ministère
Éducation
nationale

CAPES
CONCOURS EXTERNE ET CAFEP

Section : MATHEMATIQUES

EPREUVES D'ADMISSIBILITE

Ce sujet est constitué de trois problèmes totalement indépendants.

PROBLÈME N°1

Le but de ce problème est d'établir l'existence de la décomposition polaire dans $GL_n(\mathbb{R})$ et d'en donner une conséquence topologique.

Dans tout le problème, n désigne un entier naturel non nul.

Notations et conventions

- $[\![1, n]\!]$: l'ensemble des nombres entiers compris entre 1 et n
- Si E est un ensemble, id_E désigne l'application identité de E sur E
- Si A est une matrice, A^t désigne sa transposée
- $\mathscr{M}_n(\mathbb{R})$: l'ensemble des matrices carrées à n lignes et n colonnes
- I_n : la matrice identité dans $\mathscr{M}_n(\mathbb{R})$
- $GL_n(\mathbb{R})$: l'ensemble des matrices inversibles dans $\mathscr{M}_n(\mathbb{R})$
- $O_n(\mathbb{R})$: l'ensemble des matrices orthogonales dans $\mathscr{M}_n(\mathbb{R})$, *i.e.*

$$O_n(\mathbb{R}) = \{A \in \mathscr{M}_n(\mathbb{R}); A^t A = I_n\}$$

- $S_n(\mathbb{R})$ (respectivement $S_n^+(\mathbb{R})$, $S_n^{++}(\mathbb{R})$) : l'ensemble des matrices symétriques (respectivement symétriques positives, symétriques définies positives) dans $\mathscr{M}_n(\mathbb{R})$
- Si E est un espace euclidien, $S(E)$ (respectivement $S^+(E)$, $S^{++}(E)$) désigne l'ensemble des endomorphismes autoadjoints (respectivement autoadjoints positifs, autoadjoints définis positifs) de E

I. Racine carrée d'une matrice symétrique réelle définie positive

Soit $A \in S_n^{++}(\mathbb{R})$. Le but de cette partie est d'établir l'existence et l'unicité d'une matrice $S \in S_n^{++}(\mathbb{R})$ telle que $A = S^2$. (*La matrice S est appelée la racine carrée de A.*)

Soient E un espace euclidien et $f \in S^{++}(E)$. On note $\lambda_1, ..., \lambda_r$ les valeurs propres distinctes de f, $E_1, ..., E_r$ les espaces propres respectivement associés à $\lambda_1, ..., \lambda_r$ et $d_1, ..., d_r$ leurs dimensions respectives.

1) Supposons qu'il existe $g \in S^{++}(E)$ tel que $f = g^2$.
   a) Montrer que $f \circ g = g \circ f$ et en déduire que, pour tout $i \in [\![1, r]\!]$, g laisse stable E_i. Pour tout $i \in [\![1, r]\!]$, on note alors g_i la restriction de g à E_i.
   b) Soit $i \in [\![1, r]\!]$.
      i) Montrer que g_i est diagonalisable et que ses valeurs propres $\mu_1, ..., \mu_{d_i}$ sont strictement positives.
      ii) Montrer que $g_i^2 = \lambda_i id_{E_i}$ et en déduire que $\mu_1 = ... = \mu_{d_i} = \sqrt{\lambda_i}$, puis que $g_i = \sqrt{\lambda_i} id_{E_i}$.
   c) En déduire que g est unique.
2) Utiliser 1.c) pour montrer qu'il existe $g \in S^{++}(E)$ tel que $f = g^2$.
3) Conclure.

II. Décomposition polaire dans $GL_n(\mathbb{R})$

Le but de cette partie est de montrer que pour tout $M \in GL_n(\mathbb{R})$, il existe un et un seul couple $(O, S) \in O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R})$ tel que $M = OS$. (*Cette décomposition unique de M est appelée sa décomposition polaire.*)

II.1. Existence de (O, S)

Soit donc $M \in GL_n(\mathbb{R})$.

a) Montrer que $M^tM \in S_n^{++}(\mathbb{R})$.

On note alors S la racine carrée de M^tM et on pose $O = (M^{-1})^tS$.

b) Montrer que O appartient à $O_n(\mathbb{R})$ et que $M = OS$.

II.2 Unicité de (O, S)

Soient $O, O' \in O_n(\mathbb{R})$ et $S, S' \in S_n^{++}(\mathbb{R})$ tels que $M = OS = O'S'$.

Calculer M^tM de deux façons différentes et en déduire $S = S'$ puis $O = O'$.

