UW$ divise P.

4-2-4 L'homorphisme de k-algèbres π de $k[U, V, W]$ dans $k[X^2, XY, Y^2]$ défini par $\pi(U) = X^2$, $\pi(V) = XY$, $\pi(W) = Y^2$ est clairement surjectif. La question 4-2-3 montre que son noyau est contenu dans l'idéal $(V^2 - UW)$, et comme $\pi(V^2 - UW) = 0$ ce noyau est égal à l'idéal $(V^2 - UW)$. Donc π induit un isomorphisme de k-algèbres du quotient $k[U, V, W]/(V^2 - UW)$ sur $k[X^2, XY, Y^2]$.

5 et 6 *Groupe orthogonal*

5-1 Si $ae_1 = g(v)$ avec $g \in O(V)$, on a nécessairement $|a| = \|ae_1\| = \|v\|$, donc, comme a est positif, $a = \|v\|$. Il reste à voir qu'il existe bien $g \in O(V)$ tel que $g(v) = \|v\|e_1$. Si $v = 0$, n'importe quel g convient. On suppose donc que $v \neq 0$. Soit $(f_2, \ldots, f_n)$ une base orthonormée de $v^\perp$. La famille $(v/\|v\|, f_2, \ldots, f_n)$ est une base orthonormée de V, et donc l'application linéaire g définie par $g(v) = \|v\|e_1$ et $g(f_i) = e_i$ pour $i = 2, \ldots, n$ est bien dans $O(V)$.

5-2 Puisque tout $g \in O(V)$ préserve le carré de la norme, on a clairement

$$\mathbf{R}[X_1^2 + \ldots + X_n^2] \subset S(V)^{O(V)}.$$

Montrons l'inclusion inverse. Soit $\varphi \in S(V)^{O(V)}$. Alors $\varphi(ae_1)$ est un polynôme en a; ce polynôme en a est invariant par $a \mapsto -a$ puisque $-\mathrm{Id}_V \in O(V)$ et donc $\varphi(-ae_1) = \varphi(ae_1)$. On en déduit qu'il existe un polynôme P d'une variable tel que $\varphi(ae_1) = P(a^2)$ (4-2-1 pour $n = 1$). D'après 5-1 et 1-3-2, on obtient $\varphi(v) = \varphi(\|v\|e_1) = P(\|v\|^2)$ et donc, modulo l'identification entre $S(V)$ et $k[X_1, \ldots, X_n]$, on a $\varphi(X_1, \ldots, X_n) = P(X_1^2 + \cdots + X_n^2)$.

6-1 Soit $g \in O(2)$. On calcule

$$\begin{aligned}(g \cdot L)(x, y) &= L\big(g^{-1} \cdot (x, y)\big) = L\big(g^{-1}(x), g^{-1}(y)\big)\\ &= H\big(g^{-1}(x).g^{-1}(y), g^{-1}(x).g^{-1}(x), g^{-1}(y).g^{-1}(y)\big)\\ &= H(x.y, x.x, y.y) = L(x, y),\end{aligned}$$

ce qui montre que L est $O(2)$-invariant.

6-2 Ecrivons $K = \sum_{\alpha,\beta,\gamma} \kappa_{\alpha,\beta,\gamma} a^\alpha b^\beta c^\gamma$. Puisque F est invariant par $-\mathrm{Id}_V$, K est invariant par la substitution $a \mapsto -a$, $b \mapsto -b$, $c \mapsto -c$. Donc si $\kappa_{\alpha,\beta,\gamma} \neq 0$, on doit avoir $\alpha + \beta + \gamma$ pair (comme en 4-2-1). Par ailleurs F est invariant par la symétrie orthogonale d'axe $\mathbf{R}e_1$ qui envoie (x, y) sur $(x, -y)$. Donc K est invariant par la substitution $c \mapsto -c$, et si $\kappa_{\alpha,\beta,\gamma} \neq 0$, alors γ est pair, et aussi $\alpha + \beta$ est pair d'après la condition précédente. Donc K est un polynôme en a^2, ab, b^2, c^2.

6-3 La question 5-1 montre que tout élément (x, y) a dans son orbite sous $O(V)$ un élément de la forme $(\|x\|e_1, v) = (a, 0, b, c)$. On a $a = \|x\|$, $b^2 + c^2 = y.y$ et $ab = x.y$. On sait d'après 1-3-2 que $F(x,y) = F(a,0,b,c) = K(a,b,c)$, et on sait d'après 6-2 que $K(a,b,c)$ est un polynôme en $a^2 = x.x$, $ab = x.y$, b^2, c^2. Si $x \neq 0$, on peut écrire :

$$\begin{aligned} b^2 &= \frac{(x.y)^2}{x.x}, \\ c^2 &= y.y - \frac{(x.y)^2}{x.x} = \frac{(y.y)(x.x) - (x.y)^2}{x.x}. \end{aligned}$$

Quand on remplace a^2, ab, b^2, c^2 par ces valeurs dans $K(a,b,c)$ et que l'on réduit au même dénominateur qui est une puissance $(x.x)^\alpha$, on obtient :

$$F(x,y) = \frac{M(x.y, x.x, y.y)}{(x.x)^\alpha}$$

où M est un polynôme en trois variables à coefficients réels.

