1. Les questions suivantes sont indépendantes.

(a) Soit V un espace vectoriel de dimension finie sur un corps k, $f\colon V^{n-1} \to k$ une application $(n-1)$-linéaire alternée. Montrer que si $x_1, \dots, x_n \in V$ sont tels que $x_1 \wedge \cdots \wedge x_n = 0$ alors :

$$\sum_{j=1}^{j=n} (-1)^j f(x_1, \dots, \widehat{x_j}, \dots, x_n)\, x_j = 0$$

(l'expression $\widehat{x_j}$ signifie que x_j a été omis).

[**Erreur dans l'énoncé :** La question avait été posée avec l'expression sans le x_j, soit : $\sum_{j=1}^{j=n} (-1)^j f(x_1, \dots, \widehat{x_j}, \dots, x_n) = 0$.]

(b) Soit u un endomorphisme d'un espace vectoriel V de dimension finie n, de matrice X dans une base fixée de V. Si p est un entier $1 \leq p \leq n-1$ et H, R des parties de $\{1, \dots, n\}$ à p éléments, on désigne par $X_{H,R}$ la matrice extraite de X où l'on a gardé les lignes indexées par H et les colonnes indexées par R. On désigne par H' et R' les parties complémentaires de H et R dans $\{1, \dots, n\}$. On note enfin $\rho_{H,H'} = (-1)^\nu$, où ν est le nombre de couples $(i, j) \in H \times H'$ tels que $i > j$.

On fixe une partie H à p éléments comme ci-dessus. Montrer que :

$$\det(X) = \rho_{H,H'} \sum \rho_{R,R'} \det(X_{R,H}) \det(X_{R',H'})$$

où la somme est étendue à toutes les parties à p éléments.

Corrigé. (a) Montrons que l'application ∂f (manifestement) n-linéaire définie par $\partial f\colon (x_1, \dots, x_n) \mapsto \sum_{j=1}^{j=n} (-1)^j f(x_1, \dots, \widehat{x_j}, \dots, x_n)\, x_j$ est alternée : pour cela, il suffit de supposer que $x_{i_1} = x_{i_2}$ pour deux indices i_1, i_2 distincts, mettons $i_1 < i_2$ et montrer que dans ce cas $\sum_{j=1}^{j=n} (-1)^j f(x_1, \dots, \widehat{x_j}, \dots, x_n)\, x_j = 0$. Or les termes pour lesquels $j \notin \{i_1, i_2\}$ sont nuls car f est alternée, et le terme $j = i_1$ compense le terme $j = i_2$ (la signature du cycle $(i_1\ i_1+1\ \cdots\ i_2-1)$ est $(-1)^{i_2-i_1+1}$). Ainsi, on a bien définie ∂f une application n-linéaire alternée. Et l'hypothèse $x_1 \wedge \cdots \wedge x_n$ assure justement que toute application n-linéaire alternée s'annule en $(x_1, \dots, x_n)$.

[Pour justifier que l'énoncé tel que formulé était erroné, il suffit de prendre $n = 2$, pour V un espace vectoriel non nul quelconque, $x_1 = 0$ (ce qui entraîne certainement $x_1 \wedge x_2 = 0$!) et $x_2 \neq 0$ et pour f une forme linéaire non nulle sur x_2.]

(b) Soit $\psi(X)$ le membre de droite de l'égalité qu'on cherche à prouver : soit $\psi(X) = \rho_{H,H'} \sum \rho_{R,R'} \det(X_{R,H}) \det(X_{R',H'})$. Premièrement, observons que chaque terme dans cette écriture, $\det(X_{R,H}) \det(X_{R',H'})$, est linéaire en chaque ligne de X (en effet, chaque ligne est soit dans H soit dans H', et, selon le cas, l'un ou l'autre facteur est linéaire et l'autre est constant).

