Algèbre

Exercice 1.
a. *On pose* $M_n = 2^n - 1$. *Montrer que, si* M_n *est premier,* n *est premier. Montrer que, si* p *et* q *sont premiers et si* $q \mid M_p$, *alors* q *est de la forme* $2kp + 1$.
b. *On pose* $G_n = 2^n + 1$. *Montrer que si* G_n *est premier,* n *est de la forme* 2^k.
c. *On pose* $H_k = G_{2^k}$. *Montrer que, si* $k \neq \ell$, *alors* H_k *et* H_ℓ *sont premiers entre eux.*
d. *Montrer que* H_k *divise* $2^{H_k} - 2$.

●●●●●●

a. $n = ab \Rightarrow M_n = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)\sum_{k=0}^{b-1} 2^{ak}$.
Donc M_n n'est pas premier. Par contraposition, si M_n est premier, alors n est premier.
Notons que la réciproque est fausse : $M_{11} = 23 \times 89$.

Si $q|M_p$ alors $q|(2^p - 1)$. Donc $2^p \equiv 1 \text{mod } q$. L'ordre de 2 modulo q est un diviseur de p. Si p est premier et $q \neq 2$ alors l'ordre de 2 est p.

Or q est premier, d'après le théorème de Fermat, $2^{q-1} \equiv 1 \text{ mod } q$.
Il en découle que $q-1$ est un multiple de p. Comme $q-1$ est pair, $q = 2kp+1$.
b. Si $n = 2^a(2b+1)$, $G_n = 2^n+1 = 2^{2^a(2b+1)}+1 = (2^{2^a})^{2b+1}+1 = \big(2^{2^a}+1\big)N$ avec $N \in \mathbb{N}^\star$. Donc G_n n'est pas premier.
c. Rappelons que $F_n = 2^{2^n} + 1$ est appelé : nombre de Fermat. $H_n = F_n$.
$H_{n+1} = 2^{2^{n+1}} + 1 = \big(2^{2^n}\big)^2 + 1 = \big(2^{2^n} + 1 - 1\big)^2 + 1 = (F_n - 1)^2 + 1$.
On déduit du théorème de Bézout : $F_n \wedge F_{n+1} = 1$. Donc $p \neq q \Rightarrow F_p \wedge F_q = 1$.
d. F_n divise $\big(2^{2^{2^n}} - 1\big)\big(2^{2^{2^n}} + 1\big) = 2^{2^{n+1}} - 1$.
$n = 1 \leqslant 2^n \Rightarrow 2^{2^{n+1}} - 1 \big| 2^{2^n} - 1$ qui divise $2\big(2^{2^n} - 1\big) = 2^{2^{n+1}} - 2 = 2^{F_n} - 2$.
Donc $F_n | 2^{F_n} - 2$.

Exercice 2.
Soit p *un nombre premier impair. Montrer que* $-\overline{1}$ *est un carré dans* $\mathbb{Z}/p\mathbb{Z}$ *si et seulement si* $p \equiv 1 \text{ mod } 4$.

●●●●●●

$-\overline{1} = x^2 \Rightarrow x^{p-1} = \big(x^2\big)^{\frac{p-1}{2}} = 1$ car $\mathbb{Z}/p\mathbb{Z}$ est un corps de cardinal $p-1$.

Donc $\exists k \in \mathbb{N}, \dfrac{p-1}{2} = 2k$. D'où $p = 4k + 1$.

Réciproquement, d'après le théorème de Wilson : $(p-1)! \equiv -1 \bmod p$ car p est premier.
Donc $1.2\dots(2k)(4k-(2k-1))\dots(4k-1)(4k) \equiv -1 \bmod p$
Donc $1.2\dots(2k)(-(2k-1))\dots(-1)(-1) \equiv -1 \bmod p$
D'où $((2k)!)^2(-1)^{2k} \equiv -1 \bmod p$. Il existe x tel que $x^2 \equiv -1 \bmod p$.

