Correction de la composition de *Mathématiques générales* Agrégation 1994

Partie I. Préliminaires.

Question 1.1. Montrons par récurrence sur n la propriété suivante :

> $(\mathcal{P}_n)$ *Soit $P \in k[X_1, \ldots, X_n]$ tel que la fonction associée soit identiquement nulle sur $A_1 \times \cdots \times A_n$. Alors $P = 0$.*

La propriété $(\mathcal{P}_1)$ découle du fait qu'un polynôme en une variable n'a qu'un nombre fini de racines.

Soit maintenant $n \geqslant 2$ et supposons que la propriété $(\mathcal{P}_{n-1})$ est vraie. Écrivons

$$P = \sum_{i=0}^{d} P_i X_n^i,$$

où les P_i appartiennent à $k[X_1, \ldots, X_{n-1}]$. Fixons $(a_1, \ldots, a_{n-1}) \in A_1 \times \ldots A_{n-1}$ et posons

$$Q = \sum_{i=0}^{d} P_i(a_1, \ldots, a_{n-1}) X_n^i.$$

Alors Q est un polynôme en une indéterminée (l'indéterminée X_n) et, si $a \in k$, on a $Q(a) = P(a_1, \ldots, a_{n-1}, a)$. Par conséquent, $Q(a) = 0$ pour tout $a \in A_n$. Puisque A_n est infinie, il résulte de $(\mathcal{P}_1)$ que $Q = 0$. En d'autres termes, $P_i(a_1, \ldots, a_{n-1}) = 0$ pour tout i. Ceci étant vrai pour tout $(a_1, \ldots, a_{n-1}) \in A_1 \times \cdots \times A_{n-1}$, l'hypothèse de récurrence implique que $P_0 = P_1 = \cdots = P_d = 0$. Donc $P = 0$, ce qui montre $(\mathcal{P}_n)$.

Question 1.2. Puisque $U \neq \varnothing$, choisissons $(x_1, \ldots, x_n) \in U$. Puisque U est ouvert, et puisque la topologie de k^n est la topologie produit, il existe une famille $(U_i)_{1 \leqslant i \leqslant n}$ d'ouverts de k tels que $x_i \in U_i$ et $U_1 \times \cdots \times U_n \subset U$. Donc, par hypothèse, P est identiquement nul sur $U_1 \times \cdots \times U_n$ et les ensembles U_i sont infinis (ouverts non vides). Il résulte de la question **1.1** que $P = 0$.

Question 1.3. (1.3.1) Montrons d'abord que cela définit bien une action de groupes *sur un ensemble*. Soient g, $h \in G$ et $f \in F(V)$ et soit $v \in V$. Alors $1.f(v) = f(1.v) = f(v)$ donc $1.f = f$. D'autre part,

$$\big(g.(h.f)\big)(v) = (h.f)(g^{-1}.v) = f\big(h^{-1}.(g^{-1}.v)\big) = f\big((gh)^{-1}.v\big) = \big((gh).f\big)(v),$$

ce qui montre que l'on a bien défini une action de G sur *l'ensemble* $F(V)$.

Pour montrer que cela définit bien une action de G sur *l'espace vectoriel* $F(V)$, il suffit de montrer que, si $g \in G$, λ, $\lambda' \in k$ et f, $f' \in F(V)$, alors $g.(\lambda f + \lambda' f') = \lambda(g.f) + \lambda'(g.f')$, ce qui se vérifie aisément en évaluant en $v \in V$.

(1.3.2) Soit $h \in F(V)^G$ et soit $v \in V$. Soit alors w un élément de l'orbite de v. Par définition, il existe $g \in G$ tel que $w = g^{-1}.v$. Par suite,

$$h(w) = h(g^{-1}.v) = (g.h)(v) = v,$$

la dernière égalité découlant du fait que $g.h = h$ car $h \in F(V)^G$ est invariant. Donc h est constante sur $\mathcal{O}_v$.

Réciproquement, soit $f \in F(V)$ constante sur toutes les G-orbites. On a alors, pour tous $g \in G$ et $v \in V$,

$$(g.f)(v) = f(g^{-1}.v) = f(v),$$

la dernière égalité découlant du fait que f est constante sur les G-orbites. Donc $g.f = f$. Ceci étant vrai pour tout $g \in G$, f est G-invariante.