6-4 L'image de $(\mathbf{R}^2 \setminus \{0\}) \times (\mathbf{R}^2 \setminus \{0\})$ par l'application $(x,y) \mapsto (x.y, x.x, y.y)$ est

$$\{(u,v,w) \in \mathbf{R}^3;\ v > 0 \text{ et } w > 0 \text{ et } u^2 \leq vw\}.$$

Il est clair que l'image est contenue dans cet ensemble, et réciproquement tout (u,v,w) de cet ensemble est l'image de

$$\left(\sqrt{v}\, e_1, \frac{u}{\sqrt{v}}\, e_1 + \sqrt{\frac{vw - u^2}{v}}\, e_2\right).$$

L'mage contient donc l'ouvert non vide

$$U = \{(u,v,w) \in \mathbf{R}^3;\ v > 0 \text{ et } w > 0 \text{ et } u^2 < vw\}.$$

Par hypothèse, les polynômes $W^p P(U,V,W)$ et $V^q Q(U,V,W)$ prennent les mêmes valeurs sur U, donc ils sont égaux d'après 1-2.

6-5 D'après 6-1, on a

$$\mathbf{R}[X_1Y_1 + X_2Y_2, X_1^2 + X_2^2, Y_1^2 + Y_2^2] \subset \mathbf{R}[X_1, X_2, Y_1, Y_2]^{O(2)}.$$

Montrons l'inclusion inverse. Soit $F \in \mathbf{R}[X_1, X_2, Y_1, Y_2]^{O(2)}$. On a vu en 6-3 qu'il existe un polynôme $P \in \mathbf{R}[U,V,W]$ et un entier positif ou nul q tels que, si $x \neq 0$,

$$F(x,y) = \frac{P(x.y, x.x, y.y)}{(x.x)^q}.$$

De même, en renversant les rôles de x et de y, il existe un polynôme $Q \in \mathbf{R}[U,V,W]$ et un entier positif ou nul p tels que, si $y \neq 0$,

$$F(x,y) = \frac{Q(x.y, x.x, y.y)}{(y.y)^p}.$$

D'après 6-4, les deux polynômes $W^p P$ et $V^q Q$ sont égaux. Par la factorialité de $\mathbf{R}[U,V,W]$, on obtient que V^q divise P. Donc $F(x,y)$ a mêmes valeurs qu'un polynôme en $x.y, x.x, y.y$ sur l'ouvert des (x,y) tels que $x \neq 0$. Par 1.2, on en déduit que $F(X_1, X_2, Y_1, Y_2)$ appartient à $\mathbf{R}[X_1Y_1 + X_2Y_2, X_1^2 + X_2^2, Y_1^2 + Y_2^2]$.

7 *Conjugaison*

7-1 Les n valeurs propres d'un endomorphisme u sont les racines du polynômes caractéristique P_u de u. Ces n racines sont distinctes si et seulement si le discriminant de P_u est non nul. Comme ce discriminant est un polynôme en les coefficients de la matrice de u dans une base de E, l'ensemble des u pour lesquels il est non nul est bien un ouvert de V.

Soient $\lambda_1, \ldots, \lambda_n$ les n valeurs propres distinctes de u, et soient $e_1, \ldots, e_n$ des vecteurs propres associés. L'orbite de u sous G est formée des endomorphismes v qui ont les mêmes valeurs propres que u. En effet si $v = gug^{-1}$, alors $g(e_i)$ est un vecteur propre de v associé à la valeur propre λ_i. Et réciproquement, si v a pour valeurs propres $\lambda_1, \ldots, \lambda_n$ avec vecteurs propres associés $f_1, \ldots, f_n$, alors l'automorphisme g défini par $g(e_i) = f_i$ vérifie $v = gug^{-1}$.

7-2 Soit $g \in GL(E)$. On a

$$P_{g^{-1}Ag}(T) = \det(T\,\mathrm{Id}_V - g^{-1}Ag) = \det\big(g^{-1}(T\,\mathrm{Id}_V - A)g\big) = P_A(T),$$

et donc $(g \cdot \tau_j)(A) = \tau_j(g^{-1}Ag) = \tau_j(A)$. Ceci montre $\tau_j \in S(V)^{GL(V)}$.

7-3 D'après 7-2 on a l'inclusion $k[\tau_1, \ldots, \tau_n] \subset S(V)^{GL(V)}$. Montrons l'inclusion inverse. Soit $\varphi \in S(V)^{GL(V)}$. Choisissons une base $e = (e_1, \ldots, e_n)$ de V, et notons $D(\lambda_1, \ldots, \lambda_n)$ l'élément de V dont la matrice dans e est

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

Il existe un polynôme P en n variables tel que $\varphi(D(\lambda_1, \ldots, \lambda_n) = P(\lambda_1, \ldots, \lambda_n)$. Puisque φ est invariant sous l'action des automorphismes qui permutent les e_i, ce polynôme doit être invariant par permutation des λ_i. Il s'exprime donc comme polynôme en les polynômes symétriques élémentaires en les λ_i (4-1). Ceci veut dire qu'il existe un polynôme Q en n variables tel que, pour tous $\lambda_1, \ldots, \lambda_n$,

$$\varphi(D(\lambda_1, \ldots, \lambda_n) = Q\Big(\tau_1\big(D(\lambda_1, \ldots, \lambda_n)\big), \ldots, \tau_n\big(D(\lambda_1, \ldots, \lambda_n)\big)\Big).$$

D'après 7-1, chaque u de U a dans son orbite sous $GL(V)$ un endomorphisme $D(\lambda_1, \ldots, \lambda_n)$. Comme φ et les τ_i sont constants sur les orbites (1-3-2), l'égalité ci-dessus montre que les polynômes φ et $Q(\tau_1, \ldots, \tau_n)$ prennent les mêmes valeurs sur U. Donc, d'après 1-2, les polynômes φ et $Q(\tau_1, \ldots, \tau_n)$ sont égaux.

