1 (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 $\mathbb{C}(V) = \mathbb{C}(x_1, \dots, x_n)$ une fois choisie une base $x_1, \dots, x_n$ 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 $y_1, \dots, y_n \in \mathbb{C}(V)^G$ (nécessairement en nombre n : pourquoi ?) algébriquement indépendants tels que $\mathbb{C}(V)^G = \mathbb{C}(y_1, \dots, y_n)$. (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.

Corrigé. Suivant l'indication, considérons une base de V qui diagonalise simultanément tous les éléments de G (ce qui est possible car ceux-ci commutent entre eux et car G est fini). Notons $x_1, \dots, x_n$ la base duale : alors $\mathbb{C}(V) = \mathbb{C}(x_1, \dots, x_n)$ et tout élément de G agit en multipliant chaque x_i par un certain complexe, qui est par ailleurs une racine de l'unité dont l'ordre divise l'exposant N de G. Considérons l'ensemble $L \subseteq \mathbb{Z}^n$ des n-uplets $\ell_1, \dots, \ell_n$ d'entiers relatifs tels que le « monôme » $x_1^{\ell_1} \cdots x_n^{\ell_n}$ soit invariant par G. Ainsi, L est un sous-module de $\mathbb{Z}^n$, dont le rang est n puisqu'il contient $N \cdot \mathbb{Z}^n$ (en effet, x_i^N est G-invariant quel que soit i). On peut donc trouver une base B de L : soient $y_1, \dots, y_n$ les « monômes » $x_1^{\ell_1} \cdots x_n^{\ell_n}$ pour $(\ell_1, \dots, \ell_n)$ un élément de cette base. On va vérifier que $y_1, \dots, y_n$ sont bien algébriquement indépendants et que $\mathbb{C}(V)^G = \mathbb{C}(y_1, \dots, y_n)$.

Tout d'abord, tout « monôme » $x_1^{\ell_1} \cdots x_n^{\ell_n} \in \mathbb{C}(V)^G$ peut s'exprimer comme fraction rationnelle (et même « monôme ») en les y_i, puisque $(\ell_1, \dots, \ell_n) \in L$ peut s'exprimer dans la base B. À présent, un polynôme $f \in \mathbb{C}[x_1, \dots, x_n]$ qui serait invariant par G doit avoir chacun de ses monômes invariants, puisque chacun est multiplié par une constante (une racine N-ième de l'unité) quand on applique un élément $\sigma \in G$: il s'ensuit d'après ce qu'on vient de voir que f est fraction rationnelle de $y_1, \dots, y_n$. Enfin, comme toute fraction rationnelle invariante par G est quotient de deux polynômes invariants par G (en effet, ses numérateurs et dénominateur réduits sont chacun multipliés par une constante quand on fait agir G, mais quitte à les multiplier tous les deux par un monôme approprié on peut supposer qu'ils sont bien invariants par G), on a $\mathbb{C}(V)^G = \mathbb{C}(y_1, \dots, y_n)$. Enfin, comme le degré de transcendance sur $\mathbb{C}$ de $\mathbb{C}(V)^G$ est n (puisque les n quantités $x_1^N, \dots, x_n^N$, par exemple, sont algébriquement indépendantes), on en déduit que $y_1, \dots, y_n$ doivent être algébriquement indépendants, ce qui conclut.

En matière de contre-exemple, prenons $V = \mathbb{C}^2$ sur lequel agit $G = \mathbb{Z}/2\mathbb{Z}$ par symétrie par rapport à l'origine $(z_1, z_2) \mapsto (-z_1, -z_2)$. Alors $\mathbb{C}[V]^G$ est l'algèbre formée des polynômes en x_1, x_2 dont tous les monômes ont un degré total pair (cf. exercice 2(2) de la feuille n°7) : pour montrer que ce n'est pas une algèbre de polynômes on peut invoquer le fait qu'elle n'est pas engendrée par seulement deux éléments, ou tout simplement que $(x_1x_2)^2 = (x_1^2) \cdot (x_2^2)$ alors que chacun des éléments x_1x_2 et x_1^2 et x_2^2 est irréductible. ✓

2 (« 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 1 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 $y_1, \dots, y_n$ et $x_1, \dots, x_m$ on a $k(V)^G(y_1, \dots, y_n) \cong k(W)^G(x_1, \dots, x_m)$ (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.