Question 1.4. (1.4.1) Tout d'abord, si $g \in G$, on a $\rho(g)(X^n) = g^n X^n$. L'application $k[X] \times k[X] \to k[X]$, $(P,Q) \mapsto \rho(g)(P.Q) - \rho(g)(P).\rho(g)(Q)$ étant k-bilinéaire, il suffit de montrer qu'elle s'annule sur les couples (X^m, X^n), m, $n \in \mathbb{N}$. C'est alors un calcul élémentaire.

(1.4.2) Soit $P = \sum_{i=0}^d a_i X^i$. Alors $P \in k[X]^G$ si et seulement si on a l'égalité $\sum_{i=0}^d a_i X^i = \sum_{i=0}^d a_i g^i X^i$ pour tout $g \in G$, c'est-à-dire si et seulement si $\sum_{i=0}^d a_i X^i = \sum_{i=0}^d a_i \omega^i X^i$. En d'autres termes, $P \in k[X]^G$ si et seulement si $(\omega^i - 1)a_i = 0$ pour tout i, c'est-à-dire si et seulement si $a_i = 0$ pour tout i non divisible par r. Finalement $k[X]^G \subset k[X^r]$. L'inclusion réciproque est immédiate. Donc $k[X]^G = k[X^r]$.

Question 1.5. (1.5.1) Soit $g \in \mathbf{GL}_n(k)$. Écrivons $g^{-1} = (a_{ij})_{1 \leqslant i,j \leqslant n}$. On a alors, pour tout $x = (x_1, \ldots, x_n) \in k^n$,

$$P(g^{-1}.x) = P(\sum_{j=1}^n a_{1j}x_j, \ldots, \sum_{j=1}^n a_{nj}x_j),$$

ce qui montre que $g.P$ est la fonction associée au polynôme

$$P(\sum_{j=1}^n a_{1j}X_j, \ldots, \sum_{j=1}^n a_{nj}X_j).$$

(1.5.2) La $\mathbf{GL}_n(k)$-orbite d'un vecteur non nul de k^n est $k^n - \{0\}$ (en effet, $\mathbf{GL}_n(k)$ agit transitivement sur les bases de k^n donc agit transitivement sur l'ensemble des premiers vecteurs d'une base : tout vecteur non nul peut être le premier vecteur d'une base).

(1.5.3) Soit $P \in k[X_1, \ldots, X_n]$ tel que la fonction associée soit $\mathbf{GL}_n(k)$-invariante. Alors P est constante sur l'orbite d'un vecteur non nul (voir question **1.3.2**) donc est constante sur $k^n - \{0\}$ (voir question **1.5.2**). Notons $c \in k$ cette constante. Alors la fonction associée au polynôme $P - c$ est nulle sur $(k^\times)^n \subset k^n - \{0\}$, donc $P - c = 0$ d'après la question **1.1** (et car k est infini). Donc P est un polynôme constant.

Partie II. Polynômes et actions sur des algèbres.

Question 2.1. (2.1.1) Le dual V^* de V est un sous-espace (et donc un sous-ensemble) de $F(V)$. La sous-algèbre $S(V)$ étant engendrée par une base de V^*, elle est donc égale à la sous-algèbre de $F(V)$ engendrée par V^*. Donc $S(V)$ ne dépend pas du choix de la base de V.

(2.1.2) Par la propriété universelle des algèbres de polynômes, il existe un unique morphisme de k-algèbres $\pi : k[X_1, \ldots, X_n] \to F(V)$ tel que $\pi(X_i) = X_i^0$. Son image est, par définition, la sous-algèbre $S(V)$. De plus, π est injectif d'après la question **1.1**. Donc π est un isomorphisme.

(2.1.3) On pourrait montrer ce résultat par des simples changements de variables linéaires. On va en fait faire apparaître une caractérisation intrinsèque de $S(V)_d$ ne faisant appel à aucun choix de base de V. Plus précisément, le résultat découle immédiatement du lemme suivant :

Lemme A - $S(V)_d = \{f \in S(V) \mid \forall\, v \in V,\ \forall\, \lambda \in k,\ f(\lambda v) = \lambda^d f(v)\}$.

