1. Soit V un espace vectoriel hermitien complexe de dimension finie n, de base $(e_1, \dots, e_n)$. On ne suppose pas que cette base est orthonormale. On désigne par $\langle \cdot, \cdot \rangle$ le produit scalaire de V, supposé linéaire en la deuxième variable. Pour $1 \leq i \leq n$, soit s_i une transformation unitaire telle que $s_i(e_i) = c_i e_i$ avec $c_i \neq 1$ et de sous-espace de vecteurs invariants l'orthogonal de e_i. On appelle W le sous-groupe de $GL(V)$ engendré par les s_i.

(i) Soit $x \in V$. Exprimer $s_i(x)$ comme combinaison linéaire de x et de e_i.

(ii) Soit k un entier supérieur ou égal à 1. Montrer que tout élément de $\bigwedge^k(V)$ invariant par W est nul. (On pourra procéder par récurrence sur n en considérant le sous-espace V' de base $(e_1, \dots, e_{n-1})$, et en décomposant V comme somme directe de V' et de son supplémentaire orthogonal.)

(ii) On suppose que W est fini. Montrer que pour tout élément A de $\mathrm{End}(V)$ on a :
$*\sum_{w \in W} \det(A - w) = \mathrm{card}(W) \cdot \det(A)$
$*\sum_{w \in W} \det(\mathrm{id} - Aw) = \mathrm{card}(W)$
En déduire que pour tout A de $\mathrm{End}(V)$ il existe $w \in W$ tel que Aw n'ait aucun point fixe non nul.

Corrigé. (i) Pour tout $x \in V$, on a $s_i(x) = x + \gamma_i \langle e_i, x \rangle e_i$, où $\gamma_i = \frac{c_i - 1}{\|e_i\|^2}$: il suffit de vérifier cette formule pour $x = e_i$ et pour x orthogonal à e_i, les deux cas étant clairs d'après la définition. Le fait que s_i soit supposée unitaire équivaut à $|c_i| = 1$.

(ii) Tout d'abord, un $w \in W$ agit sur $\bigwedge^k V$ en envoyant $v_1 \wedge \cdots \wedge v_k$ sur $w(v_1) \wedge \cdots \wedge w(v_k)$. Dire qu'un élément est invariant par W signifie simplement qu'il est invariant par tous les s_i.

Écrivons $V = V' \oplus \mathbb{C}q$, où $V' = \mathbb{C}e_1 \oplus \cdots \oplus \mathbb{C}e_{n-1}$ est le sous-espace vectoriel engendré par les $n - 1$ premiers vecteurs de la base, et q un vecteur orthogonal à V'. On peut alors décomposer $\bigwedge^k V$ en $\bigwedge^k V' \oplus (q \wedge \bigwedge^{k-1} V')$ — où le second terme est à comprendre comme l'ensemble des éléments de la forme $q \wedge z$ avec $z \in \bigwedge^{k-1} V'$ (qui est alors uniquement défini). Supposons maintenant $\tau \in \bigwedge^k V$, et soit $\tau = \tau' + q \wedge \tau''$ sa décomposition comme on vient de l'expliquer, où $\tau' \in \bigwedge^k V'$ et $\tau'' \in \bigwedge^{k-1} V'$. Pour $1 \leq i \leq n-1$, on a $s_i(\tau) = s_i(\tau') + q \wedge s_i(\tau'')$ (puisque q est invariant par s_i). Si on suppose τ invariant par $s_1, \dots, s_n$, on voit alors que τ' et τ'' sont invariants par la restriction de $s_1, \dots, s_{n-1}$ à V' : en procédant par récurrence sur n (l'hypothèse de récurrence portant sur tout $k \geq 1$), on peut donc supposer $\tau' = 0$, et $\tau'' = 0$ sauf dans le cas où $k = 1$. Il n'y a donc plus que ce seul cas à traiter : on a alors $\tau = \lambda q \in V$ orthogonal à $e_1, \dots, e_{n-1}$, mais l'invariance par s_n (et le fait que $c_n \neq 1$) montre qu'on a aussi $\tau \perp e_n$. Donc τ ne peut être que nul.