III. Compacité de $O_n(\mathbb{R})$

Le but de cette partie est de montrer que $O_n(\mathbb{R})$ est une partie compacte de $\mathscr{M}_n(\mathbb{R})$ et maximale pour cette propriété parmi les sous-groupes de $GL_n(\mathbb{R})$.

III.1. Préliminaire

Pour toute matrice $A = (a_{ij})_{i,j} \in \mathscr{M}_n(\mathbb{R})$, on pose $N(A) = \max\{|a_{ij}|; (i,j) \in [\![1,n]\!]^2\}$.

a) Montrer que l'application N ainsi définie sur $\mathscr{M}_n(\mathbb{R})$ est une norme.

Dans toute la suite du problème, on considérera le $\mathbb{R}$-espace vectoriel $\mathscr{M}_n(\mathbb{R})$ ainsi normé.

b) Soient une suite $(A_p)_p$ dans $\mathscr{M}_n(\mathbb{R})$ et un élément A de $\mathscr{M}_n(\mathbb{R})$. On note $A = (a_{ij})_{i,j}$ et pour tout $p \in \mathbb{N}$, $A_p = (a_{ij}^{(p)})_{i,j}$.
Montrer que la suite $(A_p)_p$ converge vers A si, et seulement si, pour tout $(i,j) \in [\![1,n]\!]^2$, la suite $(a_{ij}^{(p)})_p$ converge vers a_{ij}.

c) Montrer que les applications t et p respectivement définies par

$$t : \mathscr{M}_n(\mathbb{R}) \longrightarrow \mathscr{M}_n(\mathbb{R}), A \longmapsto A^t$$

et

$$p : \mathscr{M}_n(\mathbb{R}) \times \mathscr{M}_n(\mathbb{R}) \longrightarrow \mathscr{M}_n(\mathbb{R}), (A,B) \longmapsto AB$$

sont continues.

III.2. Compacité de $O_n(\mathbb{R})$

a) Montrer que $O_n(\mathbb{R})$ est une partie fermée dans $\mathscr{M}_n(\mathbb{R})$.

b) Soit $A = (a_{ij})_{i,j} \in O_n(\mathbb{R})$.

i) Montrer que, pour tout $i \in [\![1,n]\!]$, on a $\sum_{j=1}^{n} a_{ji}^2 = 1$.

ii) En déduire que $N(A) \leq 1$.

c) En déduire que $O_n(\mathbb{R})$ est une partie compacte de $\mathscr{M}_n(\mathbb{R})$.

III.3. Propriété de maximalité

Soit G un *sous-groupe* de $GL_n(\mathbb{R})$ tel que G soit une partie compacte de $\mathscr{M}_n(\mathbb{R})$ contenant $O_n(\mathbb{R})$.

Soit $M \in G$. On considère la décomposition polaire $M = OS$ de M.

a) Rappeler pourquoi il existe $P \in O_n(\mathbb{R})$, $\lambda_1, ..., \lambda_n \in \mathbb{R}^{*+}$ et $D = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \lambda_n \end{pmatrix}$ tels que $PSP^{-1} = D$.

b) Montrer que S et P appartiennent à G puis que, pour tout $p \in \mathbb{N}$, D^p appartient aussi à G.

c) En déduire, en utilisant que G est un sous-groupe, compact, de $GL_n(\mathbb{R})$, que pour tout $i \in [\![1, n]\!]$ on a $\lambda_i = 1$.

d) En déduire que $M = O$ et conclure.

PROBLÈME N°2

Le but de ce problème est de déterminer tous les couples de *nombres rationnels* (x, y) solutions du système

$$(S) \quad \begin{cases} x^y = y^x \\ 0 < x < y \end{cases}$$

Notations et conventions

Pour a et b dans $\mathbb{N}$, on note $a \wedge b$ le plus grand diviseur commun positif de a et b.

I. Solutions entières

Dans cette partie, on va déterminer tous les couples de *nombres entiers* (x, y) solutions du système (S), de deux façons différentes, analytique et arithmétique.

I.1. Méthode analytique

1) Vérifier que le couple $(2, 4)$ est solution de (S).

2) À l'aide de la fonction f définie sur $[1, +\infty[$ par $f(t) = \dfrac{\ln(t)}{t}$, montrer que le couple $(2, 4)$ est le seul couple de nombres entiers solution.

I.2. Méthode arithmétique

On exclut pour cette méthode tout recours à l'analyse.

Soit (x, y) un couple de nombres *entiers* solution de (S).