Preuve - Posons $H_d = \{f \in S(V) \mid \forall\, v \in V,\ \forall\, \lambda \in k,\ f(\lambda v) = \lambda^d f(v)\}$. Il est tout d'abord clair que $S(V)_d \subset H_d$. Le point délicat est de montrer la réciproque. Soit donc $P \in k[X_1, \ldots, X_n]$ tel que la fonction associée à P appartienne à H_d. Notons Q le polynôme en $n+1$ variables $X_1, \ldots, X_n$, X égal à

$$Q(X_1, \ldots, X_n, X) = P(XX_1, \ldots, XX_n) - X^d P(X_1, \ldots, X_n).$$

Par hypothèse, la fonction sur k^{n+1} associée à Q est identiquement nulle. Donc, d'après la question **1.1**, on a $Q = 0$, c'est-à-dire

$$P(XX_1, \ldots, XX_n) = X^d P(X_1, \ldots, X_n).$$

En identifiant les coefficients des monômes de ces deux polynômes, on obtient immédiatement que $P(X_1, \ldots, X_n)$ ne fait intervenir que des monômes de degré d. Donc $H_d \subset S(V)_d$. ■

Question 2.2. (2.2.1) D'après la question **1.3.1**, il suffit de montrer que, si f, $f' \in F(V)$ et $g \in G$, alors $g.(ff') = (g.f).(g.f')$. Soit donc $v \in V$. On a

$$\big(g.(ff')\big)(v) = (ff')(g^{-1}.v) = f(g^{-1}.v).f'(g^{-1}.v) = (g.f)(v).(g.f')(v) = \big((g.f).(g.f')\big)(v),$$

d'où le résultat.

(2.2.2) Cela résulte du lemme A et du fait que G agit linéairement sur V.

(2.2.3) Puisque le morphisme d'algèbres π est un isomorphisme, on a

$$S(V) = \bigoplus_{d \geqslant 0} S(V)_d.$$

Soit $f \in S(V)^G$ et écrivons $f = \sum_{d=0}^{m} f_d$, où $f_d \in S(V)_d$ (cette décomposition est unique). On a alors, pour tout $g \in G$,

$$\sum_{d=0}^{m} f_d = f = \rho(g)(f) = \sum_{d=0}^{m} \rho(g)(f_d).$$

D'autre part, l'action de G sur $S(V)$ stabilise chaque composante homogène $S(V)_d$. Donc $\rho(g)(f_d) \in S(V)_d$. Par l'unicité de la décomposition de f en somme de composantes homogènes, on obtient que $\rho(g)(f_d) = f_d$ pour tout $d \geqslant 0$ et tout $g \in G$. Donc

$$f \in \bigoplus_{d \geqslant 0} \big(S(V)^G \cap S(V)_d\big).$$

Cela montre l'inclusion

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

L'inclusion réciproque est évidente.

Partie III. Exemples.

3. Groupe spécial linéaire.

Question 3.1. Tout d'abord, si $r > n$, alors U_r est vide, donc ouvert. Supposons donc maintenant dans cette question que $r \leqslant n$.

Par le choix d'une base de V, on peut identifier V^r avec l'espace vectoriel des matrices $\mathrm{Mat}_{n\times r}(k)$ à coefficients dans k (cette identification, linéaire, respecte la topologie). Il suffit donc de montrer que l'ensemble $\mathcal{U}_r$ des matrices $M \in \mathrm{Mat}_{n\times r}(k)$ de rang r est un ouvert. Pour cela, posons $m = \binom{n}{r} \geqslant 1$ et notons $I_1,\ldots, I_m$ les parties de $\{1,2,\ldots,n\}$ à r éléments. Si $1 \leqslant i \leqslant m$ et si $M \in \mathrm{Mat}_{n\times r}(k)$, on note $f_i(M)$ la matrice de taille $r \times r$ extraite de M correspondant à la partie I_i de $\{1,2,\ldots,n\}$. Alors l'application

$$\begin{array}{rccc} \varphi : & \mathrm{Mat}_{n\times r}(k) & \longrightarrow & k^m \\ & M & \longmapsto & \big(\det(f_1(M)),\ldots,\det(f_m(M))\big) \end{array}$$

est continue (car polynômiale). D'autre part, $M \in \mathcal{U}_r$ si et seulement si $\varphi(M) \neq 0$ (car $r \leqslant n$). En d'autres termes,

$$\mathcal{U}_r = \varphi^{-1}(k^m - \{0\}),$$

donc $\mathcal{U}_r$ est ouvert (car $k^m - \{0\}$ est ouvert dans k^m et φ est continue).