(iii) Soient $v_1, \dots, v_n$ des éléments quelconques de V : si on développe complètement $(v_1 - w(e_1)) \wedge \cdots \wedge (v_n - w(e_n))$, l'un des termes est $v_1 \wedge \cdots \wedge v_n$, et tous les autres peuvent s'écrire comme $\pm \tau_w \wedge \mu$, où τ_w est de la forme $w(e_{i_1}) \wedge \cdots \wedge w(e_{i_k}) \in \bigwedge^k V$ avec $k \geq 1$ et μ est dans $\bigwedge^{n-k} V$ et indépendant de w ; or si on somme sur tous les $w \in W$, le facteur τ_w donne une somme $\sum_{w \in W} \tau_w$ invariante par l'action de W, donc nulle d'après la question (i), donc $\sum_{w \in W} \tau_w \wedge \mu = 0$ aussi. Ceci prouve que $\sum_{w \in W} (v_1 - w(e_1)) \wedge \cdots \wedge (v_n - w(e_n)) = \mathrm{card}(W) \cdot v_1 \wedge \cdots \wedge v_n$ (tous les autres termes s'annulent ainsi qu'on vient de le voir) : c'est exactement la première formule qu'il s'agissait de prouver (avec $v_i = A(e_i)$). Pour ce qui est de la seconde, on peut par exemple remarquer qu'elle découle de la première lorsque A est inversible (de $\sum_{w \in W} \det(A^{-1} - w) = \mathrm{card}(W) \cdot \det(A^{-1})$ on déduit $\sum_{w \in W} \det(\mathrm{id} - Aw) = \mathrm{card}(W)$ en multipliant par $\det(A)$), et, comme il s'agit d'une égalité entre fonctions polynomiales, l'égalité sur une partie dense (les matrices inversibles) suffit à conclure.

Enfin, si Aw avait un point fixe non nul pour tout $w \in W$, cela voudrait dire que le noyau de $\mathrm{id} - Aw$ n'est jamais réduit à $\{0\}$, donc $\det(\mathrm{id} - Aw) = 0$ toujours, ce qui contredit la seconde formule qu'on vient de prouver. ✓

2. (i) Montrer que si un sous-groupe transitif du groupe symétrique $\mathfrak{S}_n$ contient un $(n-1)$-cycle et une transposition, alors ce groupe est $\mathfrak{S}_n$.

(ii) Déterminer le groupe de Galois sur $\mathbb{Q}$ du polynôme
$P(X) = X^6 - 12X^4 + 15X^3 - 6X^2 + 15X + 12$.

Corrigé. (i) Quitte à réordonner les éléments, on peut supposer que le $(n-1)$-cycle est $(2\ 3\ \cdots\ n)$. Si la transposition est $(a\ b)$, puisque le groupe est transitif on peut supposer $a = 1$ (en conjuguant par un élément qui s'y ramène) et quitte à conjuguer par la bonne puissance du cycle que $b = 2$. Or il est assez clair que $(1\ 2)$ et $(2\ 3\ \cdots\ n)$ engendrent bien $\mathfrak{S}_n$.

(ii) Le polynôme P est irréductible : cela découle du critère d'Eisenstein appliqué au nombre premier 3. En réduisant P modulo 2, on trouve $X^6 + X^3 + X = X\,(X^5 + X^2 + 1)$, et $X^5 + X^2 + 1$ est irréductible modulo 2 (il suffit de vérifier qu'il n'a de racine ni dans $\mathbb{F}_2$ ni dans $\mathbb{F}_4$, ce qui prouve qu'il n'a de facteur ni de degré 1 ni de degré 2) ; donc le groupe de Galois de P sur les rationnels (vu comme sous-groupe de $\mathfrak{S}_6$) doit contenir un 5-cycle. Enfin, en réduisant modulo 5, on trouve $X^6 - 2X^4 - X^2 + 2 = (X-1)(X-2)(X-3)(X-4)(X^2-2)$, et $X^2 - 2$ est irréductible modulo 5 ; donc le groupe de Galois de P doit contenir une transposition. Le (i) permet alors de conclure que ce groupe de Galois est $\mathfrak{S}_6$ tout entier. ✓

3. Soit $K \subseteq L$ une extension galoisienne finie. On considère L comme un K-espace vectoriel et, pour tout $x \in L$, l'application K-linéaire de L dans L donnée par la multiplication par x. Montrer que le déterminant de cette application linéaire est le produit de tous les conjugués de x (comptés avec leur multiplicité).

En déduire que si K est un corps fini ou bien le corps $\mathbb{C}(t)$, il existe pour tout entier naturel d un polynôme homogène de degré d en d variables sur K dont le seul zéro est le zéro trivial (l'origine).

