1. On considère le sous-groupe G de $GL_n(\mathbb{R})$ engendré par les matrices de permutation et les matrices de changement de signe sur un nombre pair de coordonnées. On le fait agir naturellement sur les fonctions polynomiales. Montrer que la sous-algèbre des fonctions polynomiales invariantes par G est une algèbre de polynômes et déterminer explicitement un système basique d'invariants.

Corrigé. Montrons que G est engendré par des réflexions, ce qui permettra d'affirmer que l'algèbre $k[x_1, \ldots, x_n]^G$ des polynômes invariants par G est une algèbre de polynômes : or manifestement G est engendré par les transpositions entre deux coordonnées, d'une part, et d'autre part par les changements de signe sur deux coordonnées. Les premières sont bien des réflexions, et les secondes n'en sont pas, mais elles sont composées de la transposition entre les deux coordonnées et la transposition avec changement de signe, et on a là deux réflexions (dans G). Si on préfère, G est engendré par les réflexions par rapport aux hyperplans $x_i = x_j$ et $x_i = -x_j$ pour (i, j) parcourant tous les couples d'éléments distincts de $\{1, \ldots, n\}$.

Reste à trouver explicitement un système basique d'invariants. Notons $\Psi_1, \ldots, \Psi_n$ les fonctions symétriques élémentaires non pas sur les coordonnées $x_1, \ldots, x_n$ elles-mêmes mais sur leurs carrés $x_1^2, \ldots, x_n^2$: autrement dit, on pose $\Psi_1 = x_1^2 + \cdots + x_n^2$ et $\Psi_2 = \sum_{i<j}(x_i x_j)^2$ et ainsi de suite jusqu'à $\Psi_n = (x_1 \cdots x_n)^2$. Notons que Ψ_n est le carré de $\Sigma_n = x_1 \cdots x_n$. Remarquons que l'algèbre de polynômes engendrée par $x_1^2, \ldots, x_n^2$ est l'algèbre $k[x_1, \ldots, x_n]^{(\mathbb{Z}/2\mathbb{Z})^n}$ des polynômes (en $x_1, \ldots, x_n$) invariants par changement de signe sur un nombre quelconque de coordonnées, et que par conséquent l'algèbre de polynômes engendrée par $\Psi_1, \ldots, \Psi_n$ est l'algèbre $k[x_1, \ldots, x_n]^{G'}$ des polynômes invariants par toute permutation des coordonnées et tout changement de signe d'un nombre quelconque d'entre eux (on appelle G' le sous-groupe de $GL_n(\mathbb{R})$ entendré par les matrices de permutation et les matrices de changement de signe sur un nombre quelconque de coordonnées). On a certainement $k[x_1, \ldots, x_n]^{G'} \subseteq k[x_1, \ldots, x_n]^G$, et on va montrer que $k[x_1, \ldots, x_n]^G = k[\Psi_1, \ldots, \Psi_{n-1}, \Sigma_n]$. Comme chaque Ψ_i, et aussi Σ_n, sont invariants par G, une inclusion est claire.

Si $f \in k[x_1, \ldots, x_n]^G$ (autrement dit, si f est un polynôme en $x_1, \ldots, x_n$ invariant par permutation quelconque des variables ou par changement de signe sur un nombre pair d'entre elles), appelons $\widehat{f}$ le polynôme obtenu en remplaçant x_1 par $-x_1$ dans f. On vérifie que $\widehat{f}$ est encore invariant par G : c'est tout à fait évident pour un changement de signe sur un nombre pair de coordonnées, et pour ce qui est d'une permutation d'entre elles on remarque que quitte à changer éventuellement le signe de deux coordonnées (x_1 et celle en laquelle elle a été permutée) on se ramène effectivement à $\widehat{f}$. Par conséquent, $f_+ = \frac{1}{2}(f + \widehat{f})$ et $f_- = \frac{1}{2}(f - \widehat{f})$ sont encore dans $k[x_1, \ldots, x_n]^G$; on peut les appeler partie paire et partie impaire de f respectivement. La première est dans $k[x_1, \ldots, x_n]^{G'}$; la seconde change de signe si on change de signe l'une quelconque des variables, autrement dit, il s'agit d'un polynôme impair en chaque variable, donc multiple de chacune d'elles, donc cette partie impaire est multiple de Σ_n, et le quotient h est dans $k[x_1, \ldots, x_n]^{G'}$. On a ainsi montré que tout élément f de $k[x_1, \ldots, x_n]^G$ s'écrit de façon unique comme $f_+ + h\Sigma_n$ avec f_+ et h dans $k[x_1, \ldots, x_n]^{G'}$ (et, qui plus est, uniquement définis : si on préfère, $k[x_1, \ldots, x_n]^G$ est un module libre de rang 2 sur $k[x_1, \ldots, x_n]^{G'}$ avec pour base $\{1, \Sigma_n\}$). Puisque $k[x_1, \ldots, x_n]^{G'} = k[\Psi_1, \ldots, \Psi_n]$ (et comme $\Psi_n = \Sigma_n^2$), on en déduit $k[x_1, \ldots, x_n]^G = k[\Psi_1, \ldots, \Psi_{n-1}, \Sigma_n]$, ce qui répond à la question posée (on a trouvé n générateurs de l'algèbre intègre $k[x_1, \ldots, x_n]^G$ dont le corps des fractions $k(x_1, \ldots, x_n)^G$ est de degré de transcendance n, donc ces générateurs sont bien algébriquement indépendants sur k).

