1. Les questions suivantes sont indépendantes.

(a) Soit V un espace vectoriel de dimension finie, et V_1 et V_2 des sous-espaces de V. Montrer que les algèbres extérieures satisfont à : $\wedge(V_1 \cap V_2) = \wedge(V_1) \cap \wedge(V_2)$.

(b) Soit u un endomorphisme d'un espace vectoriel V de dimension finie n et p un entier $0 \leq p \leq n$. Montrer que $\det(\wedge^p u) = (\det(u))^{C_{n-1}^{p-1}}$. (On pourra commencer par le cas où u est triangulaire supérieur dans une base convenable, puis utiliser un système de générateurs de $GL(V)$.)

Corrigé. (a) Tout d'abord, observons que si W est un sous-espace vectoriel de V alors les algèbres extérieures satisfont naturellement $\wedge(W) \subseteq \wedge(V)$: cela peut se voir par exemple par l'inclusion correspondante sur les algèbres tensorielles, qui passe au quotient, mais pour démontrer la suite il vaut mieux compléter une base de W en une base de V, ce qui donne des bases explicites de $\wedge(W)$ et de $\wedge(V)$ avec inclusion de l'une dans l'autre. Précisément, si $e_1, \ldots, e_m$ est une base de W et $e_1, \ldots, e_n$ (avec $n = \dim V \geq \dim W = m$) une base de V alors les $e_{i_1} \wedge \cdots \wedge e_{i_r}$ où $1 \leq i_1 < \cdots < i_r \leq n$ forment une base de $\wedge(V)$ dont le sous-ensemble où $i_r \leq m$ est une base de $\wedge(W)$.

Cela donne un sens à $\wedge(V_1) \cap \wedge(V_2)$ (les deux $\wedge(V_i)$ étant vues dans $\wedge(V)$) et on en déduit également que $\wedge(V_1 \cap V_2) \subseteq \wedge(V_i)$ pour $i = 1, 2$ et donc $\wedge(V_1 \cap V_2) \subseteq \wedge(V_1) \cap \wedge(V_2)$.

Reste à expliquer l'inclusion réciproque : on utilise la description donnée ci-dessus en termes de bases. Par exemple, si on part d'une base de $V_1 \cap V_2$, qu'on complète en une base de V_1 puis en une base de V_2, la réunion desquelles donne une base de $V_1 + V_2 \subseteq V$ qu'on peut encore compléter en une base de V, on obtient une base $e_1, \ldots, e_n$ de V et deux parties I_1 et I_2 de $\{1, \ldots, n\}$ telles que $(e_i)_{i \in I_1}$ soit une base de V_1 et $(e_i)_{i \in I_2}$ de V_2. Dans ces conditions, les $e_{i_1} \wedge \cdots \wedge e_{i_r}$ (avec $1 \leq i_1 < \cdots < i_r \leq n$) forment une base de $\wedge(V)$ dont le sous-ensemble où tous les i_j sont dans I_1 (resp. I_2) est une base de $\wedge(V_1)$ (resp. $\wedge(V_2)$) : et de même le sous-ensemble où tous les i_j sont dans $I_1 \cap I_2$ est une base de $\wedge(V_1 \cap V_2)$ qui est donc égal à $\wedge(V_1) \cap \wedge(V_2)$.

(b) Comme le déterminant et les puissances extérieures ne dépendent pas du corps de définition sur lequel on les calcule (ils commutent à l'extension des scalaires), on peut supposer le corps de base algébriquement clos. On peut alors considérer $e_1, \ldots, e_n$ une base de V sur laquelle la matrice de u est triangulaire supérieure, c'est-à-dire que $u(e_i) = \lambda_i e_i + (\cdots)$ où l'expression omise $(\cdots)$ ne fait intervenir que les e_j avec $j < i$, et $\det(u)$ est égal au produit $\prod_i \lambda_i$ des coefficients diagonaux. Les $e_{i_1} \wedge \cdots \wedge e_{i_p}$ (avec $1 \leq i_1 < \cdots < i_p \leq n$) forment une base de $\wedge(V)$: ordonnons-la par l'ordre lexicographique qui donne à i_p le plus de poids[1]. Il est alors facile de voir en développant et en utilisant la multilinéarité (alternée) que $u(e_{i_1}) \wedge \cdots \wedge u(e_{i_p}) = \lambda_{i_1} \cdots \lambda_{i_p}\, e_{i_1} \wedge \cdots \wedge e_{i_p} + (\cdots)$ (toujours en omettant des termes antérieurs sur la base), c'est-à-dire que $\wedge^p u$ a dans cette base une matrice triangulaire supérieure, dont le produit des termes diagonaux est $\prod_{i_\bullet} (\lambda_{i_1} \cdots \lambda_{i_p})$, c'est-à-dire le produit de tous les λ_i, chacun apparaissant autant de fois qu'il y a de parties de cardinal p de $\{1, \ldots, n\}$ contenant i, soit C_{n-1}^{p-1}. On a donc bien $\det(\wedge^p u) = (\det(u))^{C_{n-1}^{p-1}}$. ✓