PARTIE IV – LES FORMES BINAIRES

8 *Un exemple*

8-1 On a $\big(\pi_2(g)P\big)(u,v,w) = P\big(\rho_2(g^{-1})(uX^2+vXY+wY^2)\big)$ et comme $\rho(g^{-1})(X) = \alpha X+\beta Y$ et $\rho(g^{-1})(Y)=\gamma X+\delta Y$,

$$\begin{aligned}\rho_2(g^{-1})(uX^2+vXY+wY^2) &= u(\alpha X+\beta Y)^2+v(\alpha X+\beta Y)(\gamma X+\delta Y)+w(\gamma X+\delta Y)^2\\ &= (u\alpha^2+v\alpha\gamma+w\gamma^2)X^2+(2u\alpha\beta+v(\alpha\delta+\beta\gamma)+2w\gamma\delta)XY+(u\beta^2+v\beta\delta+w\delta^2)Y^2.\end{aligned}$$

Donc

$$\big(\pi_2(g)P\big)(u,v,w) = P(u\alpha^2+v\alpha\gamma+w\gamma^2, 2u\alpha\beta+v(\alpha\delta+\beta\gamma)+2w\gamma\delta, u\beta^2+v\beta\delta+w\delta^2).$$

On peut vérifier que $\pi_2(g)\Delta=\Delta$ pour tout $g\in SL_2(k)$ par le calcul.

$$\begin{aligned}&\Delta(u\alpha^2+v\alpha\gamma+w\gamma^2, 2u\alpha\beta+v(\alpha\delta+\beta\gamma)+2w\gamma\delta, u\beta^2+v\beta\delta+w\delta^2) =\\ &\qquad= (2u\alpha\beta+v(\alpha\delta+\beta\gamma)+2w\gamma\delta)^2-4(u\alpha^2+v\alpha\gamma+w\gamma^2)(u\beta^2+v\beta\delta+w\delta^2)\\ &\qquad= v^2\big((\alpha\delta+\beta\gamma)^2-4\alpha\beta\gamma\delta\big)+uw\big(8\alpha\beta\gamma\delta-4(\alpha^2\delta^2+\beta^2\gamma^2)\big)\\ &\qquad= v^2(\alpha\delta-\beta\gamma)^2-4uw(\alpha\delta-\beta\gamma)^2 = v^2-4uw=\Delta(u,v,w).\end{aligned}$$

Ceci montre que $\Delta(u,v,w)$ appartient à $S(R_2)^{SL_2(k)}$.

8-2 On veut

$$\rho_2(g)(uX^2+vXY+wY^2) = X^2-\frac{\Delta(u,v,w)}{4}\,Y^2$$

(et non pas $\pi_2(g)$ comme écrit par erreur dans l'énoncé), c.-à-d.

$$\begin{aligned}uX^2+vXY+wY^2 &= \rho_2(g^{-1})\big(X^2-\frac{\Delta(u,v,x)}{4}\,Y^2\big)\\ &= (\alpha X+\beta Y)^2-\frac{\Delta(u,v,w)}{4}\,(\gamma X+\delta Y)^2.\end{aligned}\qquad (*)$$

Si $u\neq 0$, on peut choisir $t\in k$ avec $t^2=u$ et écrire (en "complétant le carré") :

$$uX^2+vXY+wY^2 = \big(tX+\frac{v}{2t}\,Y\big)^2-\frac{\Delta(u,v,w)}{4u}\,Y^2,$$

et on observe que l'on trouve une solution à l'équation $(*)$ en prenant

$$g=\begin{pmatrix} t & v/2t\\ 0 & 1/t\end{pmatrix}\qquad \text{(remarquer que } \det g = 1).$$

Soit $P\in S(R_2)^{SL_2(k)}$. D'après ce que l'on vient de voir, on doit avoir, pour tout (u,v,w) avec $u\neq 0$,

$$P(u,v,w) = P\big(1,0,\Delta(u,v,w)/4\big),$$

puisque P est constant sur les orbites sous l'action de G par ρ_2. D'après 1-1 les deux polynômes P et $P(1,0,\Delta/4)$ sont égaux et donc $P\in k[\Delta]$. Comme on a vu en 8-1 que $\Delta\in S(R_2)^{SL_2(k)}$, on a bien l'égalité $S(R_2)^{SL_2(k)} = k[\Delta]$.

9 *Cas général*

9-1 On a $\rho_d(g_a)(P) = P(a^{-1}X, aY)$, et dans la base $(X^d, X^{d-1}Y, \dots, Y^d)$ la matrice de $\rho_d(g_a)$ est la matrice diagonale

$$\begin{pmatrix} a^{-d} & & & \\ & a^{-d+2} & & 0 \\ & & \ddots & \\ 0 & & & a^d \end{pmatrix}.$$

Sa trace est

$$a^{-d}(1 + a^2 + \cdots + a^{2d}) = a^{-d}\,\frac{1 - a^{2d+2}}{1 - a^2} = \frac{a^{d+1} - a^{-(d+1)}}{a - a^{-1}}.$$

9-2 On a $R_0 = k$ et $SL_2(k)$ agit trivialement sur R_0, ce qui veut dire que pour tout $g \in SL_2(k)$, $\rho_0(g) = \mathrm{Id}_k$. Donc $(R_0)^{SL_2(k)} = R_0 = k$.

Soit $d > 0$ et $P = a_d X^d + a_{d-1}X^{d-1}Y + \cdots + a_0 y^d \in R_d^{SL_2(k)}$. De $\rho_2(g_2)(P) = P$ on tire $a_\ell = 2^{-d+2\ell}a_\ell$, et donc $a_\ell = 0$ sauf dans le cas où $d = 2k$ est pair, et $\ell = k$. Alors $P = a_k X^k Y^k$, et en prenant

$$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(k)$$

on a $\rho_{2k}(g)(P) = a_k(X - Y)^k Y^k$, qui ne peut être égal à P que si $a_k = 0$. En conclusion, $(R_d)^{SL_2(k)} = \{0\}$.

