Corrigé de la composition de Mathématiques générales (1994)

Université de Grenoble I, Institut Fourier

Devoir en temps limité du 7 novembre 1997

Étant donné un corps commutatif k infini et un groupe G, on se propose d'étudier les actions linéaires $\rho : G \to \mathrm{GL}(V)$ de G sur un k-espace vectoriel V.
Notations: L'ensemble des invariants de V par l'action de G sera noté V^G. On note $k[X_1, \ldots, X_n]$ l'algèbre des polynômes à n indéterminées sur k, et S_d le sous-espace des polynômes homogènes de degré d.

Partie I. Préliminaires

Soit n un entier non nul.

1-1. Si un polynôme $P \in k[X_1, \ldots, X_n]$ s'annule sur un produit $A_1 \times \cdots \times A_n$ de parties infinies de k, alors $P = 0$. Montrons en effet cette propriété par récurrence sur n. Si $n = 1$, la propriété est vraie, car un polynôme non nul n'admet qu'un nombre fini de racines. Supposons la propriété vraie pour $n-1$ indéterminées et écrivons $P \in k[X_1, \ldots, X_n]$ sous la forme $P = \sum Q_i(X')X_n^i$ où les Q_i sont des polynômes des $n-1$ indéterminées $X' = (X_1, \ldots X_{n-1})$. Pour $a' \in A_1 \times \cdots \times A_{n-1}$ fixé, le polynôme $P(a', X_n) = \sum Q_i(a')X_n^i \in k[X_n]$ s'annule pour tout $X_n = a_n \in A_n$ par conséquent ce polynôme est nul et on a donc $Q_i(a') = 0$ pour tout i et tout $a' \in A_1 \times \cdots \times A_{n-1}$. Par récurrence, on en déduit $Q_i = 0$, d'où $P = 0$.

1-2. Si $k = \mathbb{R}$ ou $\mathbb{C}$, tout ouvert non vide U de k^n contient un produit de parties infinies, à savoir un pavé assez petit $\prod]a_i - \varepsilon, \alpha_i + \varepsilon[$ si $k = \mathbb{R}$ (resp. un polydisque $\prod D(a_i, \varepsilon)$ si $k = \mathbb{C}$). Il résulte donc de I-1 que si la fonction associée au polynôme P est nulle sur U, alors $P = 0$ (comme polynôme formel).

1-3. Soit G un groupe agissant sur un espace vectoriel V, et $F(V)$ l'espace des fonctions $V \to k$ avec l'action
$$G \times F(V) \longrightarrow F(V), \qquad (g, f) \longmapsto g \cdot f, \quad g \cdot f(v) = f(g^{-1} \cdot v).$$

1-3-1. Comme
$$(g_1 g_2) \cdot f(v) = f((g_1 g_2)^{-1} \cdot v) = f(g_2^{-1} g_1^{-1} \cdot v) = (g_2 \cdot f)(g_1^{-1} \cdot v) = (g_1 \cdot (g_2 \cdot f))(v),$$
on a bien $(g_1 g_2) \cdot f = g_1 \cdot (g_2 \cdot f)$, de sorte que ceci est bien une action (à gauche!) du groupe G sur $F(V)$. De plus cette action est clairement linéaire, de sorte que $\rho(g) \in \mathrm{GL}(F(V))$.

1-3-2. Soit $\mathcal{O}_v = G \cdot v$ la G-orbite d'un vecteur $v \in V$. Si $h \in F(V)^G$, alors par définition $g \cdot h = h$, donc $h(g^{-1} \cdot v) = h(v)$ pour tout $g \in G$ ce qui montre que h est constante sur toutes les G-orbites $\mathcal{O}_v = G^{-1} \cdot v$. Inversement, si $f \in F(V)$ est constante sur toutes les G-orbites, il est évident qu'on a bien $f \in F(V)^G$.

1-4. Soit $r > 0$ un entier. On suppose que k est de caractéristique nulle ou non multiple de r. On note $G = \mu_r$ le groupe des racines r-ièmes de l'unité dans k, et on suppose que k contient une racine r-ième primitive ω (ce qui revient à dire que μ_r possède r éléments). On fait agir G sur $k[X]$ par $\rho(\omega)(X^n) = \omega^n X^n$. Ceci entraîne aisément $(g \cdot P)(X) = P(gX)$ pour tout $g \in G$ et $P \in k[X]$. On a bien ainsi une action à gauche de G.

1-4-1. La propriété $\rho(g)(PQ) = \rho(g)(P)\rho(g)(Q)$ est bien claire, car ces deux polynômes coïncident avec $(PQ)(gX) = P(gX)Q(gX)$.

1-4-2. Montrons que $k[X]^G = k[X^r]$. D'une part $\rho(g)(X^{kr}) = g^{kr}X^{kr} = X^{kr}$, de sorte que $k[X^r] \subset k[X]^G$. Inversement si $P(X) = \sum a_i X^i$ est invariant, alors $P(X) = P(gX) = \sum a_i g^i X^i$ donc $a_i = a_i g^i$ pour tout i et tout $g \in G$. Si i est non multiple de r et $g = \omega$, alors $\omega^i \neq 1$, donc $a_i = 0$. Il en résulte que $P \in k[X^r]$, donc $k[X]^G \subset k[X^r]$.

1-5. Soit $G = \mathrm{Gl}_n(k)$ le groupe des matrices inversibles $n \times n$ à coefficients dans k.

1-5-1. Étant donné $P \in k[X_1, \ldots, X_n]$, la fonction associée sera encore notée par abus $P \in F(k^n)$. Pour $g \in P$, la fonction $(g \cdot P)(v) = P(g^{-1} \cdot v)$ est encore un polynôme, car obtenue par substitution à la variable v de $g^{-1} \cdot v$ dont les composantes sont des formes linéaires en v (et donc des polynômes de degré 1). On voit de plus que $\deg(g \cdot P) \leq \deg P$, et l'inégalité inverse est également vraie puisque $P = g^{-1} \cdot (g \cdot P)$, donc $\deg(g \cdot P) = \deg P$.

