1. (a) Soit $K \subseteq L$ une extension galoisienne de groupe de Galois G, et $u\colon G \to L^\times$ une application à valeurs dans le groupe multiplicatif telle que : $u(gh) = u(g)\,g(u(h))$ $(\forall g, h \in G)$. Montrer qu'il existe un élément non nul $v \in L^\times$ tel que : $u(h) = v\,h(v)^{-1}$ $(\forall h \in G)$. (On pourra chercher v sous la forme $v = \sum_{g\in G} u(g)\,g(w)$ pour un $w \in L$ bien choisi.)

(b) On suppose de plus que G est cyclique d'ordre n, engendré par h. Soit $x \in L$ tel que $x\,h(x)\,h^2(x)\cdots h^{n-1}(x) = 1$. Montrer qu'il existe $y \in L$ tel que $x = y\,h(y)^{-1}$.

(c) On revient à la situation du (a) (G n'est pas nécessairement cyclique). Soit $\phi\colon G \to L$ une application telle que $\phi(gh) = \phi(g) + g(\phi(h))$ $(\forall g, h \in G)$. Montrer qu'il existe $c \in L$ tel que $\phi(g) = c - g(c)$ $(\forall g \in G)$. (On pourra montrer qu'il existe w tel que $\sum_{g\in G} g(w) = 1$.)

(d) On suppose à nouveau G cyclique d'ordre n, de générateur h. Soit $x \in L$ tel que $x + h(x) + \cdots + h^{n-1}(x) = 0$. Montrer qu'il existe $z \in L$ tel que $x = z - h(z)$.

(e) On suppose que le corps K est de caractéristique $p \neq 0$ et que $K \subseteq L$ est une extension cyclique de degré p. Montrer qu'il existe $c \in L$ tel que $L = K(c)$ et $c^p - c \in K$.

Corrigé. (a) Suivant la suggestion de l'énoncé, posons $v = \sum_{h\in G} u(h)\,h(w)$, pour un $w \in L$ restant à déterminer. Pour $g \in G$, on a alors $g(v) = \sum_{h\in G} g(u(h))\,g(h(w))$, et d'après la propriété (dite « de cocycle ») vérifiée par u on a $g(u(h)) = u(g)^{-1}\,u(gh)$, donc $g(v) = u(g)^{-1}\sum_{h\in G} u(gh)\,(gh)(w) = u(g)^{-1}\sum_{h\in G} u(h)\,h(w)$, ce qui prouvera $u(g) = v\,g(v)^{-1}$ (comme souhaité) dès lors qu'on aura $v \neq 0$ (et donc $g(v) \neq 0$ pour tout g). Il reste donc à expliquer pourquoi on peut trouver w tel que $\sum_{g\in G} u(g)\,g(w)$ soit non nul ; mais si cette expression était nulle pour tout $w \in L$, l'indépendance linéaire des caractères (théorème de Dirichlet) montrerait que $u(g) = 0$ (pour tout g) ce qui est contraire à l'hypothèse.

(b) On va définir un $u\colon G \to L^\times$ vérifiant les hypothèses de la question (a). Précisément, on pose, pour k entre 0 et $n-1$, $u(h^k) = x\,h(x)\cdots h^{k-1}(x)$ (ce produit est non nul, puisque manifestement $x \neq 0$). On vérifie aisément, d'après l'hypothèse faite sur x, que u vérifie la condition « de cocycle », $u(gg') = u(g)\,g(u(g'))$. La conclusion de la question (a) permet d'affirmer qu'il existe $y \in L^\times$ tel que $x = u(h) = y\,h(y)^{-1}$, ce qu'on voulait.