Question 3.2. Tout d'abord, il est clair que G stabilise U_r. Pour montrer que U_r est une G-orbite, il suffit donc de montrer que G agit transitivement sur U_r. Soient $(v_1,\ldots,v_r)$ et $(w_1,\ldots,w_r)$ deux éléments de U_r. Par le théorème de la base incomplète, il existe des vecteurs $v_{r+1},\ldots, v_n$, $w_{r+1},\ldots, w_n$ tels que $(v_1,\ldots,v_n)$ et $(w_1,\ldots,w_n)$ soient des bases de V. Notons $g : V \to V$ l'unique application linéaire telle que $g(v_i) = w_i$ pour tout i. Alors $g \in \mathbf{GL}(V)$. Notons λ le déterminant de g et notons $u : V \to V$ l'unique application linéaire telle que $u(w_1) = w_1,\ldots, u(w_{n-1}) = w_{n-1}$ et $u(w_n) = \lambda^{-1}w_n$. Alors $\det(u) = \lambda^{-1}$ donc $\det(ug) = 1$. En d'autres termes, $ug \in \mathbf{SL}(V)$ et, puisque $r < n$, on a

$$ug(v_1,\ldots,v_r) = (w_1,\ldots,w_r),$$

ce qui montre que U_r est une $\mathbf{SL}(V)$-orbite.

Montrons maintenant que $S(V)^G = k$. Il est tout d'abord clair que $k \subset S(V)^G$. Réciproquement, soit $f \in S(V)^G$. Alors f est constante sur les G-orbites (voir question **1.3.1**). Donc f est constante sur U_r : notons c cette constante. Alors $f - c$ est une fonction polynomiale qui est nulle sur U_r, donc elle est identiquement nulle d'après la question **1.1**. Donc $S(V)^G = k$.

Question 3.3. (3.3.1) Remarquons tout d'abord que $f \in S(V^n)$ (c'est un polynôme en les coordonnées de v_i dans la base e). Soient $(v_1,\ldots,v_n) \in V^n$ et $g \in G = \mathbf{SL}(V)$. Alors

$$\begin{aligned} (g.f)(v_1,\ldots,v_n) &= \det{}_e(g^{-1}(v_1),\ldots,g^{-1}(v_n)) \\ &= \det(g)^{-1}\det{}_e(v_1,\ldots,v_n) \\ &= f(v_1,\ldots,v_n) \end{aligned}$$

car $\det(g) = 1$. Donc $g.f = f$. Ceci étant vrai pour tout $g \in G$, on a $f \in S(V^n)^G$.

(3.3.2) Soit $(v_1, \ldots, v_n) \in U_n$. Posons $\alpha = \det_e(v_1, \ldots, v_n)$. Notons $g : V \to V$ l'unique application linéaire telle que $g(e_1) = v_1, \ldots, g(e_{n-1}) = v_{n-1}$ et $g(e_n) = \alpha^{-1} v_n$. Alors $\det(g) = 1$, donc $g \in \mathbf{SL}(V)$ et $g(e_1, \ldots, e_{n-1}, \alpha e_n) = (v_1, \ldots, v_n)$. Donc toute G-orbite dans U_n contient un élément de la forme $(e_1, \ldots, e_{n-1}, \alpha e_n)$.

Nous allons maintenant montrer que, si α et β sont deux éléments de $k^\times$ tels que $(e_1, \ldots, e_{n-1}, \alpha e_n)$ et $(e_1, \ldots, e_{n-1}, \beta e_n)$ sont dans la même G-orbite, alors $\alpha = \beta$. Notons $g \in G$ un élément de G tel que $g(e_1, \ldots, e_{n-1}, \alpha e_n) = (e_1, \ldots, e_{n-1}, \beta e_n)$. Alors $1 = \det(g) = \beta\alpha^{-1}$. D'où le résultat.

> Conclusion - Si $(v_1, \ldots, v_n) \in U_n$, alors il existe un unique élément $\alpha \in k^\times$ tel que $(v_1, \ldots, v_n)$ appartienne à la G-orbite de $(e_1, \ldots, e_{n-1}, \alpha e_n)$. On a alors $\alpha = f(v_1, \ldots, v_n)$.

Montrons maintenant que $S(V)^G = k[f]$. Tout d'abord, d'après la question **3.3.1**, on a $k[f] \subset S(V)^G$. Réciproquement, soit $\varphi \in S(V)^G$. Notons P l'unique polynôme de $k[X]$ tel que $\varphi(e_1, \ldots, e_{n-1}, \alpha e_n) = P(\alpha)$ pour tout $\alpha \in k^\times$. Puisque φ est constante sur les G-orbites (voir question **1.3.2**), il découle de la conclusion ci-dessus que $\varphi - P(f)$ est nulle sur sur U_n. C'est une fonction polynômiale et U_n est ouvert (voir question **1.3.1**) donc $\varphi - P(f) = 0$ d'après la question **1.2**. Donc $\varphi = P(f) \in k[f]$. Donc $S(V^n)^G = k[f]$.

