1. Soient $k \subseteq K$ deux corps, et soit n un entier naturel. On munit K^n de sa topologie de Zariski[1] : (1) montrer qu'elle induit la topologie de Zariski sur le sous-ensemble k^n. (2) On suppose que k est algébriquement clos : montrer que pour tout fermé de Zariski Z de K^n défini par des équations à coefficients dans k, l'ensemble $Z \cap k^n$ est dense dans Z pour la topologie de Zariski. Ce résultat vaut-il encore si on ne suppose plus k algébriquement clos ?

2 (Fischer 1915). Soit G un sous-groupe *fini abélien* de $GL(V)$, où V est un $\mathbb{C}$-espace vectoriel de dimension finie n (et $GL(V)$ le groupe des applications linéaires inversibles $V \to V$). On note $\mathbb{C}(V)$ le corps des fractions rationnelles sur V (c'est-à-dire le corps des fractions de l'algèbre symétrique $\mathbb{C}[V] = S^\bullet(V^\vee)$, ou encore $\mathbb{C}(V) = \mathbb{C}(x_1, \ldots, x_n)$ une fois choisie une base $x_1, \ldots, x_n$ du dual de V) et $\mathbb{C}(V)^G$ le sous-corps de $\mathbb{C}(V)$ formé des éléments invariants par l'action de G qui agit à droite sur $\mathbb{C}(V)$ par $f^\sigma(v) = f(\sigma(v))$ si $\sigma \in G$, $f \in \mathbb{C}(V)$ et $v \in V$. Montrer que $\mathbb{C}(V)^G$ est une extension transcendante pure de $\mathbb{C}$, autrement dit, il existe $y_1, \ldots, y_n \in \mathbb{C}(V)^G$ (nécessairement en nombre n : pourquoi ?) algébriquement indépendants tels que $\mathbb{C}(V)^G = \mathbb{C}(y_1, \ldots, y_n)$. (Indication : se placer sur une base de V qui diagonalise simultanément tous les éléments de G, puis considérer le réseau des monômes sur cette base qui sont invariants par G.)

Montrer par un exemple simple que dans cette situation l'algèbre $\mathbb{C}[V]^G$ (des invariants sous G dans l'algèbre symétrique $\mathbb{C}[V] = S^\bullet(V^\vee)$ des polynômes sur V) n'est pas nécessairement une algèbre de polynômes.

3 (« no-name » lemma). Soit k un corps de caractéristique zéro (on ne suppose pas k algébriquement clos). Soit G un groupe fini et soient V et W deux k-espaces vectoriels (de dimensions respectives m et n, disons) sur lesquels G agit fidèlement et linéairement, c'est-à-dire qu'on se donne des morphismes injectifs de G dans $GL(V)$ et $GL(W)$. On considère les corps d'invariants $k(V)^G$ et $k(W)^G$ (on renvoie à l'exercice 2 pour des explications de ces notations). On se propose de montrer que $k(V)^G$ et $k(W)^G$ sont « stablement équivalents », c'est-à-dire que pour des indéterminées $y_1, \ldots, y_n$ et $x_1, \ldots, x_m$ on a $k(V)^G(y_1, \ldots, y_n) \cong k(W)^G(x_1, \ldots, x_m)$ (comme extensions de corps de k).

Pour cela, on commencera par montrer le lemme suivant (lemme de Speiser) : si L/K est une extension galoisienne finie de groupe G et E un L-espace vectoriel de dimension finie sur lequel est donnée une action de G vérifiant $\sigma(v + w) = \sigma(v) + \sigma(w)$ (si $v, w \in E$) et $\sigma(av) = \sigma(a) \cdot \sigma(v)$ (si $a \in L$ et $v \in E$) (une telle action est dite semi-linéaire par rapport à l'action naturelle de G sur L), et si E^G désigne les invariants de E sous l'action de G alors $E = E^G \otimes_K L$ (comme L-espaces vectoriels munis d'une action de G). (Indication : soit (b_i) une K-base de L et (σ_j) une énumération des éléments de G : rappeler pourquoi la matrice $(\sigma_j(b_i))$ est inversible, et en déduire qu'un élément $v \in E$ donné peut s'écrire comme combinaison linéaire à coefficients dans L des $w_i = \sum_j \sigma_j(b_i v)$; conclure quant à la surjectivité de la flèche naturelle $E^G \otimes_K L \to E$.) En déduire que, toujours sous les hypothèses du lemme, $L(E)^G = K(E^G)$.