Exercice 3.
Soient $E = \left\{P \in \mathbb{R}[X] \mid P = Q^2 + X\,R^2,\ (Q,R) \in \mathbb{R}[X]^2\right\}$ *et*
$F = \{P \in \mathbb{R}[X]\ ;\ \forall x \in \mathbb{R}^+,\ P(x) \geqslant 0\}$.
a. *Montrer que* E *est stable par produit.*
b. *Comparer* E *et* F.

●●●●●●

a. Si Q et R sont des polynômes qui peuvent s'écrire sous cette forme, on a $Q = Q_1 + XR_1,\ R = R_1 + XR_2$ où Q_1, Q_2, R_1, R_2 sont somme de deux carrés.
Par suite $QR = (Q_1R_1 + X^2Q_2R_2) + X(Q_1R_2 + Q_2R_1)$.
Comme, de façon évidente, les fonctions polynômes associées aux polynômes $Q_1R_1 + X^2Q_2R_2$ et $Q_1R_2 + Q_2R_1$ sont positives sur $\mathbb{R}$, d'après 1, il existe quatre polynômes A, B, C, D appartenant à $\mathbb{R}[X]$ tels que :
$QR = (A^2 + B^2) + X(C^2 + D^2)$.

b. Soit P un polynôme à coefficients réels non nul. Les assertions suivantes sont équivalentes :

(i) la fonction polynôme associée à P est positive sur $[0, +\infty[$,

(ii) les zéros strictement positifs de P sont de multiplicité paire,

(iii) il existe $(A, B, C, D) \in \left(\mathbb{R}[X]\right)^4$ tel que $P = A^2 + B^2 + X(C^2 + D^2)$.

On laisse le soin au lecteur d'établir les implications (i) ⇒ (ii) et (iii) ⇒ (i).

Pour établir (ii) ⇒ (iii), on note que seuls les zéros strictement négatifs peuvent être de multiplicité impaire. Ainsi, si l'on note $\mathcal{X}$ l'ensemble des zéros de multiplicité paire et $\mathcal{Y}$ l'ensemble des zéros de multiplicité impaire, P s'écrit sous la forme $P = \lambda \prod_{a \in \mathcal{Y}} (X+|a|)^{2\nu_a^\star + 1} \prod_{a \in \mathcal{X}} (X-a)^{2\nu_a^\star} \prod_{1 \leqslant k \leqslant q} \left((X-b_k)^2 + c_k^2\right)^{\mu_k}$.
Ainsi, $P = \lambda \prod_{a \in Y} (X + |a|)Q$ où Q est un polynôme de la forme $Q = A^2 + B^2$.
Il découle d'un examen du comportement de P au voisinage de $+\infty$ que $\lambda > 0$.
D'où l'assertion.

Exercice 4.
Soit $P = (X+1)^7 - X^7 - 1 \in \mathbb{R}[X]$.

a. *Calculer $P(j)$. En déduire la factorisation de P en facteurs irréductibles dans $\mathbb{R}[X]$.*
b. *Donner la décomposition en facteurs irréductibles de $\mathbb{R}[X]$ de :*

$$\frac{(X^3-1)^4}{((X+1)^7-X^7-1)^2}.$$

●●●●●●

a. $P(j)=0$ et $P\in\mathbb{R}[X]$ et $P(0)=0$ impliquent $X(X^2+X+1)|P$.
$P(-1)=0$. Comme $P'(X)=7(X+1)^6-7X^6$, on a $P'(j)=P'(j^2)=0$.
Comme $\deg(P)=6$, on a $P=7X(X+1)(X^2+X+1)^2$.

b. $F(X)=\dfrac{(X^3-1)^4}{((X+1)^7-X^7-1)^2}=\dfrac{(X-1)^4(X^2+X+1)^2}{49X^2(X+1)^2}$.