2. (a) Soit K le sous-corps de $\mathbb{C}$ engendré par les racines du polynôme $X^3 - 2$. Montrer que l'extension $\mathbb{Q} \subseteq K$ est galoisienne et déterminer son groupe de Galois.

(b) Montrer que $\sqrt[3]{2}$ n'est pas combinaison linéaire à coefficients rationnels de racines de l'unité.

([1]) C'est-à-dire : le p-uplet $(i_1, \ldots, i_p)$ où $1 \leq i_1 < \cdots < i_p \leq n$ vient avant $(i'_1, \ldots, i'_p)$ vérifiant la même condition lorsqu'on a $i_j < i'_j$ où j est le plus *grand* indice tel que $i_j \neq i'_j$.

Corrigé. (a) Le corps K est le corps de décomposition du polynôme X^3-2 : il est donc normal sur $\mathbb{Q}$, et séparable car $\mathbb{Q}$ est de caractéristique nulle. L'extension est donc galoisienne. Son groupe de Galois est un sous-groupe de $\mathfrak{S}_3$ qui agit sur les trois racines de X^3-2 et cette action est transitive (aucune racine n'est rationnelle) : c'est donc soit $\mathbb{Z}/3\mathbb{Z}$ (agissant par permutation cyclique) soit $\mathfrak{S}_3$ tout entier. Mais la première possibilité est exclue car la combinaison complexe, qui laisse fixe une des racines cubiques de 2 et échange les deux autres, fournit un élément d'ordre 2 du groupe de Galois. Le groupe de Galois est donc $\mathfrak{S}_3$.

(b) Si $\sqrt[3]{2}$ était combinaison linéaire à coefficients rationnels de racines de l'unité, le corps $K=\mathbb{Q}(j,\sqrt[3]{2})$ serait inclus dans le corps $\mathbb{Q}(\zeta_N)$ engendré par une racine N-ième ζ_N de l'unité avec N suffisamment grand (c'est-à-dire suffisamment divisible). Or $\mathbb{Q}(\zeta_N)$ est galoisienne sur $\mathbb{Q}$ avec groupe de Galois $(\mathbb{Z}/N\mathbb{Z})^\times$: eu égard à ce qui a été démontré en (a), ceci impliquerait que $\mathfrak{S}_3$ serait un quotient du groupe abélien $(\mathbb{Z}/N\mathbb{Z})^\times$, donc lui-même abélien, et ceci n'est manifestement pas le cas. ✓

3. Soient $p_1,\dots,p_n$ des nombres premiers distincts.

(a) Montrer les deux propriétés :

(i) Le corps $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ est de degré 2^n sur $\mathbb{Q}$.

(ii) Un élément $x\in\mathbb{Q}$ est un carré dans $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ si et seulement si il existe une partie $I\subseteq\{1,\dots,n\}$ telle que $x\prod_{i\in I}p_i$ est un carré dans $\mathbb{Q}$.

(On pourra procéder par récurrence sur n : montrer que (ii) se déduit de (i), et que l'assertion (i) au rang $n+1$ se déduit de (i) et (ii) au rang n.)

(b) Montrer que l'extension $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ est galoisienne et calculer son groupe de Galois.