Corrigé. Soit $G = \mathrm{Gal}(L/K)$ le groupe de Galois de L sur K et $x \in L$, et soit H le fixateur de x dans G ; on appellera G/H l'ensemble $\{\sigma H\}$ des classes à gauche. Alors l'ensemble des conjugués de x est $\{\sigma(x) : \bar\sigma \in G/H\}$ (dont le nombre est $\mathrm{card}(G/H) = \deg_K(x)$). Le polynôme minimal de x sur K est $\prod_{\bar\sigma \in G/H}(X - \sigma(x)) \in K[X]$, et c'est évidemment aussi le polynôme minimal de la multiplication par x (dans $K(x)$ ou dans L) donc aussi le polynôme caractéristique de la multiplication par x dans $K(x)$ (puisqu'il a le bon degré). Ainsi, le déterminant de la multiplication par x dans $K(x)$ est $\prod_{\bar\sigma \in G/H} \sigma(x)$. En voyant L comme somme de $\mathrm{card}(H) = [L : K(x)]$ copies de $K(x)$, on en déduit que le déterminant de la multiplication par x dans L est la puissance $\mathrm{card}(H)$-ième de ce qui précède, soit $\prod_{\sigma \in G} \sigma(x)$.

On a donc défini une application $\mathrm{N}\colon L \to K$ qui envoie x sur $\prod_{\sigma \in G} \sigma(x)$ et qui, puisqu'on peut la voir comme un déterminant, est un polynôme (si on considère L comme un K-espace vectoriel) de degré $[L : K]$ en $[L : K]$ variables. Ce polynôme ne s'annule que lorsqu'un des $\sigma(x)$ vaut zéro, auquel cas x lui-même vaut zéro. Par conséquent, pour trouver un polynôme homogène de degré d en d variables sur K qui ne s'annule qu'à l'origine, il suffit de trouver une extension galoisienne de degré d de K. Puisque tout corps fini admet une extension galoisienne (par ailleurs unique) en tout degré et puisque $\mathbb{C}(t)$ admet pour tout d l'extension $\mathbb{C}(t^{1/d})$ de degré d (et galoisienne car $\mathbb{C}$ contient les racines de l'unité), on a le résultat souhaité. ✓

4. (a) Soient $k \subseteq K$ deux corps algébriquement clos, $P_1, \ldots, P_r$ une famille d'éléments de $k[X_1, \ldots, X_n]$. On suppose que les P_i ont un zéro commun dans K^n. Montrer qu'ils en ont un dans k^n.

(b) Montrer que si $P \in k[X_1, \ldots, X_n]$ est irréductible, il l'est aussi dans $K[X_1, \ldots, X_n]$. (Étant donné un nombre fini d'éléments de $K[X_1, \ldots, X_n]$, on pourra considérer une base du sous-k-espace vectoriel de K engendré par les coefficients de ces polynômes.)

(c) (i) Soient $x_1, \dots, x_k$ des nombres complexes qui sont algébriques sur $\mathbb{Q}$. Montrer qu'ils sont contenus dans une extension galoisienne finie K de $\mathbb{Q}$, et qu'ils engendrent avec leurs conjugués dans K une $\mathbb{Z}[\frac{1}{N}]$-algèbre entière, où N est un entier convenable.

(ii) Soit N un entier et A une $\mathbb{Z}[\frac{1}{N}]$-algèbre entière ; montrer que pour tout nombre premier p ne divisant pas N, pA est un idéal strict de A.

(d) Soient $P_1, \dots, P_r \in \mathbb{Z}[X_1, \dots, X_n]$. Montrer que les conditions suivantes sont équivalentes :

(i) Les P_i ont un zéro commun dans $\mathbb{C}^n$.

(ii) Il existe une extension finie K de $\mathbb{Q}$ telle que les P_i ont un zéro commun dans K^n.

(iii) Pour tout nombre premier p assez grand, il existe un corps fini F de caractéristique p tel que les P_i réduits modulo p ont un zéro commun dans F^n.

Corrigé. (a) Par contraposée, on veut montrer que si les P_i n'ont pas de zéro commun dans k^n, ils n'en ont pas dans K^n. Or l'hypothèse signifie, d'après le Nullstellensatz, qu'ils engendrent l'idéal unité dans $k[X_1, \dots, X_n]$, donc qu'on peut écrire $1 = P_1Q_1 + \cdots P_rQ_r$ avec $Q_i \in k[X_1, \dots, X_n]$, ce qui vaut encore dans $K[X_1, \dots, X_n]$, donc il ne peut pas y avoir de zéro commun dans K^n.