1-5-2. L'orbite d'un vecteur v non nul dans k^n sous l'action de $G = \mathrm{Gl}_n(k)$ est égale à $k^n \smallsetminus \{0\}$. En effet, comme toute $g \in G$ définit un endomorphisme injectif, on doit avoir $g(v) \neq 0$. Inversement, si $w \in k^n \smallsetminus \{0\}$, on peut trouver des bases $(v_1, \ldots, v_n)$, $(w_1, \ldots, w_n)$ de k^n avec $v_1 = v$, $w_1 = w$, et on obtient ainsi un élement $g \in \mathrm{Gl}_n(k)$ tel que $g(v_i) = w_i$; en particulier $g(v) = w$. Il y a donc exactement deux orbites, à savoir $\{0\}$ et $k^n \smallsetminus \{0\}$.

1-5-3. Les fonctions de $F(k^n)$ invariantes par G sont les fonctions constantes sur chacune des 2 orbites. S'il s'agit d'un polynôme, ce polynôme doit être constant car $k^n \smallsetminus \{0\} \supset (k \smallsetminus \{0\})^n$ et $k \smallsetminus \{0\}$ est par hypothèse une partie infinie. On peut donc appliquer 1-1, ce qui donne $F(k^n)^G = k$.

Partie II. Polynômes et actions sur des algèbres

On considère maintenant des k-algèbres A (qu'on supposera implicitement commutatives et unitaires). Une action ρ d'un groupe G sur une algèbre A sera toujours supposée linéaire et telle que $\rho(g)(a_1 a_2) = \rho(g)(a_1)\rho(g)(a_2)$, i.e. on suppose que $\rho(g)$ est un automorphisme de l'algèbre A pour tout $g \in G$.
Si V est un espace vectoriel de dimension finie et $(e_i)_{1 \leq i \leq n}$ une base de V, on désigne par X_i^0 la forme linéaire i-ième coordonnée ($(X_i^0)_{1 \leq i \leq n}$ est donc par définition la base duale de $(e_i)_{1 \leq i \leq n}$ dans $V^\star$). Enfin, on note $S(V) = k[X_1^0, \ldots, X_n^0] \subset F(V)$ la sous-algèbre engendrée par les X_i^0.

2-1. Quelques vérifications (triviales et pénibles ...)

2-1-1. Il est clair que $\mathrm{GL}(V)$ laisse stable $k[X_1^0, \ldots, X_n^0]$: en effet $g \cdot X_i^0$ n'est autre que la forme linéaire définie par la i-ième ligne de la matrice de g^{-1} dans la base $(e_i)_{1 \leq i \leq n}$, et $g \cdot X_i^0$ est donc une combinaison linéaire de $X_1^0, \ldots, X_n^0$. Changer de base revient à faire agir l'endomorphisme g défini par la matrice de passage du changement de base. On en déduit bien que l'algèbre $S(V)$ est indépendante du choix de la base $(e_i)_{1 \leq i \leq n}$.

2-1-2. Le morphisme d'algèbre qui à X_i associe X_i^0 induit un isomorphisme de l'algèbre $S = k[X_1, \ldots, X_n]$ des polynômes vers l'algèbre $S(V)$. Le fait qu'on ait un morphisme d'algèbres et que ce morphisme soit surjectif sont clairs. L'injectivité résulte de ce qu'un polynôme dont la fonction associée est nulle est formellement nul (cf. 1-2).

2-1-3. Soit $S(V)_d$ l'image de S_d par l'isomorphisme 2-1-2. Or S_d est stable par l'action de $\mathrm{Gl}_n(k)$, du fait que cette action préserve l'homogénéité et le degré des polynômes. On en déduit que $S(V)_d$ ne dépend pas du choix de la base.

2-2. On se place dans la situation de 1-3.

2-2-1. Il est clair que l'action de G sur $F(V)$ définie en 1-3 est en fait une action d'algèbres, puisque $g \cdot (f_1 f_2) = (g \cdot f_1)(g \cdot f_2)$, ces deux fonctions coïncidant avec $v \mapsto f_1 f_2(g^{-1} \cdot v) = f_1(g^{-1} \cdot v) f_2(g^{-1} \cdot v)$.

2-2-2. Pour tout d, $S(V)_d$ est stable pour l'action de $\mathrm{GL}(V)$. Cela résulte du fait que S_d est stable par l'action de $\mathrm{Gl}_n(k)$ et de l'isomorphisme entre S_d et $S(V)_d$. Si on a une action linéaire d'un groupe G sur V définie par un morphisme de groupes $\rho : G \to \mathrm{Gl}(V)$, alors, a fortiori, $S(V)_d$ est également stable par l'action de G.

2-2-3. On a enfin

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

C'est immédiat du fait que $S(V) = \bigoplus_{d \geq 0} S(V)_d$ et que l'action de G préserve chaque composante (en effet $\rho(G) \subset \mathrm{GL}(V)$ et $\mathrm{GL}(V)$ laisse stable chaque composante, cf. 2-1-3): on a $P = \sum P_d = g \cdot P = \sum g \cdot P_d$ si et seulement si $g \cdot P_d = P_d$ pour tout $d \geq 0$.