9-3 On suppose $I = \{1, \dots, n\}$ pour fixer les idées. On choisit une base ϵ_i de H_i pour chaque i, et les bases $\epsilon_1, \dots, \epsilon_n$ mises bout à bout forment une base ϵ de H. Si A_i est la matrice de $\pi_i(h)$ dans la base ϵ_i, alors celle de $\pi(h)$ dans la base ϵ est

$$\begin{pmatrix} A_1 & & & \\ & A_2 & & 0 \\ & & \ddots & \\ 0 & & & A_n \end{pmatrix}.$$

Il est clair alors que la trace de $\pi(h)$, qui est la trace de cette matrice, est égale à la somme sur I des traces des matrices A_i, c.-à-d. des traces des $\pi_i(h)$.

9-4

9-4-1 On a $\theta^{-1} \circ \lambda(g) \circ \theta = \bigoplus_{d \geq 0} \rho_d^{n(d)}(g)$, donc, d'après 9-3 et 9-1,

$$\mathrm{trace}\,(\lambda(g_a)) = \sum_{d \geq 0} n(d)\,\mathrm{trace}\,(\rho_d(g_a)) = \sum_{d \geq 0} n(d)\,\frac{a^{d+1} - a^{-(d+1)}}{a - a^{-1}}.$$

9-4-2 On remarque d'abord qu'un polynôme de Laurent $P \in k[a, a^{-1}]$ qui est nul pour tous les $a \neq 0$ est le polynôme nul. En effet, en multipliant par une puissance convenable

a^D, on voit que $a^D P$ est un polynôme; s'il est nul pour tous les $a \neq 0$, c'est le polynôme nul et donc P aussi est le polynôme nul. Ceci permet d'identifier un polynôme de Laurent à la fonction de $k^\times$ dans k qui lui est associée.

On remarque ensuite que la trace de $\rho_d(g_a)$ est un polynôme de Laurent de degré d, et donc que la famille de ces polynômes, quand d parcourt $\mathbf{N}$, est une famille libre, par un argument de degrés échelonnés. Les $n(d)$, qui sont les coefficients de la combinaison linéaire dans $k[a, a^{-1}]$

$$\operatorname{trace}(\lambda(g_a)) = \sum_{d \geq 0} n(d) \operatorname{trace}(\rho_d(g_a))$$

sont donc entièrement déterminés par la fonction $a \mapsto \operatorname{trace}(\lambda(g_a))$, et donc par λ.

9-4-3 Il est clair, vu le c) de 9-4, que l'isomorphisme θ envoie $\bigoplus_{d \geq 0} \big((R_d)^{SL_2(k)}\big)^{n(d)}$ sur $V^{SL_2(k)}$. Donc

$$\dim_k(V^{SL_2(k)}) = \sum_{d \geq 0} n(d) \dim\big((R_d)^{SL_2(k)}\big).$$

Vu la formule de 9-4-1, pour vérifier que $\dim_k(V^{SL_2(k)})$ est le coefficient de a dans le polynôme de Laurent $(a - a^{-1}) \operatorname{trace}(\lambda(g_a))$, il suffit de vérifier que $\dim\big((R_d)^{SL_2(k)}\big)$ est le coefficient de a dans $a^{d+1} - a^{-(d+1)}$. On trouve bien 1 pour $d = 0$ et 0 pour $d > 0$, conformément au résultat de 9-2.

9-5

9-5-1 On sait que les éléments inversibles de $k[[T]]$ sont les séries formelles dont le terme constant est non nul. Le terme constant du polynôme $\det(\mathbf{1}_n - B^{-1}T)$ est $\det(\mathbf{1}_n) = 1$, donc ce polynôme est inversible dans $k[[T]]$.

9-5-2 Pour abréger, on notera $b_i = b_{i,i}$ les coefficients diagonaux de B. Puisque B est triangulaire supérieure, les coefficients diagonaux de B^{-1} sont les b_i^{-1}. On a donc

$$\det(\mathbf{1}_n - B^{-1}T) = \prod_{i=1}^{n} (1 - b_i^{-1}T),$$

d'où

$$\begin{aligned}\big(\det(\mathbf{1}_n - B^{-1}T)\big)^{-1} &= \prod_{i=1}^{n} (1 - b_i^{-1}T)^{-1} \\ &= \prod_{i=1}^{n} (1 + b_i^{-1}T + b_i^{-2}T^2 + \cdots + b_i^{-k}T^k + \cdots),\end{aligned}$$

et le coefficient de T^e dans cette série est $\sum_{e_1 + \cdots + e_n = e} b_1^{-e_1} \cdots b_n^{-e_n}$. On va comparer avec $tr_e(B)$.