(b) Supposons qu'on ait $P = QR$ dans $K[X_1, \dots, X_n]$. Considérons $c_1, \dots, c_s$ une base du sous-k-espace vectoriel de K engendré par les coefficients de Q et de R, et dans cette base écrivons $Q = c_1Q_1 + \cdots + c_sQ_s$ et de même $R = c_1R_1 + \cdots + c_sR_s$, où $Q_i, R_i \in k[X_1, \dots, X_n]$. Manifestement, Q s'annule en un point $(x_1, \dots, x_n) \in k^n$ si et seulement si tous les Q_i s'y annulent, et de même R s'y annule si et seulement si tous les R_i s'y annulent : donc l'ensemble $V_k(P)$ des zéros de P dans k^n est la réunion de l'ensemble $V_k(Q_1, \dots, Q_s)$ des zéros communs des Q_i et de celui $V_k(R_1, \dots, R_s)$ des zéros communs des R_i ; mais puisque P est irréductible, $V_k(P)$ est irréductible (au sens de la topologie de Zariski), donc l'un de ces deux ensembles, mettons $V_k(Q_1, \dots, Q_s)$, doit être $V_k(P)$ tout entier. Ainsi, dès que $P(x_1, \dots, x_n) = 0$ (où $(x_1, \dots, x_n) \in k^n$) on a $Q_i(x_1, \dots, x_n) = 0$ pour tout i ; or ceci implique (d'après le Nullstellensatz) qu'une certaine puissance de Q_i est multiple de P (dans $k[X_1, \dots, X_n]$), donc Q_i lui-même l'est (car P est irréductible dans $k[X_1, \dots, X_n]$ qui est un anneau factoriel). Alors Q est multiple de P (dans $K[X_1, \dots, X_n]$) : on a bien prouvé que P est irréductible dans $K[X_1, \dots, X_n]$ (dans l'écriture $P = QR$, un des facteurs est constant).

(c) (i) Chaque x_i est racine de son polynôme minimal $f_i \in \mathbb{Q}[X]$, dont les (autres) racines s'appellent conjugués algébriques (sur $\mathbb{Q}$) de x_i : si K est le corps engendré par tous les x_i et tous leurs conjugués, i.e., la clôture normale de $\mathbb{Q}(x_1, \dots, x_k)$, alors K est normal donc galoisien (sur $\mathbb{Q}$). Mieux : si N est le ppcm des coefficients dominants de tous les f_i, alors chaque x_i (ou chaque conjugué d'icelui) est entier sur $\mathbb{Z}[\frac{1}{N}]$ puisque, justement, le coefficient dominant de f_i est inversible dans $\mathbb{Z}[\frac{1}{N}]$ (donc on peut le chasser) : ceci montre que l'algèbre engendrée par tous les x_i et tous leurs conjugués (dans K) est entière sur $\mathbb{Z}[\frac{1}{N}]$.

(ii) On veut montrer que pA n'est pas tout A, autrement dit, que p n'est pas inversible dans A. Or si c'était le cas, on aurait $pu = 1$ pour un certain $u \in A$ qui serait entier sur $\mathbb{Z}[\frac{1}{N}]$, mettons $u^d + c_{d-1}u^{d-1} + \cdots + c_0 = 0$ avec $c_j \in \mathbb{Z}[\frac{1}{N}]$; alors $1 + c_{d-1}p + \cdots + c_0p^d = 0$, ce qui est impossible : en multipliant par N^ℓ avec ℓ assez grand pour que tous les termes soient entiers, on voit que le premier n'est pas multiple de p tandis que tous les autres le sont.

(d) Si (i) est satisfaite, alors la question (a) prouve que les P_i ont un zéro commun dans $\bar{\mathbb{Q}}^n$ (où $\bar{\mathbb{Q}}$ désigne la fermeture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$), et un tel zéro existe alors dans une certaine extension finie K (qu'on peut même choisir galoisienne, comme on l'a vu) de $\mathbb{Q}$, ce qui montre (ii). Le fait que (ii) implique (i) est clair. Donc (i) et (ii) sont équivalents.

Montrons maintenant l'équivalence de (ii) et (iii). Si (ii) est satisfaite, alors d'après (c) le