Ainsi, ψ est une forme n-linéaire sur les lignes de X. Montrons qu'elle est antisymétrique : le plus simple est encore de montrer qu'elle change de signe par échange de deux lignes adjacentes (puisque les transpositions de deux éléments adjacents engendrent le groupe symétrique) ; or si ces deux lignes sont toutes deux dans H ou toutes deux dans H', c'est clair par la propriété correspondante de $\det(X_{R,H})$ ou $\det(X_{R',H'})$, et si l'une est dans H et l'autre dans H' on ne change pas $\det(X_{R,H})$ ni $\det(X_{R',H'})$ en échangeant les lignes en question, mais on change le signe de $\rho_{H,H'}$, donc il y a bien antisymétrie. En caractéristique différente de 2, ceci montre que ψ est une forme alternée des lignes de X ; en caractéristique 2, il faut encore expliquer que prendre deux lignes égales donne $\psi(X) = 0$, mais d'après ce qu'on vient de prouver on peut au moins placer les lignes en question à n'importe quel endroit souhaité, et si elles sont toutes deux dans H ou toutes deux dans H' le résultat est clair d'après la propriété alternée de

$\det(X_{R,H})$ ou $\det(X_{R',H'})$ (et le seul cas restant, $n = 2$ avec H et H' des singletons, est assez trivial en lui-même).

Enfin, il reste à considérer le cas où $X = I_n$ est la matrice identité : dans ce cas, $X_{R,H}$ est inversible si et seulement si $R = H$ (car il faut que chaque ligne contienne un coefficient non nul, donc il faut avoir la colonne correspondante), et on a donc $\psi(X) = \rho_{H,H'}^2 = 1 = \det(X)$. Mais puisque $\det$ est la seule forme n-linéaire alternée sur les lignes de X normalisée par $\det(I_n) = 1$, on a prouvé $\psi = \det$ comme souhaité. ✓

2. Soit p un nombre premier et $P \in \mathbb{Q}[X]$ un polynôme irréductible de degré p ayant 2 racines complexes conjuguées x_1, x_2 et $p-2$ racines réelles, $x_3, \ldots, x_p$. On note $K = \mathbb{Q}(x_1, \ldots, x_p)$ le corps engendré par les racines de P dans $\mathbb{C}$, et on identifie $\mathrm{Gal}(K/\mathbb{Q})$ à un sous-groupe du groupe des permutations $\mathfrak{S}_p$.

(a) Montrer que la permutation $\tau = (12)$ appartient à $\mathrm{Gal}(K/\mathbb{Q})$.

(b) Montrer que $\mathrm{Gal}(K/\mathbb{Q})$ contient un p-cycle σ.

(c) Que vaut $\mathrm{Gal}(K/\mathbb{Q})$?

(d) Application : $P(X) = X^5 - 6X + 3$.

Corrigé. (a) On a plongé K dans $\mathbb{C}$, ce dernier possédant l'automorphisme sur $\mathbb{Q}$ de conjugaison complexe. Comme K est normal sur $\mathbb{Q}$ (c'est le corps de décomposition de P), il est stable par tout $\mathbb{Q}$-automorphisme de $\mathbb{C}$ et en particulier par la conjugaison complexe. Or les hypothèses faites sur les racines assurent justement que la conjugaison complexe échange x_1 et x_2 et laisse fixes $x_3, \ldots, x_p$, donc détermine la permutation τ demandée.

(b) On sait que $\mathrm{Gal}(K/\mathbb{Q})$ agit transitivement sur $\{x_1, \ldots, x_p\}$, qui est de cardinal p : le stabilisateur d'un élément a donc indice p, ce qui montre que $\mathrm{Gal}(K/\mathbb{Q})$ a un cardinal multiple de p, et par un théorème de Cauchy (p étant premier) il a un élément d'ordre p. Cet élément σ, en tant que permutation, ne peut être qu'un unique cycle de longueur p car si sa décomposition en cycles a des longueurs plus petites que p leurs ordres ne seront pas multiples de p donc (de nouveau, p étant premier) l'ordre de σ non plus.

(c) Classique : la transposition de deux éléments adjacents peut s'obtenir en conjuguant τ par la bonne puissance de σ, et on sait que les transpositions de deux éléments adjacents engendrent $\mathfrak{S}_p$. Donc $\mathrm{Gal}(K/\mathbb{Q}) = \mathfrak{S}_p$.