Partie III. Exemples

3. Cas du groupe spécial linéaire $\mathrm{SL}(V)$

On suppose ici $k = \mathbb{R}$ ou $k = \mathbb{C}$. On rappelle que $\mathrm{SL}(V) \subset \mathrm{GL}(V)$ est le sous-groupe des endomorphismes de déterminant 1. On fait agir $\mathrm{SL}(V)$ diagonalement sur V^r. Enfin, on note $U_r \subset V^r$ l'ensemble formé des r-uples de vecteurs linéairement indépendants. Cet ensemble est stable sous $\mathrm{SL}(V)$ (et même sous $\mathrm{GL}(V)$) car le rang d'un système de vecteurs est préservé par tout isomorphisme linéaire. De plus, on a évidemment $U_r = \emptyset$ pour $r > n$.

3.1. L'ensemble U_r est ouvert. Il suffit de le voir lorsque $r \leq n$. Soit $(e_i)_{1\leq i\leq n}$ une base de V. Alors U_r est la réunion de chacun des ensembles décrits par les conditions que les mineurs de rang r sont non nuls. Or les mineurs sont des fonctions polynômes, donc des fonctions continues des coordonnées des vecteurs $(v_1, \ldots, v_r) \in V^r$.

3.2. Pour $r < n$, U_r forme une seule orbite sous l'action de $\mathrm{SL}(V)$. En effet, étant donnés $(v_1, \ldots, v_r) \in U_r$ et $(w_1, \ldots, w_r) \in U_r$, on peut compléter ces vecteurs en des bases $(v_1, \ldots, v_n)$ et $(w_1, \ldots, w_n)$ de V. Soit g_0 l'application linéaire telle que $g_0(v_i) = w_i$ et $\lambda = \det(g_0) \neq 0$. Alors l'application linéaire g telle que $g(v_i) = w_i$, $1 \leq i < n$ et $g(v_n) = \lambda^{-1} w_n$ est dans $\mathrm{SL}(V)$ et envoie bien $(v_1, \ldots, v_r)$ sur $(w_1, \ldots, w_r)$. Par suite tout élément de $S(V^r)^G$ est constant sur l'ouvert non vide $U_r \subset V^r$, donc $S(V^r)^G = k$ d'après 1-2.

3.3. On va voir que la situation est différente pour $r = n$.

3-3-1. Le polynôme

$$f(v_1, \ldots, v_n) = \det_{(e_i)}(v_1, \ldots, v_n)$$

est invariant sous $\mathrm{SL}(V)$, d'après la formule

$$\det_{(e_i)}(g(v_1), \ldots, g(v_n)) = \det(g) \det_{(e_i)}(v_1, \ldots, v_n).$$

3-3-2. Le raisonnement de 3.2 montre que tout élément de $(v_1, \ldots, v_n) \in U_n$ a dans son orbite un unique élément de la forme $(e_1, \ldots, e_{n-1}, \alpha e_n)$, $\alpha \in k^\star$, donné par $\alpha = \det_{(e_i)}(v_1, \ldots, v_n)$. Si $g \in S(V^n)^G$, on a donc

$$g(v_1, \ldots, v_n) = g(e_1, \ldots, e_{n-1}, \alpha e_n).$$

Le membre de droite est un polynôme en α, qu'on notera $P(\alpha)$. On trouve alors

$$g(v_1, \ldots, v_n) = P\big(\det_{(e_i)}(v_1, \ldots, v_n)\big),$$

par suite $g = P(f) \in k[f]$ et $S(V^n)^G \subset k[f]$. Comme l'autre inclusion est évidente d'après 3-3-1, on en conclut que $S(V^n)^G = k[f]$.

4. Quelques groupes finis

4-1. On fait agir le groupe symétrique $G = \mathfrak{S}_n$ sur $k[X_1, \ldots, X_n]$ en posant $\pi(X_i) = X_{\pi(i)}$ pour tout $\pi \in \mathfrak{S}_n$. Par définition, l'algèbre $k[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ est constituée des polynômes symétriques en $X_1, \ldots, X_n$. On sait que cette algèbre est engendrée par les polynômes symétriques élémentaires

$$\sigma_1 = X_1 + \cdots + X_n,\ \ldots\ ,\ \sigma_2 = \sum_{i<j} X_i X_j,\ \ldots\ ,\ \sigma_p = \sum_{i_1 < \ldots < i_p} X_{i_1} \ldots X_{i_p},\ \ldots\ ,\ \sigma_n = X_1 X_2 \ldots X_n.$$

Comme les polynômes symétriques élémentaires sont par ailleurs algébriquement indépendants, il vient $k[X_1, \ldots, X_n]^{\mathfrak{S}_n} = k[\sigma_1, \ldots, \sigma_n]$ et l'algèbre des invariants est bien une algèbre de polynômes (en les indéterminées $\sigma_1, \ldots, \sigma_n$).

4-2. Soit $G = \{1, \varepsilon\} \simeq \mathbb{Z}/2\mathbb{Z}$ où $\varepsilon^2 = 1$. On suppose que la caractéristique de k est différente de 2 et on fait agir G sur $k[X_1, \ldots, X_n]$ en posant $\varepsilon \cdot X_j = -X_j$. L'action de G est donnée par $\varepsilon \cdot P(X) = P(-X)$.

4-2-1. L'algèbre des invariants de G consiste clairement en les polynômes *pairs*, c'est-à-dire les polynômes dont tous les monômes sont de degré total pair. On peut alors regrouper les indéterminées par paires, ce qui montre que

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

4-2-2. Pour $n \geq 2$, $k[X_1, \ldots, X_n]^G$ n'est pas un anneau factoriel, en effet on a par exemple

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

tandis que les éléments X_1^2, X_2^2, $X_1 X_2$ sont tous irréductibles dans $k[X_1, \ldots, X_n]^G$ (puisque ces éléménts sont de degré pair minimal). En particulier, pour $n \geq 2$, $k[X_1, \ldots, X_n]^G$ n'est pas isomorphe à une algèbre de polynômes (puisque les algèbres de polynômes constituent des anneaux factoriels).