Exercice 5.
Soit $\varphi:\mathbb{R}[X]\to\mathbb{R}[X]$, $P\mapsto\dfrac{1}{2}\left(P(X)+P(-X)\right)+\dfrac{X}{2}\left(P(X)-P(-X)\right)$.
a. *Montrer que φ est linéaire.*
b. *Montrer que* $\mathrm{Ker}(\varphi)=\{(X-1)Q\ ;\ Q\in\mathbb{R}[X],\ Q$ *impair*$\}$.
c. *Montrer que* $\mathrm{Im}(\varphi)\oplus\mathrm{Ker}(\varphi)=\mathbb{R}[X]$.
d. *Caractériser φ.*

●●●●●●

a. Vérification immédiate.

b. $P\in\mathrm{Ker}(\varphi)\iff(X+1)P(X)+(1-X)P(-X)=0\qquad(1)$.

$(1)\Rightarrow P(1)=0\Rightarrow P(X)=(X-1)Q(X)$ où $Q\in\mathbb{R}[X]$.

$(1)\Rightarrow(X^2-1)Q(X)+(1-X)(-X-1)Q(-X)=0\Rightarrow Q(X)=-Q(-X)$
Donc (1) implique $P(X)=(X-1)Q(X)$ où Q est impaire.

Réciproque : si $P(X)=(X-1)Q(X)$ où Q est impaire, on vérifie que $\varphi(P)=0$.
D'où le résultat.

c. $\mathrm{Im}(\varphi)\subset\mathcal{P}$ où $\mathcal{P}$ est l'ensemble des polynômes pairs.
Si $Q\in\mathcal{P},\varphi(Q)=Q$. Donc $\mathrm{Im}(\varphi)=\mathcal{P}$.

$2\varphi(P)=(X-1)\big(P(X)-P(-X)\big)+2P(X)$. Donc $P=\varphi(P)+(X-1)Q$ où Q est impair.
$P\in\mathrm{Im}(\varphi)\cap\mathrm{Ker}(\varphi)\Rightarrow P=0$, d'où $\mathrm{Im}(\varphi)\oplus\mathrm{Ker}(\varphi)=\mathbb{R}[X]$.

d. φ est un projecteur de $\mathbb{R}[X]$.

Exercice 6.
Soit $(a,b)\in(\mathbb{R}^*)^2$. Soit $\phi\in\mathcal{L}(\mathfrak{M}_n(\mathbb{R}))$ définie par $\phi(M)=aM+b\,{}^tM$.
Donner une condition nécessaire et suffisante sur (a,b) pour que ϕ soit bijectif.
Calculer $\det(\phi)$ *et* $\mathrm{tr}(\phi)$.

●●●●●●

$\phi = aI_d + b\varphi$ où $\varphi : \mathfrak{M}_n(\mathbb{R}) \to \mathfrak{M}_n(\mathbb{R}), M \mapsto {}^tM$ et $\varphi^2 = I_d$.
φ est la symétrie de $\mathfrak{M}_n(\mathbb{R})$ par rapport $E_1(\varphi)$ et parallèlement à $E_{-1}(\varphi)$
$E_1(\varphi) = \mathcal{S}_n(\mathbb{R})$ de dimension $\dfrac{n(n+1)}{2}$.
$E_{-1}(\varphi) = \mathcal{A}_n(\mathbb{R})$ de dimension $\dfrac{n(n-1)}{2}$.
Si $\mathcal{B}_1$ est une base de $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{B}_2$ une base de $\mathcal{A}_n(\mathbb{R})$, alors $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ est une bse de $\mathfrak{M}_n(\mathbb{R})$ et $M_{\mathcal{B}}(\phi) = \mathrm{Diag}(a+b, a+b, \ldots, a+b, a-b, a-b, \ldots, a-b)$ où $a+b$ figure $\omega_1 = \dim(\mathcal{S}_n(\mathbb{R})$ fois et $(a-b)$ figure $\omega_2 = \dim(\mathcal{A}_n(\mathbb{R}))$ fois.
Donc $\det(\phi) = (a+n)^{\omega_1}(a-b)^{\omega_2}$ et $\mathrm{tr}(\phi) = a+b)\alpha_1 + (a-b)\omega_2 = an^2 + bn$.