4. Quelques groupes finis.

Question 4.1. Notons $\sigma_i \in k[X_1, \ldots, X_n]$ le i-ième polynôme symétrique élémentaire :

$$\sigma_i = \sum_{1 \leqslant j_1 < \cdots < j_i \leqslant n} X_{j_1} \cdots X_{j_i}.$$

Le théorème des polynômes symétriques dit que l'application

$$\begin{array}{ccc} k[X_1, \ldots, X_n] & \longrightarrow & k[X_1, \ldots, X_n]^{\mathfrak{S}_n} \\ P & \longmapsto & P(\sigma_1, \ldots, \sigma_n) \end{array}$$

est un isomorphisme de k-algèbres. En d'autres termes, $k[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ est une algèbre de polynômes engendrée par $\sigma_1, \ldots, \sigma_n$.

Question 4.2. On vérifie facilement que l'action définie est bien une action du groupe G sur l'algèbre $k[X_1, \ldots, X_n]$.

(4.2.1) Si $P \in S(V)_d$, alors $\varepsilon.P = (-1)^d P$. Donc P est invariant si et seulement si d est pair. D'après la question **2.2.3**, on a

$$S(V)^G = \bigoplus_{d \geqslant 0} S(V)_{2d}.$$

Il est ensuite facile de vérifier par récurrence sur d que tout monôme homogène de degré $2d$ est un produit de monômes de degré 2. D'où le résultat.

(4.2.2) Pour des raisons de degré, les éléments X_1^2, X_2^2 et X_1X_2 sont des éléments irréductibles de $k[X_1, \ldots, X_n]^G$ deux à deux non associés. Or, $X_1^2.X_2^2 = (X_1X_2)^2$, donc

$k[X_1, \ldots, X_n]^G$ n'est pas factoriel. En particulier, ce n'est pas une algèbre de polynômes (car une algèbre de polynômes est factorielle).

(4.2.3) Soit $P \in k[U, V, W]$ tel que $P(X^2, XY, Y^2) = 0$. Voyons P et $V^2 - UW$ comme des polynômes en la variable V à coefficients dans l'anneau intègre $k[U, W]$. Alors $V^2 - UW$ est unitaire donc la division euclidienne de P par $V^2 - UW$ nous donne deux polynômes A et B dans $k[U, W][V]$ tels que $B = 0$ ou $\deg(B) \leqslant 1$ (le degré de B en la variable V) et

$$P(U, V, W) = (V^2 - UW)A + B.$$

Écrivons $B = \alpha(U, W)V + \beta(U, W)$ où α et β sont deux polynômes en U et W uniquement déterminés. On a alors

$$0 = P(X^2, XY, Y^2) = B(X^2, XY, Y^2) = XY\alpha(X^2, Y^2) + \beta(X^2, Y^2).$$

En effectuant le changement de variables $X \mapsto -X$ et $Y \mapsto Y$, on obtient aussi que

$$-XY\alpha(X^2, Y^2) + \beta(X^2, Y^2) = 0,$$

donc, en sommant ces deux égalités et en utilisant le fait que k n'est pas de caractéristique 2, on déduit que $\beta(X^2, Y^2) = 0$, ce qui implique que $\beta = 0$. Par conséquent, $\alpha = 0$ et donc P est un multiple de $V^2 - UW$.

(4.2.4) Soit $\pi : k[U, V, W] \to k[X^2, XY, Y^2]$, $P \mapsto P(X^2, XY, Y^2)$. Puisque $\pi(U) = X^2$, $\pi(V) = XY$ et $P(W) = Y^2$, π est surjectif. D'autre part, $\pi(V^2 - UW) = 0$, donc l'idéal engendré par $V^2 - UW$ est contenu dans le noyau de π. La question **4.2.3** montre en fait que $\operatorname{Ker} \pi = (V^2 - UW)$. Le théorème de factorisation nous dit qu'il existe un unique morphisme d'algèbres $\bar{\pi} : k[U, V, W]/(V^2 - UW) \to k[X^2, XY, Y^2]$ rendant le diagramme

$$\begin{tikzcd}
k[U, V, W] \arrow[r, "\pi"] \arrow[d] & k[X^2, XY, Y^2] \\
k[U, V, W]/(V^2 - UW) \arrow[ur, "\bar{\pi}"'] &
\end{tikzcd}$$

commutatif. Le morphisme $\bar{\pi}$ est alors un isomorphisme (car π est surjectif et $\operatorname{Ker} \pi = (V^2 - UW)$).