zéro commun des P_i vit dans une certaine $\mathbb{Z}[\frac{1}{N}]$-algèbre finie (= entière de type fini) A (pour N convenable), et pour p premier supérieur à N l'idéal pA de A est strict, donc contenu dans un idéal maximal $\mathfrak{m}$, et alors $F = A/\mathfrak{m}$ est un corps de caractéristique p, qui est fini sur $\mathbb{F}_p$ puisque A l'est sur $\mathbb{Z}[\frac{1}{N}]$ donc c'est un corps fini, et il est clair que les P_i réduits modulo p ont le zéro commun dans F^n : ceci montre (iii). Supposons maintenant que (ii) n'est pas satisfaite : alors d'après le Nullstellensatz, on peut écrire $P_1Q_1 + \cdots + P_sQ_s = 1$ pour certains polynômes $Q_1, \ldots, Q_s \in \bar{\mathbb{Q}}[X_1, \ldots, X_n]$; comme ci-dessus, on trouve un corps fini F tel qu'en réduction on ait $\tilde{P}_1\tilde{Q}_1 + \cdots + \tilde{P}_s\tilde{Q}_s = 1$ où $\tilde{P}_i$ sont les réductions des P_i modulo p : ceci montre que les $\tilde{P}_i$ ne peuvent pas avoir de zéro commun dans $\bar{\mathbb{F}}_p$, contredisant (iii). ✓

5. Soit V un espace vectoriel réel euclidien de dimension n, G un sous-groupe fini du groupe orthogonal $O(V)$ engendré par des réflexions. Une fois fixée une base de V, G agit naturellement dans l'algèbre des polynômes $\mathbb{R}[X_1, \ldots, X_n]$. Soit $P_1, \ldots, P_n \in \mathbb{R}[X_1, \ldots, X_n]$ une famille de polynômes homogènes algébriquement indépendants qui engendrent la sous-algèbre $\mathbb{R}[X_1, \ldots, X_n]^G$ des invariants. On appelle $J \in \mathbb{R}[X_1, \ldots, X_n]$ le déterminant jacobien de l'application

$$\phi\colon (X_1, \ldots, X_n) \mapsto (P_1(X_1, \ldots, X_n),\ \ldots\ P_n(X_1, \ldots, X_n))$$

On dit qu'un élément $Q \in \mathbb{R}[X_1, \ldots, X_n]$ est anti-invariant si :
pour tout $w \in G$, $w(Q) = \det(w) \cdot Q$.

(i) Montrer que J est anti-invariant.

(ii) Pour chaque réflexion $s \in G$, soit H_s l'hyperplan des points fixes de s et l_s une forme linéaire non nulle de noyau H_s. Montrer qu'il existe un réel non nul λ tel que : $J = \lambda \prod_s l_s$, où le produit porte sur l'ensemble des réflexions de G.

(On pourra montrer que J s'annule sur chacun des hyperplans H_s.)

(iii) Montrer qu'un élément $Q \in \mathbb{R}[X_1, \ldots, X_n]$ est anti-invariant si et seulement si Q est le produit de J par un élément de $\mathbb{R}[X_1, \ldots, X_n]^G$.

Corrigé. (i) J est le déterminant de la matrice $\mathscr{J}$ des $\frac{\partial P_i}{\partial X_j}$. Or si $w \in G$, on a $\frac{\partial P_i}{\partial X_j} = \frac{\partial P_i(w^{-1}(X_1,\ldots,X_n))}{\partial X_j} = \sum_k \frac{\partial P_i(Y_1,\ldots,Y_n)}{\partial Y_k}|_{\underline{Y}=w^{-1}(\underline{X})} \cdot \frac{\partial (w^{-1})_k}{X_i}$ (la première égalité étant par invariance des P_i et la seconde différentiation de la composée $\phi \circ w^{-1}$), c'est-à-dire que $\mathscr{J} = (\mathscr{J} \circ w^{-1}) \cdot w^{-1}$, et en passant au déterminant, $J = (J \circ w^{-1}) \cdot \det(w)^{-1}$, soit, puisqu'on fait agir w par $w(J) = J \circ w^{-1}$, justement $w(J) = \det(w)\, J$.

(ii) Si $s \in G$ est une réflexion, d'hyperplan H_s, alors d'après ce qu'on vient de voir, $J \circ s = -J$, donc J s'annule sur H_s. On en déduit que J est multiple de l_s (en tant que polynôme à n indéterminées) : comme ceci vaut pour chaque réflexion $s \in G$ (et que les l_s sont des éléments irréductibles de l'anneau des polynômes qui est factoriel), J est multiple de $\prod_s l_s$. Mais en comparant les degrés (on sait que la somme des degrés des P_i diminués de 1, c'est-à-dire le degré de J, est justement le nombre de réflexions dans G), ces deux polynômes coïncident à une constante près.

(iii) Si Q est anti-invariant, on a de nouveau $Q \circ s = -Q$ pour toute réflexion $s \in G$, donc Q s'annule sur chaque H_s donc est multiple de chaque l_s. Donc Q est multiple de J, mettons $Q = RJ$. Mais alors R est laissé invariant par chaque réflexion dans G, donc $R \in \mathbb{R}[X_1, \ldots, X_n]^G$. ✓