4-2-3. Soit $P \in k[U, V, W]$ tel que $P(X^2, XY, Y^2)$ soit nul dans $k[X, Y]$. Effectuons la division euclidienne de P par $V^2 - UW$, vu comme polynôme unitaire en V sur l'anneau $k[U, W]$. On trouve alors

$$P = (V^2 - UW)Q + R$$

où $Q, R \in k[U,V,W]$ et R est de degré partiel ≤ 1 en V, de sorte que $R = R_1(U,W)V + R_0(U,W)$. Par la substitution $U = X^2$, $V = XY$, $W = Y^2$ il vient

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

Si $P(X^2, XY, Y^2)$ est nul, alors nécessairement $R_1(X^2, Y^2)XY = 0$ et $R_0(X^2, Y^2) = 0$, puisque le premier termes contient des monômes de degrés partiels impairs en X, Y, tandis que $R_0(X^2, Y^2)$ ne contient que des monômes de degrés partiels pairs. On a donc $R_1(X^2, Y^2) = R_0(X^2, Y^2) = 0$, d'où $R_1 = R_2 = 0$, d'où enfin $R = 0$, ce qui implique $P = (V^2 - UW)Q$.

4-2-3. On a par définition un homomorphisme surjectif

$$k[U,V,W] \longrightarrow k[X^2, XY, Y^2], \qquad U \mapsto X^2, \quad V \mapsto XY, \quad W \mapsto Y^2,$$

et la question 4-2-2 montre que le noyau de cet homomorphisme coïncide avec l'idéal $(V^2 - UW)$ dans l'anneau $k[U,V,W]$. Par passage au quotient, on trouve un isomorphisme

$$k[U,V,W]/(V^2 - UW) \xrightarrow{\simeq} k[X^2, XY, Y^2].$$

5 et 6. Groupe Orthogonal (sur le corps des réels)

5. Soit V un espace vectoriel réel de dimension finie n, muni d'un produit scalaire, et $O(V)$ le groupe orthogonal correspondant. Il agit naturellement sur V et sur $S(V)$. On utilise ici une identification entre $S(V)$ et $k[X_1, \dots, X_n]$ réalisée au moyen d'une *base orthonormée* $(e_1, \dots, e_n)$.

5-1. Tout élément $v \in V$ a pour orbite sous $O(V)$ la sphère de rayon $\|v\|$. Cette orbite contient un unique élément ae_1, $a \in \mathbb{R}_+$, à savoir $\|v\|\, e_1$.

5-2. Il est clair que le polynôme $X_1^2 + \cdots + X_n^2$ est invariant par le groupe orthogonal, et on a donc $\mathbb{R}[X_1^2 + \cdots + X_n^2] \subset S(V)^{O(V)}$. Inversement, si $P \in S(V)^{O(V)}$ est un polynôme invariant, alors

$$P(v) = P(\|v\|\, e_1).$$

Le polynôme $P(Xe_1) \in \mathbb{R}[X]$ est pair, donc s'écrit $P(Xe_1) = Q(X^2)$ pour un certain polynôme $Q \in \mathbb{R}[X]$. On en déduit

$$P(v) = P(\|v\|\, e_1) = Q(\|v\|^2) = Q(X_1^2 + \cdots + X_n^2),$$

par suite $S(V)^{O(V)} = \mathbb{R}[X_1^2 + \cdots + X_n^2]$.

6. On munit $E = \mathbb{R}^2$ du produit scalaire usuel, et on fait agir $G = O(2)$ sur $V = E^2 = \mathbb{R}^4$ de manière diagonale. Soit $F(x_1, x_2, y_1, y_2) = F(x, y)$, $x = (x_1, x_2) \in E$, $y = (y_1, y_2) \in E$, une fonction polynôme sur V qui soit G-invariante.

6-1. Soit $H \in \mathbb{R}[X_1, X_2, X_3]$ et $L \in \mathbb{R}[X_1, X_2, Y_1, Y_2]$ tel que

$$L(x, y) = H(x \cdot y, x \cdot x, y \cdot y) = H(x_1y_1 + x_2y_2, x_1^2 + x_2^2, y_1^2 + y_2^2).$$

Comme les polynômes $x \cdot y, x \cdot x, y \cdot y$ sont $O(2)$-invariants par l'action diagonale de $O(2)$ sur E^2, il en est de même pour L.

6-2. On pose, pour tout $(a, b, c) \in \mathbb{R}^3$, $K(a, b, c) = F(a, 0, b, c)$. L'invariance de F sous l'action diagonale de $-\mathrm{Id} \in O(2)$ implique que $K(-a, -b, -c) = K(a, b, c)$, et l'invariance de F sous l'action de la symétrie orthogonale d'axe $\mathbb{R}e_1$ implique $K(a, b, -c) = K(a, b, c)$. Il en resulte que K ne contient que des monômes de degré total pair, et de degré partiel pair en c. On voit alors facilement que K est engendré par a^2, b^2, c^2, ab.

6-3. Tout élément (x, y) de V a dans son orbite sous G un élément (u, v) tel que $u = ae_1$, $a \in \mathbb{R}_+$. En effet il suffit de prendre $a = \|x\|$ et un élément $g \in O(2)$ qui envoie x sur u. Par conséquent

$$F(x, y) = F(u, v) = K(a, v_1, v_2) \qquad \text{où } K(a, b, c) = F(a, 0, b, c).$$

On a de plus $a = \|x\|$,

$$v_1 = \frac{1}{a} u \cdot v = \frac{x \cdot y}{\|x\|}, \qquad v_2^2 = \|v\|^2 - v_1^2 = y \cdot y - \frac{(x \cdot y)^2}{x \cdot x}.$$

Par ailleurs, il existe d'après 6-2 un polynôme de 4 indéterminées tel que

$$F(a, v_1, v_2) = P(a^2, v_1^2, v_2^2, av_1) = P\Big(x \cdot x, \frac{(x \cdot y)^2}{x \cdot x}, y \cdot y - \frac{(x \cdot y)^2}{x \cdot x}, x \cdot y\Big).$$