Corrigé. Montrons d'abord le lemme proposé. Soit donc $b_1, \dots, b_r$ une K-base de L, et soit $\sigma_1, \dots, \sigma_r$ une énumération des éléments de G, avec, disons, $\sigma_1 = \mathrm{id}_L$. L'indépendance linéaire des caractères montre que la matrice $(\sigma_j(b_i))$, matrice $n \times n$ à coefficients dans L, a des colonnes indépendantes (il n'existe pas de relation $\sum_j \lambda_j \sigma_j(b_i) = 0$, où $\lambda_j \in L$, pour tout i), c'est-à-dire qu'elle est inversible. Considérons maintenant $v \in E$ et posons $w_i = \sum_j \sigma_j(b_i v)$ comme suggéré : on a alors manifestement $w_i \in E^G$. Mais par l'hypothèse faite sur l'action de G, on peut réécrire $w_i = \sum_j \sigma_j(b_i)\,\sigma_j(v)$. Puisque la matrice $(\sigma_j(b_i))$ est inversible, ceci nous permet d'exprimer les $\sigma_j(v)$ et notamment $\sigma_1(v) = v$, comme combinaisons linéaires, à coefficients dans L, des w_i. On a donc prouvé que l'application L-linéaire $E^G \otimes_K L \to E$ est surjective. Pour ce qui est de son injectivité, si (e_ℓ) est une K-base de E^G, et si $\sum_\ell a_\ell e_\ell = 0$ (dans E) avec $a_\ell \in L$, on écrit $a_\ell = \sum_i c_{\ell,i} b_i$ où $c_{\ell,i} \in K$, ce qui donne $\sum_{\ell,i} c_{\ell,i} \sigma_j(b_i) e_\ell = 0$ pour tout j donc, toujours par l'inversibilité de la matrice $\sigma_j(b_i)$, $c_{\ell,i} e_\ell = 0$ pour tout i, et par l'indépendance linéaire sur K des e_ℓ, $c_{\ell,i} = 0$ pour tous ℓ, i, soit $a_\ell = 0$ pour tout ℓ, ce qui montre que la L-base $(e_\ell \otimes 1)$ de $E^G \otimes_K L$ s'envoie sur une famille L-linéairement indépendante (e_ℓ) de E, d'où l'injectivité de l'application naturelle. Ceci conclut la démonstration du lemme.

Toujours sous les hypothèses du lemme, en considérant $e_1, \dots, e_s$ une base de E^G et $t_1, \dots, t_s$ sa base duale, on a $K(E^G) = K(t_1, \dots, t_s)$ et le lemme montre que E est le L-espace vectoriel de base $e_1, \dots, e_s$, avec l'action galoisienne naturelle de G, donc $L(E) = L(t_1, \dots, t_s)$ avec l'action galoisienne de G, de sorte que $L(E)^G = K(t_1, \dots, t_s) = K(E^G)$.

Revenant au problème initial, on applique le lemme à l'extension galoisienne $k(V)^G \subseteq k(V)$ galoisienne de groupe G et au $k(V)$-espace vectoriel $k(V) \otimes_k W$: alors le lemme (ou plutôt la remarque qui suit) montre que l'extension $k(V \oplus W)^G = k(V)(W)^G$ est transcendante pure sur $k(V)^G$ (avec, plus précisément, comme base de transcendance la base duale d'une $k(V)^G$-base de $(k(V) \otimes_k W)^G$). Et en échangeant le rôle de V et W elle est transcendante pure sur $k(W)^G$. On a donc bien prouvé l'équivalence stable de $k(V)^G$ et $k(W)^G$ (le nombre de variables à faire intervenir est donné par le degré de transcendance de $k(V \oplus W)^G$ sur $k(V)^G$ ou $k(W)^G$, c'est-à-dire la dimension de W ou V). ✓

3 (théorème de Hilbert-Noether). Soit k un corps (ou plus généralement un anneau noethérien) et soit $B = k[x_1, \dots, x_r]$ une algèbre de type fini sur k (ici, $x_1, \dots, x_r$ 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.