On rapporte $k[X_1, \ldots, X_n]_e$ à la base des monômes $X_1^{e_1} \cdots X_n^{e_n}$, où $e_1 + \cdots + e_n = r$. On a, puisque B, et donc aussi B^{-1}, sont triangulaires supérieures,

$$B \cdot X_1^{e_1} \cdots X_n^{e_n} = \big(b_1^{-1}X_1 + L_1(X_2, \ldots, X_n)\big)^{e_1} \big(b_2^{-1}X_2 + L_2(X_3, \ldots, X_n)\big)^{e_2} \cdots (b_n^{-1}X_n)^{e_n}$$

où $L_2, \dots, L_{n-1}$ sont des formes linéaires. En développant, on voit que le coefficient de $X_1^{e_1} \cdots X_n^{e_n}$ est $b_1^{-e_1} \cdots b_n^{-e_n}$. Donc $tr_e(B)$, qui est la somme des coefficients diagonaux de la matrice de l'action de B, vaut bien $\sum_{e_1+\cdots+e_n=e} b_1^{-e_1} \cdots b_n^{-e_n}$. On a établi

$$\big(\det(\mathbf{1}_n - B^{-1}T)\big)^{-1} = \sum_{e\geq 0} tr_e(B)T^e.$$

9-5-3 Puisque k est algébriquement clos, on peut trouver une matrice de changement de base M telle que la matrice $M^{-1}BM$ soit triangulaire supérieure. Le changement de base dans k^n laisse $\det(\mathbf{1}_n - B^{-1}T)$ invariant, et 2-1 montre que $k[X_1, \dots, X_n]_e$, et $tr_e(B)$, ne dépend pas non plus du choix de la base. L'égalité établie en 9-5-2 vaut donc pour toutes les matrices inversibles B.

9-6 En suivant les définitions précédentes, on a $\chi_{d,e}(a) = \operatorname{trace}(\pi_{d,e}(g_a)) = tr_e(\rho_d(g_a))$. En utilisant la formule de 9-5, et la description de la matrice de $\rho_d(g_a)$ donnée en 9-1, on obtient

$$\begin{aligned}\sum_{e\geq 0} \chi_{d,e}(a)T^e &= \big(\det(\mathbf{1}_n - T\rho_d(g_a)^{-1})\big)^{-1} \\ &= \Big[(1-a^{-d}T)(1-a^{-d+2}T)\cdots(1-a^dT)\Big]^{-1}.\end{aligned}$$

9-7 On raisonne par récurrence sur d. Pour $d = 0$, $F_U(W) = 1 - W$ et donc $\big[F_U(W)\big]^{-1} = \sum_{e\geq 0} W^e$. On a $M_{0,e}(U) = 1$ pour tout $e \geq 0$.

Supposons maintenant $d > 0$, et que l'on connaisse les polynômes $M_{d-1,e}(U) \in \mathbf{Z}[U]$. On a

$$\begin{aligned}\big[F_U(W)\big]^{-1} &= \Big(\sum_{e\geq 0} M_{d-1,e}(U)W^e\Big)(1-U^dW)^{-1} \\ &= \Big(\sum_{e\geq 0} M_{d-1,e}(U)W^e\Big)\Big(\sum_{k\geq 0} U^{dk}W^k\Big),\end{aligned}$$

d'où l'on tire $M_{d,e}(U) = \sum_{k=0}^{e} U^{dk} M_{d-1,e-k}(U) \in \mathbf{Z}[U]$.

9-8 De 9-6 et de 9-7 on obtient

$$\begin{aligned}\sum_{e\geq 0} \chi_{d,e}(a)T^e &= \big[F_{a^2}(a^{-d}T)\big]^{-1} \\ &= \sum_{e\geq 0} M_{d,e}(a^2)\,(a^{-d}T)^e,\end{aligned}$$

d'où il vient $\chi_{d,e}(a) = a^{-de}M_{d,e}(a^2)$.

9-9 On a vu en 9-4 que $m_{d,e} = \dim_k S(R_d)_e^{SL_2(k)}$ est égal au coefficient de a dans le polynôme de Laurent

$$(a - a^{-1})\operatorname{trace}\pi_{d,e}(g_a) = (a-a^{-1})\chi_{d,e}(a).$$

On calcule, grâce à 9-8,

$$\begin{aligned}(a-a^{-1})\chi_{d,e}(a) &= (a-a^{-1})a^{-de}\sum_{i\geq 0} c(d,e,i)a^{2i}\\ &= \sum_{i\geq 0} c(d,e,i)a^{2i+1-de} - \sum_{i\geq 0} c(d,e,i)a^{2i-1-de}\end{aligned}$$

Le coefficent de a dans cette dernière expression est nul si de est impair, et si de est pair il vaut $c(d,e,de/2)-c(d,e,(de/2)+1)$ (c'est bien $+1$ et non -1 comme l'indique l'énoncé).

PARTIE V – GROUPE SYMÉTRIQUE

10 *Polarisation*

10-1 On a

$$\lambda'(t) = \sum_{i=1}^{n} Y_i \frac{\partial f}{\partial U_i}(U_1+tY_1,\ldots,U_n+tY_n),$$

et donc $\lambda'(0) = D_{U,Y}f$. Il est clair que $f\mapsto \lambda'(0)$ est B-linéaire, et si $\mu(t)=g(U+tY)$, on a $(\lambda\mu)'(0)=\lambda(0)\mu'(0)+\mu(0)\lambda'(0)$, ce qui donne $D_{U,Y}(fg) = gD_{U,Y}f + fD_{U,Y}g$. Donc $D_{U,Y}$ est bien une dérivation.

10-2 Soit $F\in B[X_1,\ldots,X_p]$ tel que $f=F(h_1,\ldots,h_p)$. On calcule :

$$\begin{aligned}D_{U,Y}f &= \sum_{i=1}^{n} Y_i\frac{\partial f}{\partial U_i} = \sum_{i=1}^{n} Y_i\Big(\sum_{j=1}^{p}\frac{\partial F}{\partial X_j}(h_1,\ldots,h_p)\,\frac{\partial h_j}{\partial U_i}\Big)\\ &= \sum_{j=1}^{p}\frac{\partial F}{\partial X_j}(h_1,\ldots,h_p)\Big(\sum_{i=1}^{n} Y_i\frac{\partial h_j}{\partial U_i}\Big) = \sum_{j=1}^{p}\frac{\partial F}{\partial X_j}(h_1,\ldots,h_p)\,D_{U,Y}h_j,\end{aligned}$$

et la dernière expression appartient visiblement à $B[h_1,\ldots,h_p,D_{U,Y}h_1,\ldots,D_{U,Y}h_p]$.