En passant une puissance assez grande de $x \cdot x$ au dénominateur, on voit qu'il existe un entier $\alpha \in \mathbb{N}$ et un polynôme $M \in \mathbb{R}[U, V, W]$ tel que

$$F(x, y) = \frac{M(x \cdot y, x \cdot x, y \cdot y)}{(x \cdot x)^\alpha}, \qquad x \neq 0.$$

6-4. On suppose que les polynômes $P, Q \in \mathbb{R}[U, V, W]$ vérifient

$$(y \cdot y)^p P(x \cdot y, x \cdot x, y \cdot y) = (x \cdot x)^q Q(x \cdot y, x \cdot x, y \cdot y)$$

pour tous $x, y \in E \smallsetminus \{0\}$, p et q étant des entiers positifs ou nuls. Or étant donnés trois réels a, b, c vérifiant les conditions $b > 0$,$c > 0$ $a^2 < bc$, on peut trouver des vecteurs (forcément non nuls) $x, y \in E$ tels que $a = x \cdot y$, $b = x \cdot x$, $c = y \cdot y$ (il suffit de, prendre des vecteurs de normes adéquates, formant un angle θ tel que $\cos\theta = a/\sqrt{bc}$). On en déduit que le polynôme $c^p P(a, b, c) - b^q Q(a, b, c)$ s'annule sur l'ouvert non vide $\{(a, b, c)\ ;\ b > 0,\ c > 0, a^2 < bc\} \subset \mathbb{R}^3$. D'après 1-2 ce polynôme est nul, d'où $W^q P(U, V, W) = V^q Q(U, V, W)$.

6-5. En échangeant les rôles de x et y dans 6-3, on voit qu'on peut écrire

$$F(x, y) = \frac{P(x \cdot y, x \cdot x, y \cdot y)}{(x \cdot x)^\alpha} = \frac{Q(x \cdot y, x \cdot x, y \cdot y)}{(y \cdot y)^\beta}$$

pour tous $x \neq 0$, $y \neq 0$. La question 6-4 montre alors qu'on a l'identité formelle $W^\beta P(U, V, W) = V^\alpha Q(U, V, W)$. Comme l'anneau $\mathbb{R}[U, V, W]$ est factoriel et que les éléments V, W sont premiers entre eux, on conclut que V^α divise P, i.e. $P(U, V, W) = V^\alpha R(U, V, W)$ pour un certain polynôme R. Il vient donc $F(x, y) = R(x \cdot y, x \cdot x, y \cdot y)$. Cette conclusion, jointe à l'observation 6-1, entraîne que

$$S(E^2)^G = \mathbb{R}[X_1, X_2, Y_1, Y_2]^G = \mathbb{R}[X_1Y_1 + X_2Y_2, X_1^2 + X_2^2, Y_1^2 + Y_2^2].$$

7. Conjugaison

Soit E un $\mathbb{C}$-espace vectoriel de dimension finie n. On fait agir $G = \mathrm{GL}(E)$ sur $V = \mathrm{End}_{\mathbb{C}}(E)$ par conjugaison: $g \cdot a = gag^{-1}$.

7-1. L'ensemble U des éléments de V dont les n-valeurs propres sont distinctes est constitué des endomorphismes a tel que $\Delta(P_a) \neq 0$, où P_a est le polynôme caractéristique de a et $\Delta(P_a)$ son discriminant. Or $\Delta(P_a)$ est un polynôme en les coefficients (a_{jk}) de a. Par suite, l'ensemble $U = \{a; \Delta(P_a) \neq 0\}$ est ouvert (on peut noter de plus que cet ouvert est non vide, puisque, une base étant fixée, on peut prendre les endomorphismes dont la matrice est diagonale à coefficients diagonaux distincts). Si $u \in U$, l'orbite de u est constituée des endomorphismes v ayant le même ensemble $\{\lambda_1, \ldots, \lambda_n\}$ de valeurs propres que u. En effet, si $(e_1, \ldots, e_n)$ est une base de vecteurs propres pour u, alors $v = gug^{-1}$ admet $(g(e_1), \ldots, g(e_n))$ comme base de vecteurs propres avec les mêmes valeurs propres; inversement, si v admet $(\varepsilon_1, \ldots, \varepsilon_n)$ comme base de vecteurs propres avec valeurs propres $(\lambda_1, \ldots, \lambda_n)$, on a $v = gug^{-1}$ où g est l'endomorphisme tel que $g(e_j) = \varepsilon_j$.

7-2. Soit $a \in V$ et

$$P_a(T) = \det(T \cdot \mathrm{Id} - a) = T^n - \tau_1(a)T^{n-1} + \cdots + (-1)^{n-1}\tau_{n-1}(a)T + (-1)^n \tau_n(a)T \in k[T]$$

son polynôme caractéristique. Comme

$$P_{g \cdot a}(T) = P_{gag^{-1}}(T) = \det\big(g(T \cdot \mathrm{Id} - a)g^{-1}\big) = \det(T \cdot \mathrm{Id} - a) = P_a,$$

on voit que $\tau_j(g \cdot a) = \tau_j(a)$ pour tout $j = 1, \ldots, n$, i.e. $\tau_j \in S(V)^G$.