5. Groupe orthogonal.

Question 5.1. Tout d'abord, deux éléments de V qui sont dans la même $\mathbf{O}(V)$-orbite ont la même norme. Cela montre l'unicité du réel positif ou nul a.

Montrons l'existence. Soit $v \in V$ et posons $a = \sqrt{v.v}$. Si $a = 0$, alors $v = 0$ est dans la même $\mathbf{O}(V)$-orbite que $ae_1 = 0$. Supposons $a > 0$. Il existe une base orthonormée de V de la forme $(v/a, v_2, \ldots, v_n)$. Notons $g : V \to V$ l'unique application linéaire telle que $g(e_1) = v/a$ et $g(e_i) = v_i$ si $i \geqslant 2$. Alors $g \in \mathbf{O}(V)$ et $g(v) = ae_1$, donc v est dans la même $\mathbf{O}(V)$-orbite que ae_1.

CONCLUSION - Si $v \in V$, alors il existe un unique élément $a \in \mathbb{R}$ tel que v appartienne à la $\mathbf{O}(V)$-orbite de ae_1. On a alors $a = \sqrt{v.v}$.

Question 5.2. Notons N le polynôme $X_1^2 + \cdots + X_n^2$. Comme l'action d'un élément de $\mathbf{O}(V)$ conserve la norme, il est clair que $N \in S(V)^{\mathbf{O}(V)}$. Puisque $S(V)^{\mathbf{O}(V)}$ est une sous-algèbre de $S(V)$, on a $\mathbb{R}[N] \subset S(V)^{\mathbf{O}(V)}$.

Réciproquement, soit $f \in S(V)^{\mathbf{O}(V)}$ et notons $P(X)$ le polynôme en une variable tel que $P(a) = f(ae_1)$. Puisque ae_1 et $-ae_1$ ont la même norme, ils sont dans la même $\mathbf{O}(V)$-orbite (voir la question **5.1**) et donc $P(a) = P(-a)$ pour tout $a \in \mathbb{R}$ (voir la question **1.3.2**). Par suite, d'après la question **1.4.2** (appliquée au cas où $r = 2$), il existe un polynôme $Q(X)$ tel que $P(X) = Q(X^2)$.

Alors, si $v \in V$, notons $a = \sqrt{v.v}$. On a $f(v) = f(ae_1) = P(a) = Q(a^2) = Q(N(v))$. Cela montre que $f = Q \circ N$, et donc que $f \in \mathbb{R}[N]$.

6. Groupe orthogonal (suite).

Question 6.1. On peut identifier L avec la fonction $E \times E \to \mathbb{R}$, $(x, y) \mapsto H(x.y, x.x, y.y)$. Soit maintenant $g \in \mathbf{O}(E)$ et $(x, y) \in V \times V$. On a

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

la troisième égalité découlant du fait que g respecte le produit scalaire. Donc $g.L = L$ pour tout $g \in G$, c'est-à-dire $L \in S(V)^G$.

Question 6.2. Soit $g : E \to E$, $(x_1, x_2) \mapsto (x_1, -x_2)$. Alors $g \in \mathbf{O}(E)$ et donc, si $(a, b, c) \in \mathbb{R}^3$, alors $F(a, 0, b, c) = (g.F)(a, 0, b, c) = F(a, 0, b, -c)$. Par conséquent,

$$(*) \qquad K(a,b,c) = K(a,b,-c).$$

Soit maintenant $h : E \times E$, $(x_1, x_2) \mapsto (-x_1, x_2)$. Alors $h \in \mathbf{O}(E)$ et donc, si $(a, b, c) \in \mathbb{R}^3$, alors $F(a, 0, b, c) = (g.F)(a, 0, b, c) = F(-a, 0, -b, c)$. Par conséquent,

$$(**) \qquad K(a,b,c) = K(-a,-b,c).$$

D'autre part, K est une fonction associée à un polynôme en trois indéterminées (A, B, C) que nous noterons encore $K \in \mathbb{R}[A, B, C]$. Écrivons