10-3 Soit $g\in G$, et soit $(a_{i,j})$ la matrice de $u\mapsto g^{-1}\cdot u$. On a

$$\frac{\partial(g\cdot f)}{\partial U_i} = \sum_{j=1}^{n} a_{j,i}\big(g\cdot\frac{\partial f}{\partial U_j}\big)\,,$$

et on s'en sert pour calculer

$$\begin{aligned}D_{U,Y}(g\cdot f)(u,y) &= \sum_{i=1}^{n} y_i\frac{\partial(g\cdot f)}{U_i}\,(u) = \sum_{i=1}^{n} y_i\Big(\sum_{j=1}^{n} a_{j,i}\,\frac{\partial f}{\partial U_j}(g^{-1}\cdot u)\Big)\\ &= \sum_{j=1}^{n}\Big(\sum_{i=1}^{n} a_{j,i}y_i\Big)\frac{\partial f}{\partial U_j}(g^{-1}\cdot u)\\ &= (D_{U,Y}f)(g^{-1}\cdot u, g^{-1}\cdot y) = (g\cdot D_{U,Y}f)(u,y).\end{aligned}$$

Si $g \cdot f = f$, alors $g \cdot D_{U,Y} f = D_{U,Y}(g \cdot f) = D_{U,Y} f$. Donc si $f \in k[U]^G$, alors $D_{U,Y} f \in k[U,Y]^G$.

10-4

10-4-1 Puisque P est homogène de degré d en les $U^{[1]}$, l'identité d'Euler nous donne

$$dP = \sum_{i=1}^{n} U_i^{[1]} \frac{\partial P}{\partial U_i^{[1]}} = (D_{U^{[1]},U^{[n+1]}} P)(U^{[1]}, \dots, U^{[n]}, U^{[1]}) = Q(U^{[1]}, \dots, U^{[n]}, U^{[1]}).$$

10-4-2 Soit $f \in k[U]_r$. On voit par récurrence sur p que $\widehat{f}_p$ est homogène de degré $r+1-p$ en les $U = U^{[1]}$. Supposons que $\widehat{f}_{p+1} = \lambda\, \widehat{f}_r\big(U^{[\beta_1]}, \dots, U^{[\beta_r]}\big)$. Alors, d'après 10-4-1 et la remarque que l'on vient de faire,

$$(r+1-p)\, \widehat{f}_p = \lambda\, \widehat{f}_{p+1}\big(U^{[1]}, \dots, U^{[p]}, U^{[1]}\big) = \lambda\, \widehat{f}_r\big(U^{[\alpha_1]}, \dots, U^{[\alpha_r]}\big),$$

où $\alpha_i = 1$ si $\beta_i = p+1$ et $\alpha_i = \beta_i$ sinon. Par récurrence descendante, on a en fait

$$\widehat{f}_p = \frac{1}{(r+1-p)!}\, \widehat{f}_r\big(U^{[1]}, \dots, U^{[p]}, U^{[1]}, \dots, U^{[1]}\big).$$

11 *Action diagonale du groupe symétrique*

11-1 Puisque $D_{U,Y}(U_1 \cdots U_r) = \sum_{i=1}^{r} Y_i \left(\prod_{1 \le j \le r,\ j \ne i} U_j \right)$, on se convainc que la polarisation totale de $U_1 \cdots U_r$ est $\sum_\sigma U_1^{[\sigma(1)]} \cdots U_r^{[\sigma(r)]}$, où la somme porte sur toutes les permutations σ de $\{1, \dots, r\}$. Donc la polarisation totale de $\varphi_r = \sum_{1 \le i_1 < \dots < i_r \le n} U_{i_1} \cdots U_{i_r}$ est

$$\widehat{\varphi}_r\big(U^{[1]}, \dots, U^{[r]}\big) = \sum_{1 \le i_1 < \dots < i_r \le n} \sum_\sigma U_{i_1}^{[\sigma(1)]} \cdots U_{i_r}^{[\sigma(r)]} = \sum_{(j_1, \dots, j_r) \in \mathcal{S}} U_{j_1}^{[1]} \cdots U_{j_r}^{[r]},$$

où $\mathcal{S}$ est l'ensemble des suites de r entiers distincts entre 1 et n.

11-2 On remarque d'abord que, par définition de l'action diagonale de $\mathfrak{S}_n$, on a pour $g \in \mathfrak{S}_n$

$$g \cdot \psi_{\underline{\alpha}} = \frac{1}{r!}\, g \cdot \big(\widehat{\varphi}_r(U^{[\alpha_1]}, \dots, U^{[\alpha_r]})\big) = \frac{1}{r!}\, (g \cdot \widehat{\varphi}_r)(U^{[\alpha_1]}, \dots, U^{[\alpha_r]}).$$

Il suffit donc de montrer que $\widehat{\varphi}_r$ est invariant par $\mathfrak{S}_n$. Or, ceci découle du fait que φ_r est invariant par $\mathfrak{S}_n$, et de 10-3.