Corrigé. Si $x \in B$, alors x est racine du polynôme P défini par $P(t) = \prod_{\sigma\in G}(t-x^\sigma)$, qui est unitaire et dont les coefficients sont (au signe près) les polynômes symétriques élémentaires en les x^σ donc invariants par G, c'est-à-dire $P \in A[t]$. Donc x est bien entier sur A. En écrivant un tel polynôme P_i pour chaque élément x_i de l'ensemble fini choisi de générateurs de B, on voit que B est un C-module de type fini où C est la sous-k-algèbre de type fini de A engendrée par les coefficients des P_i. Mais C est une k-algèbre de type fini donc noethérienne, donc A, qui est un sous-C-module de B, est lui-aussi un C-module de type fini. Par conséquent, A est une algèbre finie sur une algèbre (C) de type fini sur k donc A est bien une k-algèbre de type fini, comme souhaité. ✓

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.

Corrigé. Considérons l'action du groupe symétrique $\mathfrak{S}_3$ sur $\mathbb{R}^2$ qui permute les vecteurs $(1, 0)$, $(-\frac{1}{2}, \frac{\sqrt{3}}{2})$ et $(-\frac{1}{2}, -\frac{\sqrt{3}}{2})$: ceci a bien un sens car lorsqu'on envoie deux quelconques de ces vecteurs sur deux quelconques d'entre eux, le troisième s'envoie bien sur le troisième vu que la somme des trois est nulle ; ou, si l'on préfère, les éléments de $\mathfrak{S}_3$ s'envoient sur l'identité, ou des symétries, ou des rotations d'angle $\pm\frac{2\pi}{3}$ du plan. Ceci définit bien une représentation fidèle de $\mathfrak{S}_3$ sur $\mathbb{R}^2$ (dite « représentation standard »).

Manifestement, les éléments homogènes $f = x^2 + y^2$ et $g = x^3 - 3xy^2$ qui engendrent K sont laissés invariants par cette action de $\mathfrak{S}_3$ sur $\mathbb{R}^2$ (le cas de f est clair pour des raisons de géométrie plane ; le cas de g peut se voir par exemple en le factorisant comme $g = 4x(-\frac{1}{2}x + \frac{\sqrt{3}}{2}y)(-\frac{1}{2}x - \frac{\sqrt{3}}{2}y)$). On voit d'ailleurs que f et g sont algébriquement indépendants car leur jacobien $2y^3 - 18x^2y$ n'est pas nul. Montrons que $\mathbb{R}(x, y)^{\mathfrak{S}_3}$ est bien engendré par f et g (autrement dit, qu'il n'est pas plus gros que $K = \mathbb{R}(f, g)$). Puisque $\mathfrak{S}_3 \subseteq GL(2, \mathbb{R})$ est engendré par des réflexions, on doit pouvoir écrire $\mathbb{R}[x, y]^{\mathfrak{S}_3}$ comme l'anneau des polynômes sur deux éléments algébriquement indépendants, qui sont ceux de plus petit degré possible, et on voit facilement qu'il n'y a pas d'éléments de $\mathbb{R}[x, y]$ de degré plus petit que f et g qui soient invariants, ou encore que le degré de f et de g (2 et 3) ont bien le produit et la somme attendus (respectivement le cardinal de $\mathfrak{S}_3$ et le nombre de réflexions qu'il contient plus deux). Bref, on a $\mathbb{R}[x, y]^{\mathfrak{S}_3} = \mathbb{R}[f, g]$ ce qui permet de conclure $\mathbb{R}(x, y)^{\mathfrak{S}_3} = K = \mathbb{R}(f, g)$, donc que l'extension L/K est bien galoisienne de groupe de Galois $\mathfrak{S}_3$.

On pouvait aussi calculer le degré de L/K en faisant valoir le fait que pour un point (f, g) général (sur les complexes) il existe six solutions (x, y) de $x^2 + y^2 = f$ et $x^3 - 3xy^2 = g$ (cela peut s'expliquer de diverses manières, mais ce qui joue essentiellement est le fait que le produit des degrés est 6), donc $K = \mathbb{R}(f, g)$ ne peut pas être strictement plus petit que $\mathbb{R}(x, y)^{\mathfrak{S}_3}$ puisque dans les deux cas $\mathbb{R}(x, y)$ est de degré six au-dessus. ✓