$$K = \sum_{i=0}^{d} K_i(A,B)C^i.$$

L'égalité $(*)$ montre que, par un raisonnement analogue à celui de la question **1.4.2**, que $K_i = 0$ si i est impair. Quant à elle, l'égalité $(**)$ montre, en utilisant la question **4.2.1**, que, pour tout i, il existe un polynôme $H_i \in \mathbb{R}[U, V, W]$ tel que $K_i(A, B) = H_i(AB, A^2, B^2)$. Par suite, il existe un polynôme $\mathcal{K} \in \mathbb{R}[U, V, W, T]$ tel que

$$(\#) \qquad K(A,B,C) = \mathcal{K}(AB, A^2, B^2, C^2).$$

Question 6.3. Si $(x, y) \in E^2 = V$, alors il existe $g \in \mathbf{O}(E)$ tel que $g(x)$ est proportionnel à e_1 (voir question **5.1**). Si on pose $u = g(x)$ et $v = g(y)$, alors (u, v) est dans l'orbite de (x, y) et u est proportionnel à e_1.

Notons $\mathcal{K}_0(U, V, W, T) = \mathcal{K}(U, V, W, T - W)$ et notons α le degré en W du polynôme $\mathcal{K}_0$. Alors la fraction rationnelle

$$M(U, V, T) = V^\alpha \mathcal{K}_0(U, V, U^2/V, T)$$

est en fait un polynôme en les indéterminées U, V, et T.

Fixons maintenant $x \in E \setminus \{0\}$ et $y \in E$. Soit $a = \sqrt{x.x}$ et soit $v = (b, c) \in E$ tel que (ae_1, v) soit dans la G-orbite de (x, y) (voir au-dessus). On a alors

$$\begin{aligned} (x.x)^\alpha.F(x, y) &= (x.x)^\alpha F(a, 0, b, c) \\ &= (x, x)^\alpha \mathcal{K}(ab, a^2, b^2, c^2) \\ &= (x, x)^\alpha \mathcal{K}_0(ab, a^2, b^2, b^2 + c^2) \\ &= M(ab, a^2, b^2 + c^2). \end{aligned}$$

Or, $ab = (ae_1).v = x.y$, $a^2 = x.x$ et $b^2 + c^2 = v.v = y.y$ (car (ae_1, v) et (x, y) sont dans la même G-orbite). Donc,

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

Question 6.4. Puisque $(E - \{0\}) \times (E - \{0\})$ est ouvert dans $E \times E = V$, le résultat découle de la question **1.2**.

Question 6.5. La question **6.1** montre que

$$\mathbb{R}[X_1Y_1 + X_2Y_2, X_1^2 + X_2^2, Y_1^2 + Y_2^2] \subset \mathbb{R}[X_1, X_2, Y_1, Y_2]^G.$$

Montrons l'inclusion réciproque. Soit $F \in \mathbb{R}[X_1, X_2, Y_1, Y_2]^G$. La question **6.3** (et par symétrie) montre qu'il existe deux polynômes P et Q dans $\mathbb{R}[U, V, W]$ et deux entiers naturels p et q tels que, si $(x, y) \in (E - \{0\}) \times (E - \{0\})$, alors

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

D'après la question **6.4**, les polynômes $W^q P(U, V, W)$ et $V^p Q(U, V, W)$ sont égaux. Mais, l'anneau $\mathbb{R}[U, V, W]$ étant factoriel et les polynômes V et W étant irréductibles et non associés, on obtient que V^p divise $P(U, V, W)$. Posons alors $\mathcal{P} = P(U, V, W)/V^p \in \mathbb{R}[U, V, W]$. On a alors, pour tout $(x, y) \in (E - \{0\}) \times (E - \{0\})$,

$$F(x, y) = \mathcal{P}(x.y, x.x, y.y).$$

Encore une fois, $(E - \{0\}) \times (E - \{0\})$ étant ouvert, il résulte de la question **1.2** que

$$F(X_1, X_2, Y_1, Y_2) = \mathcal{P}(X_1Y_1 + X_2Y_2, X_1^2 + X_2^2, Y_1^2 + Y_2^2),$$

ce qui montre que

$$\mathbb{R}[X_1, X_2, Y_1, Y_2]^G \subset \mathbb{R}[X_1Y_1 + X_2Y_2, X_1^2 + X_2^2, Y_1^2 + Y_2^2].$$

D'où l'égalité entre ces deux algèbres.