Corrigé. (a) On procède par récurrence sur n. Pour $n=0$, les deux affirmations sont triviales. Supposons-les vraies au rang n et cherchons à les prouver au rang $n+1$. Montrons d'abord que l'extension $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{n+1}})$ de $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ est de degré 2 (avec pour base $1,\sqrt{p_{n+1}}$) : il s'agit pour cela de prouver que p_{n+1} n'est pas un carré dans $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ — or cela résulte de l'affirmation (ii) au rang n (puisque p_{n+1} est distinct de tous les autres p_i donc aucun produit de p_i avec $i\leq n$ par p_{n+1} ne peut être un carré rationnel vu qu'il a une valuation p_{n+1}-adique égale à 1). On voit alors que $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{n+1}})$ est de degré 2 sur un corps $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ qui est lui-même (par hypothèse de récurrence) de degré 2^n sur $\mathbb{Q}$, d'où l'affirmation (i) au rang $n+1$. Prouvons maintenant (ii) au rang $n+1$. La partie « si » est claire sans aucune récurrence (si $x\prod_{i\in I}p_i=a^2$ alors x s'écrit comme le carré du produit d'un rationnel $a/\prod_{i\in I}p_i$ par $\prod_{i\in I}\sqrt{p_i}$, donc un carré dans $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{n+1}})$). Quant à la partie « seulement si », remarquons que tout élément de $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{n+1}})$ s'écrit de façon unique (vu ce qu'on a déjà prouvé) comme $\alpha+\beta\sqrt{p_{n+1}}$ où $\alpha,\beta\in\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$: son carré est alors $(\alpha^2+p_{n+1}\beta^2)+2\alpha\beta\sqrt{p_{n+1}}$: si ce carré est un rationnel x, on doit avoir $2\alpha\beta=0$ donc soit $\alpha=0$ soit $\beta=0$, et alors $x=\alpha^2$ ou $x=p_{n+1}\beta^2$: dans le premier cas, x est le carré d'un élément de $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ et l'hypothèse de récurrence s'applique et dans le second, $p_{n+1}x$ est le carré d'un élément de $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ et de nouveau on applique l'hypothèse de récurrence. Ceci conclut la récurrence.

(b) Le point essentiel est que $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{n+1}})=\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})\,\mathbb{Q}(\sqrt{p_{n+1}})$, les deux corps $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ et $\mathbb{Q}(\sqrt{p_{n+1}})$ ayant pour intersection $\mathbb{Q}$. On démontre alors par une récurrence immédiate sur n que $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{n+1}})$ est galoisien sur $\mathbb{Q}$ de groupe de Galois $(\mathbb{Z}/2\mathbb{Z})^n\times\mathrm{Gal}(\mathbb{Q}(\sqrt{p_{n+1}})/\mathbb{Q})$ soit $(\mathbb{Z}/2\mathbb{Z})^{n+1}$.

Ainsi, $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ est galoisien sur $\mathbb{Q}$ de groupe de Galois $(\mathbb{Z}/2\mathbb{Z})^n$, les éléments du groupe de Galois étant donnés par σ_ε: $\sqrt{p_i}\mapsto\varepsilon_i\sqrt{p_i}$ où $\varepsilon\in\{\pm1\}^{\{1,\dots,n\}}$ est un choix de signes. ✓

4. Soit $K \subseteq L$ une extension galoisienne et $G = \mathrm{Gal}(L/K)$ son groupe de Galois. On note $G = \{\sigma_1, \ldots, \sigma_n\}$.

(1) Soit $\theta\colon L \to L^n$ l'application définie par $\theta(b) = (\sigma_1(b), \ldots, \sigma_n(b))$. Montrer que l'image de θ engendre L^n comme L-espace vectoriel.

(2) Montrer qu'il existe des éléments a_i et b_i de L ($1 \leq i \leq n$) tels que : $\sum_{i=1}^n a_i b_i = 1$ et $\sum_{i=1}^n a_i \sigma(b_i) = 0$ pour $\sigma \in G \setminus \{\mathrm{id}\}$.

(3) Montrer que le polynôme

$$D(X_1, \ldots, X_n) = \det\left(\sum_{p=1}^{n} X_p \sigma_i^{-1}(\sigma_j(b_p))\right)_{1 \leq i,j \leq n}$$

n'est pas le polynôme nul.

(4) On suppose que K est un corps infini. Montrer qu'il existe $a \in L$ tel que les éléments $\sigma_i(a)$ ($1 \leq i \leq n$) forment une base du K-espace vectoriel L.