Exercice 7.
Pour X dans $\mathfrak{M}_{n,1}(\mathbb{Z})$, on note $d(X)$ le pgcd de ses coordonnées. Soit A dans $\mathfrak{M}_n(\mathbb{Z})$. Montrer que $\det(A) \in \{-1, 1\}$ si et seulement si, pour tout X dans $\mathfrak{M}_{n,1}(\mathbb{Z})$, $d(X) = d(AX)$.

●●●●●●

• Si $\det(A) = \pm 1$, on peut supposer que $d(X) = 1$.
D'après le théorème de Bézout, $\exists Y \in \mathfrak{M}_{n,1}(\mathbb{Z}), {}^tYX = 1$.
Comme $A^{-1} \in \mathfrak{M}_n(\mathbb{Z}), B = A^{-1}Y \in \mathfrak{M}_{n,1}(\mathbb{Z})$.
${}^tBAX = {}^tYA^{-1}AX = {}^tYX = 1 \Rightarrow d(AX) = 1$ d'après Bézout.

• Réciproquement si $\det(A) \neq \pm 1$ il existe p premier tel que $p | \det(A)$.
Dans $\mathbb{Z}/p\mathbb{Z}$, on a $\overline{A} = (\overline{a_{i,j}}) \Rightarrow \overline{\det(A)} = \det\left(\overline{A}\right) = \overline{0}$.
$\exists {}^t\overline{X} = \left(\overline{x_i}\right)_{1 \leqslant i \leqslant n} \in \mathfrak{M}_{n,1}(\mathbb{Z}/p\mathbb{Z}) \setminus \{\overline{0}\}, \overline{A}.\overline{X} = 0$.

Donc, il existe $X = (x_1, \ldots, x_n) \neq 0$ tel que p divise les coefficients de AX.
Donc $p | d(AX)$ alors que p ne divise pas $d(X)$: absurde.

Exercice 8.
Soit $n \in \mathbb{N}$ avec $n \geqslant 2$, $(a, b) \in \mathbb{R} \times \mathbb{R}^*$ et $M = (m_{i,j})_{1 \leqslant i,j \leqslant n}$ où $m_{i,j} = b$ si $i \neq j$, $m_{i,i} = a$.
a. *Déterminer les valeurs propres de M. La matrice M est-elle diagonalisable ?*
b. *Déterminer les (a, b) pour lesquels M est inversible. Calculer alors M^{-1}.*
c. *Déterminer M^p pour $p \in \mathbb{N}$.*

●●●●●●

a. Si $J \in \mathfrak{M}_n(\mathbb{R})$ est la matrice dont tous les coefficients sont égaux à 1, on a : $M = bJ + (a-b)I_n$. On sait que $J \in \mathcal{S}_n(\mathbb{R})$ est diagonalisable avec pour valeurs propres 0 de multiplicité $(n-1)$ et n de multiplicité 1. La matrice M est donc diagonalisable avec pour valeurs propres $(a-b)$ de multiplicité $(n-1)$ et $a + (n-1)b$ de multiplicité 1.

b. On en déduit que $\det(M) = (a-b)^{n-1}(a+(n-1)b)$. La matrice M est inversible si, et seulement si, $(a-b)(a+(n-1)b) \neq 0$.

Comme $\mathrm{Sp}(M) = \{a-b, a+(n-1)b\}$ et comme M est diagonalisable, son polynôme minimal est $\Pi_M = (X-(a-b))(X-(a+(n-1)b))$.

$\Pi_M(M) = 0 \iff M^2 - \big(a+(n-2)b\big)M + (a-b)(a+(n-1)b)I_n = 0$.

Donc $M^{-1} = \dfrac{1}{(a-b)(a+(n-1)b)}\Big((a+(n-2)b)I_n - M\Big)$.

c. Utilisons la méthode classique de la division euclidienne.

$\forall p \in \mathbb{N}, X^p = \Pi_M(X)Q(X) + \alpha_p X + \beta_p \Rightarrow M^p = \alpha_p M + \beta_p I_n$.