(c) Montrons d'abord qu'il existe un $w \in L$ tel que $\sum_{g\in G} g(w) = 1$: cela découle de nouveau de l'indépendance linéaire des caractères, puisqu'on ne peut pas avoir $\sum_{g\in G} g(w) = 0$ pour tout $w \in L$, donc il doit exister w avec $\mathrm{tr}(w) := \sum_{g\in G} g(w) \neq 0$, et cette quantité $\mathrm{tr}(w)$ est dans K (car invariante par tout élément de G), et quitte à diviser w par elle on est ramené à $\sum_{g\in G} g(w) = 1$. Posons maintenant $c = \sum_{h\in G} \phi(h)\,h(w)$: on a alors, en raisonnant de façon analogue à la question (a), $g(c) = -\phi(g)\sum_{h\in G} h(w) + \sum_{h\in G} \phi(gh)\,(gh)(w) = -\phi(g) + c$, donc $\phi(g) = c - g(c)$ comme annoncé.

(d) Le raisonnement est rigoureusement analogue à la question (b). On définit un $\phi\colon G \to L$ vérifiant les hypothèses de la question (c). Précisément, on pose, pour k entre 0 et $n-1$, $\phi(h^k) = x + h(x) + \cdots + h^{k-1}(x)$. On vérifie aisément, d'après l'hypothèse faite sur x, que u vérifie la condition « de cocycle », $\phi(gg') = \phi(g) + g(\phi(g'))$. La conclusion de la question (c) permet d'affirmer qu'il existe $z \in L$ tel que $x = \phi(h) = z - h(z)$, ce qu'on voulait.

(e) Soit h un générateur du groupe de Galois G de L sur K, supposé cyclique d'ordre p. La conclusion de la question (d) appliquée à $x = 1$ (qui vérifie manifestement l'hypothèse de cette question, $n = 0$ dans L) permet d'affirmer qu'il existe $c \in L$ tel que $c - h(c) = 1$. Dans ces conditions, on a $c^p - h(c^p) = (c - h(c))^p = 1$ puisque L est de caractéristique p, soit $h(c^p - c) = c^p - c$, donc $c^p - c \in K$. D'autre part, manifestement $c \notin K$ (étant donné que $h(c) \neq c$), et l'extension $K(c)$ de K, contenue dans L et de degré > 1 sur K, ne peut donc être que L. Ceci termine la démonstration.

Note : Le résultat de la question (a) (ou au moins, pour être historiquement plus précis, celui de la question (b)) est connu sous le nom de « théorème 90 » de Hilbert : en termes sophistiqués, il exprime l'annulation du groupe $H^1(G, L^\times)$ de cohomologie galoisienne, tandis que la question (c) concerne l'annulation du $H^1(G, L)$. Le résultat de la question (e) est

généralement connu sous le nom de théorème d'Artin-Schreier (et il est à mettre en parallèle avec le fait, formalisé par Kummer, que si L/K est une extension cyclique de degré n ne divisant pas la caractéristique et si K contient une racine primitive n-ième de l'unité, alors L s'obtient en extrayant une racine n-ième sur K). ✓

2. Déterminer le groupe de Galois du polynôme $X^4 + 2X^2 + X + 3$. (On pourra réduire modulo 2, 3 et 5.)

Corrigé. En réduisant modulo 2 on trouve le polynôme $X^4 + X + 1$, qui est irréductible (car il n'a aucune racine dans $\mathbb{F}_4$ comme on le vérifie immédiatement) donc le polynôme $X^4 + 2X^2 + X + 3$ est lui-même irréductible. En réduisant modulo 3 on trouve le polynôme $X^4 - X^2 + X$ sur $\mathbb{F}_3$, qui se factorise comme $X(X^3 - X + 1)$ avec deux facteurs irréductibles (car il n'y a pas d'autre racine), donc il existe un élément d'ordre 3 dans le groupe de Galois qui permute cycliquement les trois racines de $X^3 - X + 1$ modulo 3. En réduisant modulo 5 on trouve $X^4 + 2X^2 + X - 2 = (X + 1)(X + 2)(X^2 + 2X - 1)$, donc il existe un élément d'ordre 2 qui échange les deux racines de $X^2 + 2X - 1$. Le groupe de Galois est un sous-groupe de $\mathfrak{S}_4$ qui agit transitivement sur les quatre racines et contient une transposition et un 3-cycle, donc c'est $\mathfrak{S}_4$ tout entier. ✓

3. 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 $k[x_1, \dots, x_n]^G$ 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 $\{1, \dots, n\}$.