(d) On a $P'(X) = 5X^4 - 6$. Posons $\alpha = \sqrt[4]{\frac{6}{5}}$ de sorte que $P'(\alpha) = P'(-\alpha) = 0$. On veut montrer que P a exactement trois racines réelles : le tableau de variations (P strictement décroissante sur $[-\alpha; \alpha]$ et croissante sur chacun des deux demi-droites contiguës à cet intervalle) montre qu'il y a au plus trois racines réelles. Pour montrer qu'il y en a exactement trois, on estime : $\alpha^4 = \frac{6}{5}$ donc $\alpha^4 - 6 = -\frac{24}{5}$ donc $P(\alpha) = (\alpha^4 - 6)\alpha + 3 < -\frac{24}{5} + 3 < 0$, et comme $P(0) = 3 > 0$ on a bien une racine entre 0 et α, une entre $-\infty$ et $-\alpha$ et une entre α et $+\infty$. On peut aussi appliquer la règle de Sturm : la suite de Sturm est définie par $P_0 = P$, $P_1 = P'$ et ensuite $-P_{i+2}$ reste de la division euclidienne de P_i par P_{i+1}, soit ici $P_2 = \frac{24}{5}X - 3$ et $P_3 = 21451/4096$ (un peu pénible à calculer exactement, mais le signe suffira) et en regardant la différence entre nombre de changements de signe dans les P_i en $+\infty$ et en $-\infty$, soit ici 0 et 3 respectivement, on a le nombre de zéros réels. ✓

3. Soit $E \subseteq F$ une extension finie séparable, $E \subseteq K$ sa clôture galoisienne.

(a) Montrer que le nombre de E-morphismes de F vers K est $n = [F : E]$.

(b) Soient $\eta_1 = \mathrm{id}, \eta_2, \ldots, \eta_n$ ces morphismes. Montrer que des éléments $u_1, \ldots, u_n$ de F forment une base de F sur E si et seulement si $\det(\eta_i(u_j)) \neq 0$.

Corrigé. (a) Soit $G = \mathrm{Gal}(K/E)$ le groupe de Galois de K sur E et $H = \mathrm{Gal}(K/F)$ le sous-groupe associé à F : comme $\mathrm{card}\, G = [K : E]$ et $\mathrm{card}\, H = [K : F]$, on a, bien sûr,

$(G : H) = [F : E]$ (où $(G : H)$ désigne l'indice de H dans G). Par ailleurs, tout élément $\sigma \in G$ détermine, par restriction à F, un E-morphisme (plongement) de F vers K. On a $\sigma|_F = \sigma'|_F$ exactement lorsque $\sigma'^{-1}\sigma$ induit l'identité sur F, c'est-à-dire, appartient à H : ainsi, l'ensemble des E-morphismes de F vers K est exactement en bijection avec l'ensemble des classes à gauche de G modulo H, et on vient d'expliquer qu'il y en a n.

(b) L'indépendance linéaire des caractères assure que $\eta_1, \ldots, \eta_n$, vus comme applications $F \to K$, sont libres sur K. Or ils sont complètement déterminés par leur donnée sur une E-base de F : donc, si $u_1, \ldots, u_n$ est une telle base, $\det(\eta_i(u_j)) \neq 0$ (précisément, si on avait une relation linéaire non triviale $\sum_i \lambda_i \eta_i(u_j) = 0$ avec $\lambda_i \in K$ non tous nuls, alors on aurait $\sum_i \lambda_i \eta_i(x) = 0$ pour tout $x \in E$, puisque les u_i engendrent F comme E-espace vectoriel, et cela contredit l'indépendance linéaire). Réciproquement, si la famille $u_1, \ldots, u_n$ est liée, mettons $\sum_j \lambda_j u_j = 0$ avec $\lambda_j \in E$ non tous nuls, alors manifestement $\sum_j \lambda_j \eta_i(u_j) = 0$ donc $\det(\eta_i(u_j)) = 0$. ✓

4. Soit E un sous-corps du corps $\mathbb{R}$ des nombres réels. On appelle extension radicale réelle de E une extension radicale de E contenue dans $\mathbb{R}$.

(a) Soit $E \subseteq F$ une extension galoisienne finie, avec $F \subseteq \mathbb{R}$. Soit $\alpha \in \mathbb{R}$ tel que $\alpha^N \in E$, où $N \geq 2$ est un entier.

(i) Soit $m = [E(\alpha) : E(\alpha) \cap F]$ et $\beta = \alpha^m$. Montrer que β appartient à $E(\alpha) \cap F$; en déduire que : $E(\beta) = E(\alpha) \cap F$. (On pourra considérer le polynôme minimal de α sur $E(\alpha) \cap F$ et s'intéresser au terme constant de celui-ci.)

(ii) Montrer que le degré $[E(\beta) : E]$ vaut 1 ou 2 (on pourra observer qu'une certaine puissance de β appartient à E).