On détermine α_p et β_p avec le système de Cramer, puisque $b \neq 0$:

$$(\star)\ \begin{cases} (a-b)^p = \alpha_p(a-b) + \beta_p \\ (a+(n-1)b)^p = \alpha_p(a+(n-1)b) + \beta_p \end{cases}$$

$$(\star) \iff \begin{cases} \alpha_p = \dfrac{1}{nb}\Big((a+(n-1)b)^p - (a-b)^p\Big) \\ \beta_p = \dfrac{1}{nb}\Big((a-b)(a+(n-1)b)^p - (a-b)^p(a+(n-1)b\Big) \end{cases}$$

Exercice 9.

Soit $(E, \langle\ ,\ \rangle)$ un espace euclidien de dimension $n \geqslant 2$. On donne $\alpha \in \mathbb{R}$, u, v dans E et l'on considère l'application ϕ définie par $\phi : E \times E \to \mathbb{R}$, $(x,y) \mapsto \langle x,u\rangle\langle y,v\rangle + \langle x,v\rangle\langle y,u\rangle + \alpha\langle x,y\rangle$.

a. *Montrer que ϕ est une forme bilinéaire symétrique.*

b. *Établir l'existence et l'unicité de $s \in \mathcal{S}(E)$ telle que :*

$$\forall (x,y) \in E^2,\ \phi(x,y) = \langle x, s(y)\rangle.$$

c. *Montrer que ϕ est un produit scalaire si et seulement si les valeurs propres de s sont strictement positives.*

d. *Établir l'existence d'une base orthonormée $e = (e_1, \ldots, e_n)$ de E, de r et r' dans $\mathbb{R}^+$ et de θ dans $\mathbb{R}$ tels que $u = r\,e_1$, $v = r'\cos(\theta)\,e_1 + r'\sin(\theta)\,e_2$.*

e. Écrire la matrice de s dans e.

f. Donner une condition sur (r, r', α, θ) pour que ϕ soit un produit scalaire.

●●●●●●

a. Comme le produit scalaire est est une forme bilinéaire symétrique, on en déduit que ϕ est une forme bilinéaire symétrique.

b. $\mathcal{B} = (e_i)_{1\leqslant i\leqslant n}$ une base orthonormale de E et $A = (a_{i,j}) \in \mathfrak{M}_n(\mathbb{R})$ où $a_{i,j} = \phi(e_i, e_j)$. De la bilinéarité de ϕ on déduit :

$$\phi(x,y) = \phi\Big(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n y_j e_j\Big) = \sum_{i=1}^n\sum_{j=1}^n a_{i,j}x_i y_j.$$

Donc $\phi(x,y) = {}^tXAY = \big(x|s(y)\big)$ où A est la matrice de s dans la base $\mathcal{B}$.

De la symétrie de φ on déduit immédiatement que $A \in \mathcal{S}_n(\mathbb{R})$ et donc $s \in \mathcal{S}(E)$.

S'il existe $s' \in \mathcal{L}(E)$ telle que $\forall x, y \in E, \big(x|s(y)\big) = \big(x|s'(y)\big)$,
$\forall x, y \in E, \big(x|(s'-s)(y)\big) = 0 \Rightarrow \forall y \in E, (s'-s)(y) \in E^\perp = \{0\} \Rightarrow s = s'$.
D'où l'unicité de $s \in \mathcal{S}(E)$ telle que : $\forall (x, y) \in E^2$, $\phi(x, y) = \langle x, s(y)\rangle$.
Par suite, on a prouvé l'existence et l'unicité de s.

c. ϕ est un produit scalaire sur E si, et seulement si, sa matrice A est élément de $\mathcal{S}_n^{++}(\mathbb{R})$ si, et seulement si, $\mathrm{Sp}(A) = \mathrm{Sp}(s) \subset \mathbb{R}_+^\star$ par une démonstration classique que l'on doit savoir faire.