On peut vérifier que le produit des degrés de $\Psi_1, \ldots, \Psi_{n-1}, \Sigma_n$ est $2 \times 4 \times \cdots \times 2(n-1) \times n = 2^{n-1}\, n!$, qui est bien le cardinal de G, et la somme des degrés diminués de 1 est

$1+3+\cdots+(2n-3)+(n-1)=n(n-1)$, qui est bien le nombre de réflexions dans G (il y a $\frac{1}{2}n(n-1)$ hyperplans de la forme $x_i=x_j$ et autant de la forme $x_i=-x_j$). ✓

2. Soit $\phi=\frac{1}{2}(1+\sqrt{5})$ le nombre d'or et $A=\mathbb{Z}[\phi]$. On considère un $\mathbb{R}^4$ euclidien dont le produit scalaire sera noté $(x|y)$ et la base orthonormée standard $(\epsilon_i)_{i=1}^4$. Posons $\mathbf{D}_4=\{\pm\epsilon_i\pm\epsilon_j : i\neq j\}$ (ensemble de cardinal 24) et soit $\mathbf{S}$ l'ensemble des $\alpha\in\mathbb{R}^4$ tels que $|\alpha|^2=2$ et $(\alpha|\beta)\in A$ pour tout $\beta\in\mathbf{D}_4$. Quel est le cardinal de $\mathbf{S}$? A-t-on $(\alpha|\beta)\in A$ pour tous $\alpha,\beta\in\mathbf{S}$?

On considère une partie maximale $\mathbf{H}_4$ de $\mathbf{S}$ ayant la propriété que $(\alpha|\beta)\in A$ pour tous $\alpha,\beta\in\mathbf{H}_4$. Montrer que son cardinal est au plus 120. Montrer que $\mathbf{H}_4$ est stable par réflexion par rapport à l'orthogonal de tout élément de $\mathbf{H}_4$. Montrer que $\mathbf{H}_4$ a pour cardinal exactement 120.

Corrigé. On peut écrire $\mathbf{S}=\{a_1\epsilon_1+a_2\epsilon_2+a_3\epsilon_3+a_4\epsilon_4 : a_1^2+a_2^2+a_3^3+a_4^2=2 \text{ et } \forall i,j\ a_i\pm a_j\in A\}$. Manifestement on doit donc avoir $a_i\in\frac{1}{2}A$ pour chaque i. En posant $a_i=b_i+c_i\phi$ où $b_i,c_i\in\frac{1}{2}\mathbb{Z}$, on voit que les b_i doivent être tous entiers ou tous de partie fractionnaire $\frac{1}{2}$, et de même pour les c_i. Comme $a_i^2=b_i^2+c_i^2+c_i(2b_i+c_i)\phi$, on énumère facilement explicitement les éléments de $\mathbf{S}$: ce sont tous les éléments obtenus par permutation et changements de signe des coordonnées à partir de

$$\begin{aligned}
\alpha_1 &= \epsilon_1+\epsilon_2\\
\alpha_2 &= \tfrac{1}{2}(1-\phi)(\epsilon_1+\epsilon_2+\epsilon_3)+\tfrac{1}{2}(1+\phi)\epsilon_4\\
\alpha_3 &= \tfrac{1}{2}(\epsilon_1+\epsilon_2+\epsilon_3)+(\phi-\tfrac{1}{2})\epsilon_4\\
\alpha_4 &= \tfrac{1}{2}\phi(\epsilon_1+\epsilon_2+\epsilon_3)+(\tfrac{1}{2}\phi-1)\epsilon_4
\end{aligned}$$

soit $24+64+64+64=216$ éléments. Manifestement, si α' désigne l'élément obtenu à partir de $\alpha\in\mathbf{S}$ en changeant le signe de la première composante a_1, on a $(\alpha|\alpha')=2-2a_1^2$ donc $(\alpha|\alpha')\in A$ implique $a_1^2\in\frac{1}{2}A$, ce qui n'est pas le cas pour $\alpha_2,\alpha_3,\alpha_4$ ci-dessus ; donc une partie de $\mathbf{S}$ telle que $(\alpha|\beta)\in A$ pour α,β quelconques ne peut comporter qu'au plus la moitié des permutations signées sur $\alpha_2,\alpha_3,\alpha_4$, soit au plus $24+32+32+32=120$ éléments.