Reste à trouver explicitement un système basique d'invariants. Notons $\Psi_1, \dots, \Psi_n$ les fonctions symétriques élémentaires non pas sur les coordonnées $x_1, \dots, x_n$ elles-mêmes mais sur leurs carrés $x_1^2, \dots, x_n^2$: 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 $x_1^2, \dots, x_n^2$ est l'algèbre $k[x_1, \dots, x_n]^{(\mathbb{Z}/2\mathbb{Z})^n}$ des polynômes (en $x_1, \dots, x_n$) invariants par changement de signe sur un nombre quelconque de coordonnées, et que par conséquent l'algèbre de polynômes engendrée par $\Psi_1, \dots, \Psi_n$ est l'algèbre $k[x_1, \dots, x_n]^{G'}$ 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 $k[x_1, \dots, x_n]^{G'} \subseteq k[x_1, \dots, x_n]^G$, et on va montrer que $k[x_1, \dots, x_n]^G = k[\Psi_1, \dots, \Psi_{n-1}, \Sigma_n]$. Comme chaque Ψ_i, et aussi Σ_n, sont invariants par G, une inclusion est claire.

Si $f \in k[x_1, \dots, x_n]^G$ (autrement dit, si f est un polynôme en $x_1, \dots, x_n$ 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 $k[x_1, \dots, x_n]^G$; on peut les appeler partie paire et partie impaire de f respectivement. La première est dans $k[x_1, \dots, x_n]^{G'}$; 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 $k[x_1, \dots, x_n]^{G'}$. On a ainsi montré que tout élément f de $k[x_1, \dots, x_n]^G$ s'écrit de façon unique comme $f_+ + h\Sigma_n$ avec f_+ et h dans $k[x_1, \dots, x_n]^{G'}$ (et, qui plus est, uniquement définis : si on préfère, $k[x_1, \dots, x_n]^G$ est un module libre de rang 2 sur $k[x_1, \dots, x_n]^{G'}$ avec pour base $\{1, \Sigma_n\}$). Puisque $k[x_1, \dots, x_n]^{G'} = k[\Psi_1, \dots, \Psi_n]$ (et comme $\Psi_n = \Sigma_n^2$), on en déduit $k[x_1, \dots, x_n]^G = k[\Psi_1, \dots, \Psi_{n-1}, \Sigma_n]$, ce qui répond à la question posée (on a trouvé n générateurs de l'algèbre intègre $k[x_1, \dots, x_n]^G$ dont le corps des fractions $k(x_1, \dots, x_n)^G$ est de degré de transcendance n, donc ces générateurs sont bien algébriquement indépendants sur k).

On peut vérifier que le produit des degrés de $\Psi_1, \dots, \Psi_{n-1}, \Sigma_n$ 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 $x_i = -x_j$). ✓

4. Soit A un anneau commutatif, I un idéal de A contenu dans le radical de Jacobson et M un A-module de type fini. Montrer que si $m_1, \dots, m_n \in M$ sont tels que leurs images dans M/IM engendrent M/IM, alors ils engendrent M.

L'hypothèse que M est de type fini est-elle nécessaire ?

Corrigé. Posons $\tilde{M} = M/IM$ (si on préfère, $\tilde{M} = M \otimes_A (A/I)$). Pour $i = 1, \dots, n$, notons $\tilde{m}_i \in \tilde{M}$ la classe de $\tilde{m}_i$ modulo IM. Par hypothèse, la famille $\tilde{m}_1, \dots, \tilde{m}_n$ engendre $\tilde{M}$. Soit maintenant M' le sous-A-module de M engendré par $m_1, \dots, m_n$: on veut montrer que $M' = M$. Soit $N = M/M'$ le module quotient. Manifestement N est un A-module de type fini (comme quotient du A-module de type fini M), et on a $N = IN$ puisque tout élément $\bar{n} \in N$ provient d'un élément $n \in M$ qui a une réduction $\tilde{n} \in \tilde{M}$ qui est combinaison linéaire des $\tilde{m}_i$ donc quitte à modifier n par la même combinaison linéaire des m_i (ce qui ne change pas la classe $\bar{n} \in N$) on peut supposer $\tilde{n} = 0$ c'est-à-dire $n \in IM$ et donc $\bar{n} \in IN$. Le lemme de Nakayama (puisque $N = IN$ avec I inclus dans le radical de Jacobson et N de type fini) donne alors $N = 0$, ce qui signifie exactement $M' = M$ comme souhaité.