7-3. Soit $P \in S(V)^G$. Si $\tau = (\tau_1, \ldots, \tau_n) \in k^n$, on note $a_\tau \in V$ l'endomorphisme de matrice diagonale $(\tau_j \delta_{jk})$ dans une base fixée une fois pour toutes $(e_1, \ldots, e_n)$, et on définit un polynôme $Q \in k[\tau_1, \ldots, \tau_n]$ par

$$Q(\tau_1, \ldots, \tau_n) = P(a_\tau).$$

L'invariance de P sous G et le fait que tout endomorphisme diagonalisable soit conjugué à a_τ avec $\tau = (\tau_j(a))$ implique $P(a) = P(a_\tau) = Q(\tau_j(a))$. Cette égalité entre polynômes est vraie en particulier sur l'ouvert non vide $U \subset V$. D'après 1-2, cette égalité a lieu en fait sur V tout entier. On en déduit un isomorphisme

$$S(V)^G \xrightarrow{\simeq} k[\tau_1, \ldots, \tau_n], \qquad P \longmapsto Q.$$

Partie IV. Les formes binaires

Dans cette partie, $G = \mathrm{SL}_2(k)$ où G est un corps algébriquement clos de caractéristique nulle. Le groupe G agit naturellement sur k^2 et on obtient grâce à 1-3 et 2-2 une action ρ sur l'algèbre $k[X, Y]$ telle que

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(k), \quad \rho(g)(X) = X \circ g^{-1} = \delta X - \beta Y, \quad \rho(g)(Y) = Y \circ g^{-1} = -\gamma X + \alpha Y.$$

On note ρ_d l'action induite par G dans l'espace $R_d = k[X, Y]_d$ des polynômes homogènes de degré d, et π_d l'action induite par ρ_d sur $S(R_d)$.

8. Un exemple ($d = 2$)

On suppose ici que $d = 2$ et que k est algébriquement clos de caractéristique nulle. Tout élément de R_2 s'écrit $uX^2 + vXY + wY^2$, d'où une identification de $S(R_2)$ et de $k[u, v, w]$.

8-1. Si $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(k)$ et $Q(X, Y, Z) = uX^2 + vXY + wY^2 \in R_2$, alors

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

En remplaçant g par g^{-1} il vient

$$\rho_2(g^{-1})Q(X, Y, Z) = (\alpha^2 u + \alpha\gamma v + \gamma^2 w)X^2 + (2\alpha\beta u + (\alpha\delta + \beta\gamma)v + 2\gamma\delta w)XY + (\beta^2 u + \beta\delta v + \delta^2 w)Y^2.$$

Les coefficients (u, v, w) de Q deviennent $\big(\alpha^2 u + \alpha\gamma v + \gamma^2 w, 2\alpha\beta u + (\alpha\delta + \beta\gamma)v + 2\gamma\delta w, \beta^2 u + \beta\delta v + \delta^2 w\big)$ sous l'action de g^{-1} par ρ_2. Par définition, l'action induite π_2 sur $S(R_2)$ est donc telle que

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

Il en résulte facilement que le discriminant $\Delta(u, v, w) = v^2 - 4uw$ appartient à $S(R_2)^G$. En effet, un calcul montre que

$$\big(2\alpha\beta u + (\alpha\delta + \beta\gamma)v + 2\gamma\delta w\big)^2 - 4\big(\alpha^2 u + \alpha\gamma v + \gamma^2 w\big)\big(\beta^2 u + \beta\delta v + \delta^2 w\big) = (\alpha\delta - \beta\gamma)^2(v^2 - 4uw),$$

et on a ici $\alpha\delta - \beta\gamma = 1$.

8-2. Pour tout choix de $(u, v, w) \in k^3$ tel que $u \neq 0$, la réduction d'un trinôme du second degré donne

$$uX^2 + vXY + wY^2 = u\Big(X^2 + \frac{v}{u}XY + \frac{w}{u}Y^2\Big) = u\Big(X + \frac{v}{2u}Y\Big)^2 + \frac{4uw - v^2}{4u}Y^2 = X'^2 - \frac{\Delta(u, v, w)}{4}Y'^2$$

avec $X' = \sqrt{u}(X + \frac{v}{2u}Y)$ et $Y' = Y/\sqrt{u}$. De plus, l'endomorphisme $(X, Y) \mapsto (X', Y')$ est de déterminant 1. Il existe donc $g \in G$ tel que $\rho_2(g)(uX^2 + vXY + wY^2) = X^2 - \frac{\Delta(u,v,w)}{4}Y^2$. Si $P(u, v, w) \in S(R_2)^G$ est invariant, on doit avoir $P(u, v, w) = P(1, 0, -\Delta(u, v, w)/4)$ puisque $X^2 - \frac{\Delta(u,v,w)}{4}Y^2$ a pour coefficients $u' = 1$, $v' = 0$, $w = -\Delta(u, v, w)/4$, donc $P(u, v, w) \in k[\Delta]$ et $S(R_2)^G \subset k[\Delta]$. L'autre inclusion a déjà été vue, et on a donc $S(R_2)^G = k[\Delta]$.

9. Cas général

L'action π_d de G sur $S(R_d)$ laisse stable chaque sous-espace $S(R_d)_e$ et définit une action de G sur $S(R_d)_e$ que l'on notera $\pi_{d,e}$. Soit $m(d,e) = \dim_k S(R_d)_e^G$. Si $a \in k^\star$, on note

$$g_a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \in \mathrm{SL}_2(k).$$

9-1. On a $\rho_d(g_a)(X^{d-k}Y^k) = (X^{d-k}Y^k) \circ g_a^{-1} = a^{-(d-k)}X^{d-k}a^kY^k = a^{2k-d}X^{d-k}Y^k$. Or $(X^d, X^{d-1}Y, \ldots, Y^d)$ est une base de R_d; la matrice de $\rho_d(g_a)$ dans cette base est diagonale de coefficients diagonaux a^{2k-d}, $0 \le k \le d$. La trace de $\rho_d(g_a)$ vaut donc

$$\mathrm{tr}(\rho_d(g_a)) = a^{-d} + a^{-d+2} + \cdots + a^{d-2} + a^d = a^{-d}(1 + a^2 + \cdots + a^{2d}) = a^{-d}\frac{1 - a^{2(d+1)}}{1 - a^2},$$
$$\mathrm{tr}(\rho_d(g_a)) = \frac{a^{d+1} - a^{-(d+1)}}{a - a^{-1}},$$

sauf si $a = \pm 1$, auquel cas la trace vaut $d + 1$.