Revenant au problème initial, on rappelle que $k(V)^G \subseteq k(V)$ est galoisienne de groupe G : en appliquant deux fois judicieusement le lemme, montrer que $k(V \oplus W)^G$ est une extension transcendante pure à la fois de $k(V)^G$ et de $k(W)^G$, ce qui conclut.

4. On considère le sous-corps $K = \mathbb{R}(x^2 + y^2, x^3 - 3xy^2)$ de $L = \mathbb{R}(x, y)$: montrer que l'extension L/K est galoisienne d'un groupe de Galois G que l'on précisera.

([1]) On rappelle que c'est celle dont les fermés sont les $V(\mathfrak{I})$, lieu des zéros communs d'un idéal $\mathfrak{I} \subseteq K[x_1, \ldots, x_n]$ de polynômes — les équations de ce fermé.

5 (théorème de Hilbert-Noether). Soit k un corps (ou plus généralement un anneau noethérien) et soit $B = k[x_1, \ldots, x_r]$ une algèbre de type fini sur k (ici, $x_1, \ldots, x_r$ ne sont pas supposés être des indéterminées : ils engendrent simplement B). Soit G un groupe fini d'automorphismes de B laissant k invariant (on ne suppose pas que l'action de G provient d'une action linéaire sur certaines indéterminées, et on ne suppose pas non plus que l'ordre de G est inversible dans k). Soit $A = B^G$ la sous-k-algèbre de B formée des éléments invariants par l'action de G : on se propose de montrer que A est une k-algèbre de type fini (et notamment un anneau noethérien).

Pour cela, montrer que B est entier sur A : i.e., tout élément $x \in B$ est racine d'un polynôme P unitaire à coefficients dans A (on écrira explicitement un tel polynôme, en considérant les différents x^σ pour $\sigma \in G$). Mieux : en prenant des polynômes $P_i \in A[t]$ unitaires à coefficients dans A tels que $P_i(x_i) = 0$, témoignant de l'intégralité sur A des générateurs x_i de B, expliquer pourquoi B, puis $A = B^G$, sont des modules de type fini (donc des algèbres finies) sur la sous-k-algèbre C de A engendrée par les coefficients des P_i. Conclure.

Motivations : L'exercice 1 tombe comme un cheveu sur la soupe. Les exercices 2 et 3 sont les résultats élémentaires les plus classiques sur le problème dit de Noether : donnée une représentation V d'un groupe fini G (i.e. une action linéaire de G sur un espace vectoriel V), à quelle condition le corps des invariants $k(V)^G$ du corps des fractions rationnelles sur V est-il « pur » (i.e. transcendant pur), ou, géométriquement, à quelles conditions la variété quotient V/G (si on admet qu'elle a un sens) est-elle rationnelle ? Ce problème est très difficile en toute généralité. L'exercice 2 est dû à E. Fischer, et la démonstration proposée ici est tirée presque telle quelle de son article « Die Isomorphie der Invariantenkörper der endlichen Abel'schen Gruppen linearer Transformationen » (*Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1915, p. 77–80). Il faut noter qu'une hypothèse sur le corps de base (ici $\mathbb{C}$) est nécessaire (essentiellement l'existence d'une racine primitive N-ième de l'unité), puisque des contre-exemples sont connus par exemple pour le groupe $\mathbb{Z}/8\mathbb{Z}$ sur le corps $\mathbb{Q}$. L'exercice 3, auquel Dolgachev (« Rationality of fields of invariants », in *Algebraic Geometry, Bowdoin, 1985*, Proc. Sympos. Pure Math. 46, 2, AMS) donne le nom de « no-name lemma » parce qu'il a été découvert par plusieurs personnes indépendamment, introduit la notion de « rationalité stable », parfois plus approchable que la rationalité : par exemple, on peut conclure de cet exercice que si V est une représentation fidèle du groupe $\mathfrak{S}_n$, le corps des invariants $k(V)^{\mathfrak{S}_n}$ est stablement pur (la pureté pour la représentation fondamentale, $\mathfrak{S}_n$ agissant par permutation sur n indéterminées est donnée par le théorème sur les fonctions symétriques). Pour le lemme intermédiaire, on comparera avec l'exercice 4 du partiel du 2005-04-08. L'exercice 4 tente de donner une vision un peu plus explicite de l'action d'un groupe sur un corps de fractions rationnelles (bon, d'accord, elles sont vraiment pipo, mes motivations). L'exercice 5 généralise de façon pas forcément très utile un résultat du cours (le cas où B est l'algèbre de polynômes sur un espace vectoriel où G agit linéairement).