d. Soit (u, v) une famille libre de E (c'est possible car $\dim(E) \geqslant 2$). Posons $e_1 = \dfrac{u}{\|u\|}$ et e_2 tel que (e_1, e_2) soit une base orthonormale de $\mathrm{Vect}(u, v)$.
$u = re_1$ et $v = r'\big(\cos(\theta)e_1 + \sin(\theta)e_2\big)$ avec $r = \|u\|$, $r' = \|v\|$. Avec le théorème de la base incomplète et le procédé de Schmidt, on a $\mathcal{B} = (e_1, \ldots, e_n)$ une base orthonormale de E.
$\big(x|u\big) = r\big(x|e_1\big)$; $\big(y|u\big) = r\big(y|e_1\big)$; $\big(x|v\big) = r'\cos(\theta)\big(x|e_1\big) + r'\sin(\theta)\big(x|e_2\big)$.

$$\phi(x, y) = rx_1r'(\cos(\theta - y_1 + \sin(\theta)y_2) + ry_1r'(\cos(\theta)x_1 + \sin(\theta)x_2) + \alpha\sum_{i=1}^{n} x_iy_i.$$

$$\phi(x, y) = x_1y_1r'(2rr'\cos(\theta) + \alpha) + (x_1y_2 + x_2y_1)rr'\sin(\theta) + \alpha x_2y_2 + \alpha\sum_{i=3}^{n} x_iy_i.$$

$\phi(x, y) = {}^tXAY$ où $A = \mathrm{Diag}(B, I_{n-2})$ avec $B = \begin{pmatrix} \alpha + 2\cos(\theta) & rr'\sin(\theta) \\ rr'\sin(\theta) & \alpha \end{pmatrix}$
e. $A \in \mathcal{S}_n^{++}(\mathbb{R}) \iff \alpha > 0$ et $B \in \mathcal{S}_2^{++}(\mathbb{R})$.
$\chi_B = X^2 + \mathrm{tr}(B)X + \det(B)$. Donc $\mathrm{Sp}(B) \subset \mathbb{R}_+^\star \iff \mathrm{tr}(B) > 0$ et $\det(B) > 0$.
$\mathrm{tr}(B) = 2(\alpha + \cos(\theta))$ et $\det(B) = (\alpha + rr'\cos(\theta))^2 - (rr')^2$.
Donc $A \in \mathcal{S}_n^{++}(\mathbb{R}) \iff \alpha > 0$ et $rr' < \alpha + rr'\cos(\theta)$.
Comme $rr' < \alpha + rr'\cos(\theta) \iff \alpha > rr'(1 - \cos(\theta)) = 2rr'\sin^2\left(\dfrac{\theta}{2}\right)$, la condition cherchée est $\alpha > 2rr'\sin^2\left(\dfrac{\theta}{2}\right)$.

Exercice 10.
Soient $A \in \mathfrak{M}_n(\mathbb{R})$ et $\phi_A : M \in \mathfrak{M}_n(\mathbb{R}) \mapsto AM{}^tA$
a. *Donner une condition nécessaire et suffisante sur A pour que l'application ϕ_A soit inversible.*
b. *Calculer $\det \phi_A$ lorsque $A = \lambda I_n$.*
c. *Calculer $\det \phi_A$ lorsque A est diagonale.*
d. *Donner une condition nécessaire et suffisante sur A pour que ϕ_A soit un automorphisme orthogonal de $\mathfrak{M}_n(\mathbb{R})$ muni de son produit scalaire canonique.*
e. *On suppose $A \in \mathcal{O}_n(\mathbb{R})$. Calculer $\det \phi_A$.*

●●●●●●

a. Si A est inversible, on vérifie aisément que $\phi_A \circ \phi_{A^{-1}} = \phi_{A^{-1}} \circ \phi_A = I_{\mathfrak{M}_n(\mathbb{R})}$. Donc ϕ_A est inversible et son inverse est $\phi_{A^{-1}}$.

Réciproquement, ϕ_A est inversible, il existe $B \in \mathfrak{M}_n(\mathbb{R})$ telle que
$\forall M \in \mathfrak{M}_n(\mathbb{R}), \phi_A \circ \phi_b(M) = M$ *i.e.* $\forall M \in \mathfrak{M}_n(\mathbb{R}), ABM^t(AB) = M$.
Donc $AB^t(AB) = I_n$. D'où A est inversible dans $\mathfrak{M}_n(\mathbb{R})$.