7. Conjugaison.

Question 7.1. Posons $\Delta_n = \prod_{i=1}^n (X_i - X_j)^2$. Il est clair que Δ_n est un polynôme symétrique (c'est-à-dire que $\Delta_n \in \mathbb{C}[X_1, \ldots, X_n]^{\mathfrak{S}_n}$) donc, d'après la question **4.1**, il existe un polynôme $P_n \in \mathbb{C}[T_1, \ldots, T_n]$ tel que

$$(+) \qquad \Delta_n = P_n(\sigma_1, \ldots, \sigma_n),$$

où les σ_i sont les polynômes symétriques élémentaires (voir question **4.1**).

Soit maintenant $(a_1, \ldots, a_n) \in \mathbb{C}^n$ et notons $(\lambda_1, \ldots, \lambda_n)$ les racines (avec multiplicités) du polynôme

$$T^n - a_1 T^{n-1} + \cdots + (-1)^{n-1} a_{n-1} T + (-1)^n a_n.$$

Les relations entre les coefficients et les racines d'un polynôme nous disent que

$$a_i = \sigma_i(\lambda_1, \ldots, \lambda_n).$$

Il résulte de (+) que

$$(++) \qquad \Delta_n(\lambda_1, \ldots, \lambda_n) = P_n(a_1, \ldots, a_n).$$

Revenons maintenant à la question qui nous intéresse. Utilisons pour cela les notations de la question suivante **7.2** (!). L'égalité (++) nous dit que

$$u \in U \textit{ si et seulement si } P_n(\tau_1(u), \ldots, \tau_n(u)) \neq 0.$$

Or, l'application

$$\begin{array}{rccc} \Gamma : & V & \longrightarrow & \mathbb{C} \\ & u & \longmapsto & P_n(\tau_1(u), \ldots, \tau_n(u)) \end{array}$$

est clairement polynômiale (composée d'applications polynômiales), donc continue. Par suite, $U = \Gamma^{-1}(\mathbb{C}^\times)$ est ouvert.

Un élément $u \in U$ étant diagonalisable, son orbite sous G est l'ensemble des $v \in V$ tels que $P_u(T) = P_v(T)$.

Question 7.2. Comme cela a déjà été dit, τ_j est une fonction associée à un polynôme. Le fait que τ_j est invariant sous G découle du fait que le polynôme caractéristique d'un endomorphisme est invariant par conjugaison, i.e. $P_A(T) = P_{gAg^{-1}}(T)$ pour tous $A \in V$ et $g \in \mathbf{GL}(E)$.

Question 7.3. Tout d'abord, il résulte de la question **7.2** que $\mathbb{C}[\tau_1, \ldots, \tau_n] \subset S(V)^G$.

Réciproquement, soit $f \in S(V)^G$. Fixons une base $(e_1, \ldots, e_n)$ de l'espace vectoriel E. Si $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$, on note u_x l'unique endomorphisme de E tel que $u_x(e_i) = x_i e_i$ pour tout i. On pose alors

$$P(x) = f(u_x).$$

Alors P est une fonction polynomiale sur $\mathbb{C}^n$. Elle est de plus symétrique car, si x' est obtenu à partir de x par permutations des coordonnées, alors les endomorphismes u_x et $u_{x'}$ sont semblables. Donc il existe un polynôme $Q \in \mathbb{C}[T_1, \ldots, T_n]$ tel que

$$P(x) = Q(\sigma_1(x), \ldots, \sigma_n(x)).$$

Or, il est facile de vérifier que $\sigma_i(x) = \tau_i(u_x)$. Par conséquent,

$$f(u_x) = Q(\tau_1(u_x), \ldots, \tau_n(u_x)).$$

Soit maintenant $u \in U$. Alors u est diagonalisable donc il existe $x \in \mathbb{C}^n$ tel que u soit semblable à u_x. Puisque $f \in S(V)^G$, on a $f(u) = f(u_x)$ et $\tau_i(u) = \tau_i(u_x)$ (voir question **7.2**). Par suite,

$$\forall\ u \in U,\ f(u) = Q(\tau_1(u), \ldots, \tau_n(u)).$$

Puisque U est ouvert (voir question **7.1**), il résulte de la question **1.2** que

$$\forall\ u \in V,\ f(u) = Q(\tau_1(u), \ldots, \tau_n(u)).$$

Donc $f = Q(\tau_1, \ldots, \tau_n) \in \mathbb{C}[\tau_1, \ldots, \tau_n]$. Donc $S(V)^G = \mathbb{C}[\tau_1, \ldots, \tau_n]$.