Corrigé. (1) Soit $b_1, \ldots, b_n$ une K-base de L (notons que son cardinal est forcément n puisque $[L : K] = \mathrm{card}\, G = n$). Prouvons que $\theta(b_1), \ldots, \theta(b_n)$ est une L-base de L^n (ce qui montrera en particulier qu'elle l'engendre). Or ceci signifie que la matrice $\sigma_j(b_i)$ (matrice $n \times n$ à coefficients dans L) a des lignes indépendantes, et ceci se produit exactement lorsque ses colonnes le sont : il s'agit donc de prouver qu'il n'existe pas de relation $\sum_j \lambda_j\, \sigma_j(b_i) = 0$ (où $\lambda_j \in L$) pour tout i. Mais ceci découle du théorème de Dirichlet sur l'indépendance linéaire des caractères (les σ_j, étant des éléments distincts du groupe de Galois, sont L-linéairement indépendants vus comme fonctions $L \to L$) vu que $\sum_j \lambda_j\, \sigma_j(b_i) = 0$ pour tout i implique $\sum_j \lambda_j\, \sigma_j(b) = 0$ pour tout $b \in L$.

(2) On vient d'expliquer que $\theta(b_1), \ldots, \theta(b_n)$ est une L-base de L^n (où $b_1, \ldots, b_n$ est une K-base quelconque de L). Il existe donc des coefficients $a_1, \ldots, a_n$ dans L tels que $a_1\, \theta(b_1) + \cdots + a_n\, \theta(b_n) = (1, 0, 0, \ldots, 0)$ où en écrivant $(1, 0, 0, \ldots, 0)$ on a supposé que l'indice j pour lequel σ_j est l'identité (l'élément neutre de G) est le premier. Cette relation signifie précisément $\sum_i a_i b_i = 1$ et $\sum_i a_i\, \sigma(b_j) = 0$ pour tout $\sigma \neq \mathrm{id}$ dans G.

(3) A priori on a $D(X_1, \ldots, X_n) \in L[X_1, \ldots, X_n]$. Les propriétés démontrées en (2) assurent exactement que $D(a_1, \ldots, a_n)$ est le déterminant de la matrice identité, donc $D(a_1, \ldots, a_n) = 1$. En particulier, $D(X_1, \ldots, X_n)$ n'est pas le polynôme nul.

(4) Si K est infini, le polynôme $D(X_1, \ldots, X_n)$ ne peut pas[2] valoir identiquement zéro sur K^n. Il existe donc $\lambda_1, \ldots, \lambda_n \in K$ tels que $D(\lambda_1, \ldots, \lambda_n) \neq 0$. C'est-à-dire que la matrice $\left(\sum_{p=1}^n \lambda_p \sigma_i^{-1}(\sigma_j(b_p))\right)_{1 \leq i,j \leq n}$ est inversible, autrement dit $\left(\sigma_i^{-1}(\sigma_j(a))\right)_{1 \leq i,j \leq n}$ où on a posé $a = \sum_p \lambda_p b_p$. Or une relation de dépendance K-linéaire entre les $\sigma_i(a)$ donnerait une relation de dépendance linéaire entre les colonnes (ou les lignes) de cette matrice $\left(\sigma_i^{-1}(\sigma_j(a))\right)_{1 \leq i,j \leq n}$: c'est impossible, donc les $\sigma_1(a), \ldots, \sigma_n(a)$ sont K-linéairement indépendants, et sont donc une K-base de L. ✓

([2]) Rappelons brièvement pourquoi, par récurrence sur n, un $D \in L[X_1, \ldots, X_n]$ ne peut pas être identiquement nul sur K^n sauf à être le polynôme nul. Pour $n = 0$ c'est une trivialité, et pour $n = 1$, c'est le fait qu'un polynôme en une seule variable n'a qu'un nombre fini de zéros sur un corps (commutatif). Pour $n \geq 1$, par le cas $n = 1$, il existe une valeur $a \in K$ telle que le polynôme $D(X_1, \ldots, X_{n-1}, a)$ ne soit pas le polynôme nul (par exemple parce que $D \in L(X_1, \ldots, X_{n-1})[X_n]$ n'est pas le polynôme nul) : l'hypothèse de récurrence permet alors de conclure.