On conclut que A est inversible si, et seulement si, ϕ_A est inversible.

b. Si $A = \lambda I_n$, on a $\phi_A = \lambda^2 I_{\mathfrak{M}_n(\mathbb{R})}$. Donc $\det(\phi_A) = (\lambda^2)^{n^2} = \lambda^{2n^2}$.

c. Si $A = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$ et si un des λ_i est nul, on déduit de **a.** $\det(\phi_A) = 0$.

Sinon, Soit $(M_{i,j})$ la base canonique de $\mathfrak{M}_n(\mathbb{R})$ un calcul facile donne $\phi_A(M_{i,j}) = \lambda_i \lambda_j M_{i,j}$. Il en découle que $\det(\phi_A) = \det^n(A)$.

d. $\big(\phi_A(X)|Y\big) = \mathrm{tr}\left(A^t X^t A Y\right) = \mathrm{tr}\left({}^t X^t A Y A\right) = \big(X|{}^t A Y A\big)$.

Donc $\forall X, Y \in \mathfrak{M}_n(\mathbb{R}), \big(\phi_A(X)|Y\big) = \big(X|\phi_{{}^t A}(Y)\big)$.

ϕ_A est orthogonale si, et seulement si, ϕ_A est inversible et si son inverse est $\phi_{{}^t A}$ *i.e.* si, et seulement si, $A^{-1} = {}^t A$ *i.e.* $A \in \mathcal{O}(n)$.

e. $A \in \mathcal{O}(n) \Rightarrow |\det(\phi_A)| = 1$ d'après **c.**

Exercice 11.
Soit $(E, \langle\ ,\ \rangle)$ un espace euclidien.
a. *Soit $f \in \mathcal{L}(E)$. Montrer qu'il existe un unique élément de $\mathcal{L}(E)$, que l'on notera f^*, tel que : $\forall (x, y) \in E^2$, $\langle f(x), y\rangle = \langle x, f^*(y)\rangle$.*
b. *Soit $f \in \mathcal{L}(E)$. Montrer que $f^* = f$ si et seulement si $f^* \circ f = f \circ f$.*
c. *Déterminer les $f \in \mathcal{L}(E)$ telles que f est nilpotente et $f^* \circ f = f \circ f^*$.*

●●●●●●

a. Si $A \in \mathfrak{M}_n(\mathbb{R})$ est la matrice de f dans une base orthonormale $\mathcal{B}$ de E, $\big(f(x)|y\big) = {}^t(AX)Y = {}^t X {}^t A Y = \big(x|g(y)\big)$ où g est l'endomorphisme dont la matrice dans la base $\mathcal{B}$ est ${}^t A$.

Supposons l'existence de $h \in \mathcal{L}(E)$ vérifiant $\forall x, y \in E, \big(f(x)|y\big) = \big(x|h(y)\big)$.
Alors $\forall x, y \in E, \big(x|(g-h)(y)\big) = 0$. Donc $\forall y \in E, (g-h)(y) \in E^\perp = \{0\}$.
D'où $g = h$. Le résultat est donc prouvé. On notera dorénavant $g = h^*$.

b. $f^* = f \Rightarrow f^* \circ f = f \circ f$.
Réciproquement, notons $(f, g) \mapsto \mathrm{tr}(f^* \circ g)$ le produit scalaire sur$\mathcal{L}(E)$ et $\|\cdot\|$ la norme euclidienne associée.
$\|f^* - f\|^2 = \|f^*\|^2 + \|f\|^2 - 2\big(f^*|f\big) = 2\,\mathrm{tr}(f^* \circ f) - 2\,\mathrm{tr}(f^2) = 0$. Donc $f = f^*$.

c. Si f est nilpotent, $f^n = 0$. Comme $f \circ f^* = f^* \circ f$, on a :
$(f^* \circ f)^n = (f^*)^n \circ f^n = 0$.
Donc $f^* \circ f$ est nilpotente, d'où $\mathrm{tr}(f^* \circ f) = 0 \Rightarrow \big(f|f\big) = \|f\|^2 = 0 \Rightarrow f = 0$.