9-2. On a $R_0 = k$, et G opère trivialement sur les constantes, donc $(R_0)^G = k$. Supposons maintenant $d > 0$. La matrice de $\rho_d(g_a)$ calculée au 9-1 montre que, pour a non racine de l'unité, le sous-groupe $g_a^{\mathbb{Z}}$ admet comme seuls invariants dans R_d la droite $k\,X^{d/2}Y^{d/2}$ lorsque d est pair, resp. $\{0\}$ lorsque d est impair. On en déduit aisément que l'on a $R_d^G = 0$ pour tout $d > 0$. En effet, c'est clair si d est impair puisque $G \supset g_a^{\mathbb{Z}}$. Si d est pair, le sous-groupe engendré par un conjugué gg_ag^{-1} de g_a admet comme invariants la droite $k\,(X^{d/2}Y^{d/2}) \circ g^{-1}$. Or l'intersection de ces droites lorsque g varie est réduite à 0 (prendre par exemple g telle que $X \circ g^{-1} = X + Y$, $Y \circ g^{-1} = Y$).

9-3. Il est évident que si on a des représentations $(\pi_i)_{i \in I} : H \to \mathrm{GL}(V_i)$ d'un groupe H dans des espaces vectoriels V_i, alors la représentation somme directe $\pi = \bigoplus \pi_i$ sur $H = \bigoplus V_i$ vérifie $\mathrm{tr}\,\pi(h) = \mathrm{tr}\,\pi_i(h)$ pour tout $h \in H$. En effet, la matrice de $\pi(h)$ est constituée de blocs diagonaux qui sont précisément les matrices des $\pi_i(h)$.

9-4. On admet ici que $\mathrm{SL}_2(k)$ n'admet (à isomorphisme près) pas d'autres représentations irréductibles que les représentations "puissances symétriques" R_d, $d \ge 0$, déjà mises en évidence. Comme de plus $\mathrm{SL}_2(k)$ est un "groupe réductif", toute représentation λ de $G = \mathrm{SL}_2(k)$ dans un espace vectoriel V de dimension finie est isomorphe à une somme directe finie $\bigoplus_{d \ge 0} R_d^{n(d)}$.

9-4-1. D'après 9-1 et la remarque 9-3, la trace de $\lambda(g_a)$ est la somme des traces pour les représentations qui composent λ, i.e.

$$\mathrm{tr}(\lambda(g_a)) = \sum_{d \ge 0} n(d)\frac{a^{d+1} - a^{-(d+1)}}{a - a^{-1}}.$$

9-4-2. La trace ci-dessus est un polynôme de Laurent en a, et les éléments $\frac{a^{d+1} - a^{-(d+1)}}{a - a^{-1}}$ sont linéairement indépendants dans l'espace $k[a, a^{-1}]$ des polynômes de Laurent (par exemple parce que la partie positive de $\frac{a^{d+1} - a^{-(d+1)}}{a - a^{-1}}$ est un polynôme unitaire de degré d pour tout d). Il en résulte que les entiers $n(d)$ sont uniquement déterminés par λ (et même par sa classe d'isomorphisme en tant que représentation de $\mathrm{SL}_2(k)$).

9-4-3. Le coefficient de a dans le polynôme de Laurent $(a - a^{-1})\,\mathrm{tr}(\lambda(g_a))$ est égal au coefficient de a dans $\sum_{d \ge 0} n(d)(a^{d+1} - a^{-(d+1)})$, c'est-à-dire $n(0)$. Mais $V^G = \bigoplus_{d \ge 0}((R_d)^G)^{n(d)} = k^{n(0)}$ d'après 9-2, donc $\dim_k V^G = n(0)$.

9-5. Soit $B = (b_{ij})_{1 \le i,j \le n}$ une matrice inversible. On considère l'action λ sur $k[X_1, \ldots, X_n]$ définie par $B \cdot P = P \circ B^{-1}$, et on note $\mathrm{tr}_e(B)$ la trace de l'automorphisme induit $\lambda_e(B)$ sur l'espace vectoriel $k[X_1, \ldots, X_n]_e$.

9-5-1. Le polynôme $\chi(T) = \det(\mathbf{1}_n - B^{-1}T)$ admet 1 pour coefficient de T^0, il est donc de la forme $1 - TP$ où $P \in k[T]$. Il en résulte que $\chi(T)$ admet un inverse dans l'algèbre $k[[T]]$ des séries formelles, à savoir $\chi(T)^{-1} = \sum_{\ell \in \mathbb{N}} T^\ell P^\ell$ qui définit bien une série formelle (les termes d'indices $> \ell$ ne contribuent plus aux coefficients de $1, T, \ldots, T^\ell$).