La conclusion ne vaut plus si M n'est pas supposé de type fini. Par exemple, soit k un corps et soit A (également noté $k[x]_{(x)}$) le sous-anneau de $k(x)$ formé des fractions rationnelles n'ayant pas de pôle en 0 (c'est-à-dire, dont le dénominateur réduit n'appartient pas à l'idéal premier (x) de $k[x]$). Manifestement, A est un anneau local, c'est-à-dire qu'il n'a qu'un seul idéal maximal, en l'occurrence celui engendré par x (tout élément de A qui n'est pas multiple de x est inversible dans A) : le radical de Jacobson de A est donc $I = (x)$. Soit enfin pour M le corps $k(x)$ tout entier, considéré comme A-module par le plongement naturel : certainement M n'est pas nul. Pourtant, $IM = M$ puisque x n'est pas nul dans le corps $k(x)$ donc la multiplication par lui est bijective. Ceci fournit un contre-exemple au lemme de Nakayama, et aussi à l'affirmation de l'exercice (avec $n = 0$: dire qu'un module est engendré par zéro éléments signifie qu'il est nul) en retirant l'hypothèse que M est de type fini. ✓

5. Soit k un corps, $V \subseteq k^n$ et $W \subseteq k^m$ des variétés non vides. On désigne par $A(V)$ et $A(W)$ les algèbres de fonctions polynomiales sur V et W, et par $I(V) \subseteq k[X_1, \dots, X_n]$ et $I(W) \subseteq k[Y_1, \dots, Y_m]$ les idéaux annulateurs.

(a) Montrer que $V \times W \subseteq k^{n+m}$ est une variété, et que l'application naturelle donnée par le produit des fonctions détermine un morphisme d'algèbres $A(V) \otimes_k A(W) \to A(V \times W)$.

(b) On suppose que V et W sont irréductibles. Montrer que $V \times W$ est irréductible.

(c) Montrer que l'idéal $(I(V), I(W))$ de $k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$, engendré par $I(V)$ et $I(W)$ est l'idéal annulateur de $V \times W$ et que $A(V) \otimes_k A(W) \to A(V \times W)$ est un isomorphisme.

Corrigé. (a) Puisque V est un fermé de Zariski, on peut écrire $V = \{(x_1, \ldots, x_n) \in k^n : (\forall f \in I(V))\ f(x_1, \ldots, x_n) = 0\}$ et de façon analogue pour W. Alors $V \times W$ est l'ensemble des $(x_1, \ldots, x_n, y_1, \ldots, y_m) \in k^{n+m}$ tels que $f(x_1, \ldots, x_n) = 0$ pour tout $f \in I(V)$ (qu'on peut voir comme élément de $k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ ne dépendant pas des y_j) et $g(y_1, \ldots, y_m) = 0$ pour tout $g \in I(W)$. Ceci montre encore que $V \times W$ est la variété définie dans k^{n+m} par l'idéal $(I(V), I(W))$ engendré par $I(V)$ et $I(W)$ dans $k[\underline{X}, \underline{Y}]$ (on a ainsi abrégé $k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$).

En particulier, $I(V \times W) \supseteq (I(V), I(W))$ (pour l'inclusion réciproque, voir la question (c)), et il y a donc une application naturelle surjective (réduction) de $k[\underline{X}, \underline{Y}]/(I(V), I(W))$ vers $A(X \times Y) = k[\underline{X}, \underline{Y}]/I(V \times W)$. Par ailleurs, le produit entre $A(V) = k[\underline{X}]/I(V)$ et $A(W) = k[\underline{Y}]/I(W)$ définit (par le théorème chinois) un isormorphisme entre $A(V) \otimes_k A(W)$ et $k[\underline{X}, \underline{Y}]/(I(V), I(W))$. En composant ces deux morphismes, on a donc un morphisme (surjectif) $A(V) \otimes_k A(W) \to A(V \times W)$ donné par la multiplication.