11-3 On remarque que $D_{U,Y} \sigma_\nu = \sum_{j=1}^{n} \nu Y_j (U_j)^{\nu - 1}$, et on se convainc que

$$\widehat{\sigma}_\nu = \nu! \sum_{j=1}^{n} U_j^{[1]} \cdots U_j^{[\nu]}.$$

Puisque $P_{\underline{a}} = \sum_{i=1}^{n} (U_j^{[1]})^{a_1} \cdots (U_j^{[N]})^{a_N}$, on en déduit que l'on a

$$P_{\underline{a}} = (1/\nu!)\widehat{\sigma}_\nu(U^{[\beta_1]}, \ldots, U^{[\beta_\nu]}),$$

où $\beta_1 = \ldots = \beta_{a_1} = 1$, $\beta_{a_1+1} = \ldots = \beta_{a_2} = 2$, ..., $\beta_{\nu-a_N+1} = \ldots = \beta_\nu = N$.

Puisque σ_ν est un polynôme symétrique, il s'exprime comme polynôme à coefficients dans k en les polynômes symétriques élémentaires $\varphi_1, \ldots, \varphi_n$ (4-1). En utilisant 10-2 et 10-4, on en déduit que $\widehat{\sigma}_\nu$ s'exprime comme polynôme à coefficients dans k en les $\widehat{\varphi}_r(U^{[i_1]}, \ldots, U^{[i_r]})$ avec $1 \leq r \leq n$ et $i_1, \ldots, i_r$ compris entre 1 et ν. D'après la première partie de la question, $P_{\underline{a}}$ s'exprime comme polynôme à coefficients dans k en les $\widehat{\varphi}_r(U^{[\alpha_1]}, \ldots, U^{[\alpha_r]})$ avec $1 \leq r \leq n$ et $\alpha_1, \ldots, \alpha_r$ compris entre 1 et N, et donc aussi en les $\psi_{\underline{\alpha}}$ pour $\underline{\alpha} \in M$.

11-4 Il est clair que $\varphi_1(U) = U_1 + \overline{\varphi}_1(\overline{U})$ et que $\varphi_r(U) = U_1\overline{\varphi}_{r-1}(\overline{U}) + \overline{\varphi}_r(\overline{U})$ pour $1 < r < n$. Les $\overline{\varphi}_r$ s'expriment comme polynômes à coefficients dans k en U_1 et en les φ_r pour $1 \leq r < n$. D'après 10-2 et 10-4, les polarisations totales $\widehat{\overline{\varphi}}_r$ s'expriment comme polynômes à coefficients dans k en les $U_1^{[1]}, \ldots, U_1^{[n-1]}$ et en les $\widehat{\varphi}_r(U^{[\alpha_1]}, \ldots, U^{[\alpha_r]})$ avec $1 \leq r < n$ et $1 \leq \alpha_j < n$. On en déduit que les $\widehat{\overline{\varphi}}_r$ s'expriment comme polynômes à coefficients dans $k[U_1^{[1]}, \ldots, U_1^{[N]}]$ en les $\psi_{\underline{\alpha}}$ pour $\underline{\alpha} \in M$, pourvu que $N \geq n-1$ (cette condition, évidemment nécessaire, ne figure pas dans l'énoncé). Il y a par contre un énoncé valable sans restriction sur N et qui sera utile dans la suite. Posons

$$\overline{M} = \{\underline{\beta} = (\beta_1, \ldots, \beta_r);\ 1 \leq \beta_i \leq N \text{ et } 1 \leq r \leq n-1\},$$

et pour $\underline{\beta} \in \overline{M}$, définissons

$$\overline{\psi}_{\underline{\beta}} = \frac{1}{r!}\widehat{\overline{\varphi}}_r(\overline{U}^{[\beta_1]}, \ldots, \overline{U}^{[\beta_r]}).$$

Alors les $\overline{\psi}_{\underline{\beta}}$ s'expriment comme polynômes en les $\psi_{\underline{\alpha}}$, pour $\underline{\alpha} \in M$, à coefficients dans $k[U_1^{[1]}, \ldots, U_1^{[N]}]$. Ceci découle de ce qu'on a vu pour les $\widehat{\overline{\varphi}}_r$ et les $\widehat{\varphi}_r$.

11-5 Par 11-2, on sait déjà que $k[\psi_{\underline{\alpha}}]_{\underline{\alpha} \in M} \subset A^{\mathfrak{S}_n}$. C'est l'inclusion inverse qui reste à montrer.

Pour $n = 1$, $\mathfrak{S}_1$ est réduit à l'élément neutre et $A^{\mathfrak{S}_1} = A$. Comme $\psi_{\alpha_1} = U_1^{[\alpha_1]}$, on a bien le résultat.

Supposons $n > 1$. On considère $\mathfrak{S}_{n-1}$ comme le groupe des permutations de l'ensemble $\{2, \ldots, n\}$, ou encore comme le sous-groupe de $\mathfrak{S}_n$ laissant fixe 1. On pose

$$\overline{A} = k[\overline{U}^{[1]}, \ldots, \overline{U}^{[N]}]$$

L'hypothèse de récurrence est que

$$\overline{A}^{\mathfrak{S}_{n-1}} = k\left[\overline{\psi}_{\underline{\beta}}\right]_{\underline{\beta} \in \overline{M}},$$

avec les notations introduites à la fin de 11-4. Soit $f \in A^{\mathfrak{S}_n}$, qu'on écrit comme polynôme en $U_1^{[1]}, \dots, U_1^{[N]}$ à coefficients dans $\overline{A}$. Ces coefficients sont invariants par $\mathfrak{S}_{n-1}$, donc d'après l'hypothèse de récurrence ils sont dans $k\left[\overline{\psi}_{\underline{\beta}}\right]$. D'après 11-4 (remarque finale), les $\overline{\psi}_{\underline{\beta}}$ s'expriment comme polynômes en les $\psi_{\underline{\alpha}}$, à coefficients dans $k[U_1^{[1]}, \dots, U_1^{[N]}]$ ou si l'on préfère comme polynômes en les $U_1^{[1]}, \dots, U_1^{[N]}$ à coefficients dans $k[\psi_{\underline{\alpha}}]$. Donc on peut écrire

$$f = \sum_{\underline{a}} C_{\underline{a}} (U_1^{[1]})^{a_1} \cdots (U_1^{[N]})^{a_N} \qquad \text{avec } C_{\underline{a}} \in k[\psi_{\underline{\alpha}}].$$