Exercice 12.
Soit $(A_p)_{p\geqslant 0}$ une suite d'éléments de $\mathcal{S}_n(\mathbb{R})$ croissante et majorée c'est-à-dire : $\forall p\in\mathbb{N}$, $A_{p+1}-A_p\in\mathcal{S}_n^+(\mathbb{R})$ et $\exists B\in\mathcal{S}_n(\mathbb{R})$, $\forall p\in\mathbb{N}$, $B-A_p\in\mathcal{S}_n^+(\mathbb{R})$. Montrer que (A_p) converge.

••••••

On a donc $\forall p\in\mathbb{N},\forall X\in\mathbb{R}^n, {}^tXA_pX\leqslant {}^tXA_{p+1}X$ et ${}^tXA_pX\leqslant {}^tXBX$.

Pour X fixé, la suite de réels $({}^tXA_pX)_{p\in\mathbb{N}}$ est croissante et majorée. Elle converge. Notons $f(X)$ sa limite. Notons aussi $A_p=(a_{i,j}(p))_{1\leqslant i,j\leqslant n}$.

$\forall X,Y\in\mathbb{R}^n, {}^t(X+Y)A_p(X+Y)\xrightarrow[p\to\infty]{} f(X+Y)$.

Or ${}^t(X+Y)A_p(X+Y)={}^tXA_pX+{}^tXA_pY+{}^tYA_pX+{}^tYA_pY$.

Donc ${}^tXA_pY+{}^tYA_pX\xrightarrow[p\to\infty]{} f(X+Y)-f(X)-f(Y)$.

Comme $A_p\in\mathcal{S}_n(\mathbb{R})$, ${}^tXA_pY\xrightarrow[p\to\infty]{}\dfrac{1}{2}\big(f(X+Y)-f(X)-f(Y)\big)$.

$(E_i)_{1\leqslant i\leqslant n}$ étant la base canonique de $\mathfrak{M}_{n,1}(\mathbb{R})$, on sait que $a_{i,j}(p)={}^tE_iA_pE_j$.

Donc : $a_{i,j}(p)\xrightarrow[p\to\infty]{}\dfrac{1}{2}\big(f(E_i+E_j)-f(E_i)-f(E_j)\big)$ que nous notons $\ell_{i,j}$.

Donc $A_p\xrightarrow[p\to\infty]{} L=(\ell_{i,j})\in\mathcal{S}_n(\mathbb{R})$.

Exercice 13.
Déterminer les P de $\mathbb{R}[X]$ tels que $P(\mathbb{Q})\subset\mathbb{Q}$, puis les P de $\mathbb{R}[X]$ tels que $P(\mathbb{Q})=\mathbb{Q}$.

••••••

Soit $P\in\mathbb{R}[X]$ tel que $P(\mathbb{Q})\subset\mathbb{Q}$, montrons que $P\in\mathbb{Q}[X]$.
Si $\deg(P)=n$, d'après le cours sur les polynômes d'interpolation de Lagrange,
$P(X)=\displaystyle\sum_{k=0}^{n}P(k)L_k(X)$ où $L_i(X)=\displaystyle\prod_{\substack{j=0\\ j\neq i}}^{n}\Big(\frac{X-j}{i-j}\Big)\cdot$ Donc $P\in\mathbb{Q}[X]$.
Réciproquement, si $P\in\mathbb{Q}[X]$ alors $P(\mathbb{Q})\subset\mathbb{Q}$.

Montrons que les seuls polynômes de $\mathbb{R}[X]$ tels que $P(\mathbb{Q})=\mathbb{Q}$ sont les polynômes de la forme $aX+b$ avec $(a,b)\in\mathbb{Q}^\star\times\mathbb{Q}$.

Si P est constant, $P(\mathbb{R})=\mathbb{Q}$. Donc il n'y a pas de polynôme constant solution.

Si P est un polynôme solution tel que $\deg(P)>1$, on peut supposer $P\in\mathbb{Z}[X]$ de coefficient dominant >0, au besoin en multipliant P par un entier relatif.

Soit $n\in\mathbb{N}$ tel que $n>P(0)$ et q un nombre premier.