9-5-2. Si B est triangulaire supérieure de coefficients diagonaux β_i, alors $\chi(T) = \prod_i (1 - \beta_i^{-1} T)$, de sorte que

$$\chi(T)^{-1} = \prod_{1 \le i \le n} \sum_{\alpha_i \in \mathbb{N}} \beta_i^{-\alpha_i} T^{\alpha_i},$$

tandis que B opère de manière triangulaire sur $k[X_1, \dots, X_n]_e$, lorsque cet espace est muni de la base de monômes $X^\alpha = X_1^{\alpha_1} \dots X_n^{\alpha_n}$, ordonnée par l'ordre lexicographique sur les multi-indices $(\alpha_1, \dots, \alpha_n)$. Les coefficients diagonaux sont donnés par $\beta^{-\alpha} = \beta_1^{-\alpha_1} \dots \beta_n^{-\alpha_n}$. On trouve donc

$$\begin{aligned} \mathrm{tr}_e(B) &= \sum_{\alpha_1 + \dots + \alpha_n = e} \beta^{-\alpha}, \\ \sum_{e \ge 0} \mathrm{tr}_e(B)\, T^e &= \sum_{\alpha \in \mathbb{N}^n} \beta^{-\alpha} T^{\alpha_1 + \dots + \alpha_n} = \chi(T)^{-1} = \det(\mathbf{1}_n - B^{-1} T)^{-1}. \end{aligned}$$

Comme la trace et le déterminant sont invariants par conjugaison (i.e. remplacement de B par ABA^{-1}, l'automorphisme induit $\lambda_e(ABA^{-1})$ sur $k[X_1, \dots, X_n]_e$ étant alors égal au conjugué $\lambda_e(A)\lambda_e(B)\lambda_e(A)^{-1}$), l'égalité précédente reste vraie pour toute matrice inversible B. En effet, comme le corps de base k est algébriquement clos, toute matrice (inversible) est conjuguée à une matrice triangulaire (nécessairement inversible).

9-6. Soit $\chi_{d,e}(a)$ la trace de $\pi_{d,e}(a)$. Comme $\pi_{d,e}(a)$ est induit sur $S(R_d)_e$ par $B = \rho_d(a)$, qui est un endomorphisme diagonalisable de coefficients diagonaux a^{2k-d} sur la base de monômes $(X^d, X^{d-1}Y, \dots, Y^d)$ de R_d (voir 9-1), la question 9-5-2 montre que

$$\sum_{e \ge 0} \chi_{d,e}(a)\, T^e = \det(\mathbf{1} - \rho_d(a)^{-1})^{-1} = \big[(1 - a^{-d}T)(1 - a^{-d+2}T) \dots (1 - a^d T)\big]^{-1}.$$

9-7. Soit $F_U(W) \in \mathbb{Z}[U][[W]]$ défini par

$$F_U(W) = (1 - W)(1 - UW) \dots (1 - U^d W).$$

On a $F_U(W) = 1 - W G_U(W)$ où $G_U \in \mathbb{Z}[U][W]$ d'où

$$F_U(W)^{-1} = \sum_{\ell \ge 0} W^\ell G_U(W)^\ell, \qquad G_U(W)^\ell \in \mathbb{Z}[U][W].$$

En développant chaque terme de la série en fonction des puissances W^e et en regroupant les monômes obtenus suivant celles-ci, on voit que seul un nombre fini de termes $W^\ell G_U(W)^\ell$ (à savoir les termes tels que $\ell \le e$) contribuent au coefficient de W^e. Les coefficients $M_{d,e}(U)$ sont donc des polynômes dans $\mathbb{Z}[U]$, et on les écrira

$$M_{d,e}(U) = \sum_{i \ge 0} c(d,e,i) U^i, \qquad c(d,e,i) \in \mathbb{Z}.$$

9-8. Après substitution de T par $a^d T$, la formule 9-5-3 donne

$$\sum_{e \ge 0} \chi_{d,e}(a)\, a^{de} T^e = \big[(1 - T)(1 - a^2 T) \dots (1 - a^{2d} T)\big]^{-1} = F_{a^2}(T) = \sum_{e \ge 0} M_{d,e}(a^2) T^e.$$

Par identification du coefficient de T^e il vient $\chi_{d,e}(a) = a^{-de} M_{d,e}(a^2)$.

9-9. D'après la question 9-4-3, la dimension $m(d,e) = \dim_k S(R_d)_e^G$ est égale au coefficient de a dans

$$(a - a^{-1})\chi_{d,e}(a) = (a - a^{-1}) a^{-de} M_{d,e}(a^2) = (a - a^{-1}) a^{-de} M_{d,e}(a^2) = \sum_{i \ge 0} c(d,e,i) a^{2i-de} (a - a^{-1}).$$

Pour que ce coefficient soit non nul, il est nécessaire que de soit pair, et dans ce cas seuls les termes $c(d,e,i)$ avec $2i - de = 0, 2$ fournissent une contribution. On trouve alors

$$m(d,e) = c(d,e,de/2) - c(d,e,(de/2)+1).$$

Partie V. Groupe symétrique

Soit B une algèbre et $f(U_1, \ldots, U_n) \in B[U] := B[U_1, \ldots, U_n]$. On définit

$$D_{U,Y} f(U_1, \ldots, U_n, Y_1, \ldots, Y_n) = Y_1 \frac{\partial f}{\partial U_1} + \cdots + Y_n \frac{\partial f}{\partial U_n} \in B[U, Y].$$

10-1. Un calcul immédiat montre que

$$D_{U,Y} f = \frac{d}{dT}_{T=0} f(U_1 + TY_1, \ldots, U_n + TY_n).$$

D'après la règle de dérivation de Leibniz pour les polynômes formels, il en résulte que $D_{U,Y}$ est une dérivation de $B[U]$ dans $B[U, Y]$, i.e. $D_{U,Y}$ est une application B-linéaire telle que

$$D_{U,Y}(fg) = f\, D_{U,Y}(g) + g\, D_{U,Y}(f)$$

pour tous $f, g \in B[U]$.

10-2. Un calcul immédiat montre que

$$D_{U,Y} f = \frac{d}{dT}_{T=0} f(U_1 + TY_1, \ldots, U_n + TY_n).$$

D'après la règle de dérivation de Leibniz pour les polynômes formels, il en résulte que $D_{U,Y}$ est une dérivation de $B[U]$ dans $B[U, Y]$, i.e. $D_{U,Y}$ est une application B-linéaire telle que

$$D_{U,Y}(fg) = f\, D_{U,Y}(g) + g\, D_{U,Y}(f)$$

pour tous $f, g \in B[U]$.