Soit maintenant $\mathbf{H}_4$ une partie de $\mathbf{S}$ maximale pour la propriété que $(\alpha|\beta)\in A$ lorsque α,β sont dedans. Si $\alpha,\beta\in\mathbf{H}_4$ alors par définition on a encore $\alpha-(\alpha|\beta)\beta\in\mathbf{S}$ (noter que $s_\beta(\alpha)=\alpha-(\alpha|\beta)\beta$ est la réflexion de α par rapport à l'orthogonal de β). Et cet élément $\gamma=\alpha-(\alpha|\beta)\beta$ a encore la propriété que $(\gamma|\delta)\in A$ pour tout $\delta\in\mathbf{H}_4$ puisque α et β ont cette propriété : donc par maximalité $\gamma\in\mathbf{H}_4$, ce qui prouve la stabilité voulue.

D'autre part, $\mathbf{H}_4\supseteq\mathbf{D}_4$ par maximalité de $\mathbf{H}_4$ et par définition de $\mathbf{S}$. En particulier, la symétrie par rapport à l'orthogonal de tout $\pm\epsilon_i\pm\epsilon_j$ préserve $\mathbf{H}_4$, donc (cf. exercice précédent) toute permutation des coordonnées avec changement de signe sur un nombre pair d'entre elles doit préserver $\mathbf{H}_4$. Donc le cardinal de $\mathbf{H}_4$ est exactement $24+32+32+32=120$, et on peut prendre par exemple $\mathbf{H}_4=\mathbf{D}_4\cup W(\mathbf{D}_4)\alpha_2\cup W(\mathbf{D}_4)\alpha_3\cup W(\mathbf{D}_4)\alpha_4$ où $W(\mathbf{D}_4)$ est le groupe des permutations de coordonnées avec changement de signe sur un nombre pair d'entre elles. ✓

Rappel : Soit $G\subseteq GL_n(k)$ un groupe fini de transformations linéaires de k^n où k est un corps de caractéristique 0. Soit $S=k[x_1,\ldots,x_n]$ et S^G le sous-anneau des polynômes G-invariants. Si $P(t)=\sum_{d=0}^{+\infty}\dim_k(\{h\in S^G : \deg h=d\})\,t^k$ (série de Hilbert de S^G), alors on a $P(t)=\frac{F(t)}{(1-t^{d_1})\cdots(1-t^{d_r})}$, où $F\in\mathbb{Z}[t]$, si S^G est engendré par des polynômes homogènes de degrés $d_1,\ldots,d_r$, et de plus $P(t)=\frac{1}{\operatorname{card} G}\sum_{A\in G}\frac{1}{\det(I-tA)}$ (formule de Molien).

3. On pose $\sigma_i=\begin{pmatrix}0&i\\i&0\end{pmatrix}$ et $\sigma_j=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ et $\sigma_k=\sigma_i\sigma_j$ dans $GL_2(\mathbb{C})$, de sorte que $Q=\{\pm I,\pm\sigma_i,\pm\sigma_j,\pm\sigma_k\}$ forme un sous-groupe d'ordre huit isomorphe au groupe des quaternions.

Calculer la série de Hilbert pour $\mathbb{C}[x,y]^Q$. Vérifier que les polynômes $f = x^4 + y^4$ et $g = x^2y^2$ sont invariants : quelle est la série de Hilbert de la sous-algèbre $\mathbb{C}[f,g]$? Trouver un élément h de degré 6 invariant par Q, et en déduire une présentation de $\mathbb{C}[x,y]^Q$ de la forme $\mathbb{C}[f,g,h]/(R)$ où R est une relation que l'on précisera.

Corrigé. L'élément I (resp. $-I$) de Q a la valeur propre $+1$ (resp. -1) avec multiplicité 2 ; les six éléments autres que $\pm I$ ont tous les deux valeurs propres i et $-i$. D'après la formule de Molien citée en rappel, la série de Hilbert pour $\mathbb{C}[x,y]^Q$ est donc $\frac{1}{8}(\frac{1}{(1-t)^2} + \frac{1}{(1+t)^2} + \frac{6}{1+t^2}) = \frac{1+t^6}{(1-t^4)^2}$. Les polynômes $f = x^4 + y^4$ et $g = x^2y^2$ sont manifestement invariants par σ_i et σ_j donc par Q. Ils sont algébriquement indépendants (par exemple par critère jacobien) donc $\mathbb{C}[f,g] \subseteq \mathbb{C}[x,y]^Q$ est une algèbre de polynôme, dont la série de Hilbert est donc $\frac{1}{(1-t^4)^2}$.

Par ailleurs, si $h = xy(x^4 - y^4)$ alors $h \in \mathbb{C}[x,y]^Q$ (de degré 6) vérifie $h^2 = f^2g - 4g^3$ (en degré 12) ; le sous-anneau $\mathbb{C}[f,g] \oplus h\mathbb{C}[f,g]$ de $\mathbb{C}[x,y]^Q$ a donc la même série de Hilbert $\frac{1-t^{12}}{(1-t^4)^2\,(1-t^6)} = \frac{1+t^6}{(1-t^4)^2}$ que $\mathbb{C}[x,y]^Q$, donc c'est tout $\mathbb{C}[x,y]^Q$. On a donc $\mathbb{C}[x,y]^Q = \mathbb{C}[f,g,h]/(h^2 = f^2g - 4g^3)$. ✓