En prenant pour g la transposition qui échange 1 et j, on a aussi (remarquer que les $C_{\underline{a}}$ sont invariants) :

$$f = g \cdot f = \sum_{\underline{a}} C_{\underline{a}} (U_j^{[1]})^{a_1} \cdots (U_j^{[N]})^{a_N}.$$

En sommant pour tous les j, on obtient

$$f = \frac{1}{n} \sum_{\underline{a}} C_{\underline{a}} P_{\underline{a}},$$

et ceci est bien dans $k[\psi_{\underline{\alpha}}]$ d'après 11-3.

12 *Application*

12-1 Si $J \in k[V]^G$, alors

$$J(u) = (g_j^{-1} \cdot J)(u) = J\big(\pi(g_j)(u)\big) = J(u_j^{[1]}, \dots, u_j^{[n]})$$

et donc

$$\widetilde{J}(u^{[1]}, \dots, u^{[N]}) = \frac{1}{n} \sum_{1 \le j \le n} J(u_j^{[1]}, \dots, u_j^{[n]}) = J(u).$$

12-2 Soit $\tau \in \mathfrak{S}_n$. On a

$$\tau \cdot \widetilde{J} = \frac{1}{n} \sum_{1 \le j \le n} J\big(U_{\tau^{-1}(j)}^{[1]}, \dots, U_{\tau^{-1}(j)}^{[N]}\big) = \frac{1}{n} \sum_{1 \le j \le n} J(U_j^{[1]}, \dots, U_j^{[n]}) = \widetilde{J},$$

donc $\widetilde{J} \in A^{\mathfrak{S}_n}$.

12-3 L'application γ est injective, et quand on ajoute la constante 1 à son image, on trouve une base de l'espace vectoriel des polynômes de degré inférieur ou égal à n en $X_1, \dots, X_N$. Montrons par une récurrence double que la dimension de cet espace vectoriel, que l'on notera $d_{N,n}$ est égale à $\mathbf{C}_{N+n}^n$. Grâce aux remarques ci-dessus, ceci donnera bien que le cardinal de Σ est égal à $\mathbf{C}_{N+n}^n - 1 = \frac{(N+1)\cdots(N+n)}{n!} - 1$.

Pour $n = 0$, il est clair que $d_{N,0} = 1 = \mathbf{C}_N^0$. Supposons $n > 0$, et supposons que l'on ait déjà établi que $d_{N,n-1} = \mathbf{C}_{N+n-1}^{n-1}$ pour tout entier $N \ge 1$. On va montrer que $d_{N,n} = \mathbf{C}_{N+n}^n$ par récurrence sur N.

Pour $N = 1$, on sait bien que $d_{1,n} = n + 1 = \mathbf{C}^n_{1+n}$. Supposons $N > 1$, et supposons que l'on ait déjà établi que $d_{N-1,n} = \mathbf{C}^n_{N-1+n}$. Tout polynôme de degré inférieur ou égal à n en $X_1, \ldots, X_N$ s'écrit de manière unique sous la forme $P = Q + X_N R$, où Q est un polynôme de degré inférieur ou égal à n en $X_1, \ldots, X_{N-1}$, et Q un polynôme de degré inférieur ou égal à $n - 1$ en $X_1, \ldots, X_N$. Cette décomposition en somme directe nous donne la relation suivante entre les dimensions

$$d_{N,n} = d_{N-1,n} + d_{N,n-1} = \mathbf{C}^n_{N-1+n} + \mathbf{C}^{n-1}_{N+n-1} = \mathbf{C}^n_{N+n},$$

ce qu'il fallait démontrer.

12-4 Soit $\theta : A^{\mathfrak{S}_n} \to S(V)$ l'homomorphisme de k-algèbres défini par

$$\theta(f)(u) = f(u_1^{[1]}, \ldots, u_j^{[i]}, \ldots, u_n^{[N]}).$$

L'image de θ est contenue dans $S(V)^G$. En effet, un élément $g \in G$ induit une permutation $\tau \in \mathfrak{S}_n$ par $g_j g^{-1} = g_{\tau(j)}$, et

$$\begin{aligned}(g \cdot \theta(f))(u) &= \theta(f)\big(\pi(g^{-1})(u)\big) = f\big(u_{\tau(1)}^{[1]}, \ldots, u_{\tau(j)}^{[i]}, \ldots, u_{\tau(n)}^{[N]}\big) \\ &= (\tau^{-1} \cdot f)(u_1^{[1]}, \ldots, u_j^{[i]}, \ldots, u_n^{[N]}) = \theta(\tau^{-1} \cdot f)(u) = \theta(f)(u).\end{aligned}$$

On a vu en 12-1 que si $J \in S(V)^G$, alors $\theta(\widetilde{J}) = J$, donc l'image de θ est égale à $S(V)^G$. Comme les $\psi_{\underline{\alpha}}$ pour $\underline{\alpha} \in M$ engendrent $A^{\mathfrak{S}_n}$ (11-5), on en déduit que les images par θ des $\psi_{\underline{\alpha}}$ engendrent $S(V)^G$. Le cardinal de M a été calculé en 12-3. Ceci donne que $S(V)^G$ est engendrée par $\frac{(N+1)\cdots(N+n)}{n!} - 1$ générateurs.