(b) Soit $E \subseteq F$ une extension galoisienne finie, avec $F \subseteq \mathbb{R}$. Soit $E \subseteq K$ une extension radicale réelle. Montrer que $[K \cap F : E]$ est une puissance de 2. (On pourra procéder par récurrence, en introduisant une extension radicale élémentaire $E \subseteq L$, et en considérant les extensions $L \subseteq FL$ et $L \subseteq K$.)

(c) Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible de degré n, dont toutes les racines sont réelles. On suppose que l'une des racines α de P est dans une extension radicale réelle de $\mathbb{Q}$. Montrer que n est une puissance de 2.

Corrigé. (a) (i) Posons $M = E(\alpha) \cap F$. On a bien sûr $M(\alpha) = E(\alpha)$, de sorte que $m = [M(\alpha) : M]$ est le degré de α sur M. On sait que α^N appartient à E, donc à M : le polynôme minimal de α sur M divise donc $X^N - a$ où $a = \alpha^N$, donc toutes ses racines sont de la forme $\zeta\alpha$ avec ζ une racine (N-ième) de l'unité. Comme il est de degré m, son terme constant, c'est-à-dire (au signe près) le produit de ces m racines, est de la forme $\zeta\beta$ avec ζ une racine de l'unité. Mais comme β est réel et que le polynôme est à coefficients réels (car dans M), cette racine de l'unité ζ est également réelle donc $\zeta = \pm 1$, donc $\zeta \in M$, et ceci prouve bien $\beta \in M$.

L'inclusion $E(\beta) \subseteq E(\alpha) \cap F$ est alors claire. Mais comme $[E(\alpha) : E(\alpha) \cap F] = m$ (par définition) et que $[E(\alpha) : E(\beta)] \leq m$ (puisque α vérifie une équation de degré m sur $E(\beta)$), on doit bien avoir l'égalité.

(ii) On a $\alpha^N \in E$, donc certainement $\beta^N \in E$. Comme précédemment, considérons le polynôme minimal de β sur E : toutes ses racines sont de la forme $\zeta\beta$ pour ζ une certaine racine (N-ième) de l'unité. Comme β en est une racine dans F et que $E \subseteq F$ est galoisienne, toute racine de ce polynôme devrait être dans F, donc les ζ aussi. Dans le corps des réels, ceci implique $\zeta = \pm 1$, et $E(\beta)$ est donc de degré au plus 2 sur E.

(b) Si $E \subseteq L$ est une extension radicale élémentaire réelle, mettons $L = E(\alpha)$ (avec $\alpha^N \in E$ pour un certain N) alors la question (a) assure que $[L \cap F : E]$ vaut 1 ou 2. De plus,

$L \subseteq FL$ est galoisienne (et bien sûr $FL \subseteq \mathbb{R}$). Maintenant, procédons par récurrence sur le nombre minimal d'extensions radicales élémentaires composant une extension radicale réelle $E \subseteq K$: on écrit donc $E \subseteq L \subseteq K$ où $E \subseteq L$ est élémentaire et le résultat est déjà prouvé pour $L \subseteq K$ (vis-à-vis de n'importe quelle extension galoisienne de L contenue dans les réels). On sait alors que $[K \cap FL : L]$ est une puissance de 2, et $[L \cap F : E]$ également.

À présent, observons que $[FL : L] = [F : L \cap F]$ (car F est galoisien sur E) et de même $[FL : (K \cap F)L] = [F : K \cap F]$ (pour la même raison), donc $[(K \cap F)L : L] = [K \cap F : L \cap F]$ (par multiplicativité des degrés). Or $(K \cap F)L \subseteq FL \cap K$, et puisqu'on a observé que $[K \cap FL : L]$ est une puissance de 2, il en va de même de $[(K \cap F)L : L] = [K \cap F : L \cap F]$. Enfin, puisque $[L \cap F : E]$ est aussi une puissance de 2 (à savoir 1 ou 2), on conclut que $[K \cap F : E]$ en est une.

(c) Soit F le corps de décomposition de P (et $E = \mathbb{Q}$) : on a F galoisien sur $\mathbb{Q}$, donc le résultat de la question (b) montre que pour toute extension radicale réelle K de $\mathbb{Q}$ le degré $[K \cap F : \mathbb{Q}]$ est une puissance de 2. En particulier, si K contient α, on en conclut que $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ est une puissance de 2 ; mais $\mathbb{Q}(\alpha)$ est un corps de rupture de P, donc de degré n. ✓