(b) Constatons d'abord le fait suivant : si Z est un fermé de Zariski dans $V \times W$, alors l'ensemble $Z^\forall$ des $\underline{x} \in V$ tels que $(\underline{x}, \underline{y}) \in Z$ pour tout $\underline{y} \in W$ est un fermé de Zariski de V (dit autrement, l'application de projection sur la première coordonnée $V \times W \to V$ est une application *ouverte*). C'est clair car $Z^\forall$ peut se définir comme l'ensemble des $\underline{x} \in k^n$ tels que $f(\underline{x}, \underline{y}) = 0$ pour tout $\underline{y} \in W$, et pour chaque $\underline{y} \in W$ donné ceci définit un fermé $Z^{\underline{y}}$ de V, et on prend l'intersection de tous ces fermés. Supposons maintenant que Z et Z' soient deux fermés de Zariski stricts de $V \times W$, où V et W sont supposés irréductibles : dire que $Z \neq V \times W$ signifie exactement $Z^\forall \neq V$, et de même $Z'^\forall \neq V$; comme ce sont deux fermés de Zariski (d'après la remarque qu'on vient de faire), leur réunion n'est pas V tout entier (ce dernier étant irréductible), donc il existe $\underline{x} \in V$ non contenu dans $Z^\forall$ ni dans $Z'^\forall$, et alors les fermés de Zariski $Z_{\underline{x}} = \{\underline{y} \in W : (\underline{x}, \underline{y}) \in Z\}$ et $Z'_{\underline{x}}$ (défini de façon analogue) de W ne sont pas W tout entier, donc leur réunion n'est pas W tout entier (ce dernier étant irréductible), et si $\underline{y}$ n'est pas dans cette réunion, alors le couple $(\underline{x}, \underline{y})$ n'est pas dans $Z \cup Z'$. On a donc prouvé l'irréductibilité de $V \times W$.

(c) Comme on l'a signalé en (a), l'idéal annulateur $I(V \times W)$ contient au moins l'idéal $(I(V), I(W))$ engendré par $I(V)$ et $I(W)$ dans $k[\underline{X}, \underline{Y}]$. Considérons maintenant $f \in I(V \times W) \subseteq k[\underline{X}, \underline{Y}]$. On en déduit un élément $\bar{f}$ de $A(V)[\underline{Y}]$. Notons $b_1, \ldots, b_s$ une k-base de $A(V)$ ou du moins du sous-k-espace vectoriel engendré dans celui-ci par les coefficients de $\bar{f} \in A(V)[\underline{Y}]$, et écrivons $\bar{f} = b_1 f_1 + \cdots + b_s f_s$ avec $f_1, \ldots, f_s \in k[\underline{Y}]$ (uniquement déterminés). Vu dans $A(V)$ on a $\bar{f}(\underline{y}) = 0$ pour tout $\underline{y} \in W$, donc $b_1 f_1(\underline{y}) + \cdots + b_s f_s(\underline{y}) = 0$, d'où il résulte $f_i(\underline{y}) = 0$ pour tout i, ce qui donne $f_i \in I(W)$. Comme alors la différence $f - (b_1 f_1 + \cdots + b_s f_s)$ a une image nulle dans $A(V)[\underline{Y}]$, chacun de ses coefficients (dans les variables Y) est un élément de $I(V)$. En mettant tout cela ensemble, on a bien prouvé $f \in (I(V), I(W))$, et, le choix de f étant arbitraire, $I(V \times W) = (I(V), I(W))$. D'après ce qui a déjà été dit, $A(V) \otimes_k A(W) \to A(V \times W)$ est alors un isomorphisme. ✓