1) Montrer que $x \geq 2$ et $y \geq 3$.
2) Montrer que x et y ont les mêmes diviseurs premiers.
3) Montrer que x divise y. On note alors q le nombre entier tel que $y = qx$.
4) Introduisons q' tel que $q = 1 + q'$. Montrer que :

$$x^{q'} = 1 + q'.$$

5) Soit x' tel que $x = 1 + x'$.
   a) Montrer que, pour tout $(n, k) \in \mathbb{N}^2$, on a $(1 + n)^k \geq 1 + nk$.
   b) En déduire que $x' = 1$ et $q' = 1$ et conclure.

II. Solutions rationnelles

Dans cette partie, on va déterminer tous les couples de nombres *rationnels non tous deux entiers* (x, y) solutions du système (S).

On note $x = \dfrac{a}{b}$ et $y = \dfrac{a'}{b'}$ les formes irréductibles de x et y.

1) Montrer que $a \wedge b^{a'b} = 1$ et $a^{a'b} \wedge b^{a'b} = 1$.
2) En déduire : $a^{a'b} = a'^{ab'}$ et $b^{a'b} = b'^{ab'}$.
3) Montrer que $b \geq 2$ et $b' \geq 2$ puis que $b < b'$.
4) Montrer que b et b' ont les mêmes diviseurs premiers et que b divise b'.
   On note alors q le nombre entier tel que $b' = qb$.

   On montrerait de la même façon (et on l'admettra ici) que : $a \geq 2$, $a' \geq 2$, et qu'il existe un nombre entier r tel que $a' = ra$.

5) Montrer que $r > q$.

6) Montrer que a et r ont les mêmes diviseurs premiers, que b et q ont les mêmes facteurs premiers et que $q \wedge r = 1$.

7) Montrer qu'il existe deux nombres entiers $s, t \geq 2$ tels que $a = s^q$ et $b = t^q$, puis qu'on a $q = t^{r-q}$ et $r = s^{r-q}$.

8) En déduire que $r - q = 1$.

9) Calculer a, b, a', b' en fonction de q seulement.

10) Réciproquement, vérifier que, pour tout entier $q \geq 2$, les couples (x, y) définis à partir de q par les relations trouvées dans la question précédente sont bien solutions de (S).

PROBLÈME N°3

Ce problème est constitué de 3 parties et a pour but d'étudier les polynômes de Legendre définis sur $[-1, 0]$.

Notations et conventions

- $\mathbb{N}^*$ désigne l'ensemble des entiers naturels non nuls.
- Pour $k \in \mathbb{N}$, $\mathbb{R}_k[X]$ désigne l'ensemble des polynômes à coefficients réels et de degré inférieur ou égal à k (y compris le polynôme nul).
- Un polynôme dans $\mathbb{R}[X]$ et la fonction polynomiale qui lui est associée sont systématiquement identifiés.
- Si E est un $\mathbb{R}$-espace vectoriel muni d'un produit scalaire noté $< ., . >$ et si A est une partie de E, alors $A^\perp$ désigne *l'orthogonal de* A c'est-à-dire l'ensemble $\{x \in E; \forall a \in A, < x, a >= 0\}$. On rappelle que $A^\perp$ est un sous-espace vectoriel de E.

Partie 1

Pour $\alpha \in \mathbb{R}$, on note (E_α) l'équation différentielle

$$(E_\alpha) \quad \alpha y - (2x+1)y' - (x^2+x)y'' = 0.$$

Soit $n \in \mathbb{N}$.

1) Déterminer la valeur de α, qu'on notera α_n, telle que (E_α) possède au moins une solution polynomiale à coefficients réels et de degré exactement égal à n.
2) Montrer que (E_{α_n}) possède une unique solution polynomiale, notée L_n, à coefficients réels de degré exactement égal à n et telle que $L_n(0) = 1$.
3) Expliciter les coefficients de L_n à l'aide de coefficients binomiaux. (On pourra remarquer avec profit que $a(a+1) - b(b+1) = (a-b)(a+b+1)$.)

Partie 2

Dans toute cette partie, pour tous $P, Q \in \mathbb{R}[X]$ on note $< P, Q >$ le nombre réel :

$$< P, Q >= \int_{-1}^{0} P(x)Q(x)dx.$$

1) Montrer que l'application $\varphi : \mathbb{R}[X] \times \mathbb{R}[X] \longrightarrow \mathbb{R}, (P, Q) \longmapsto < P, Q >$ définit un produit scalaire sur $\mathbb{R}[X]$.
2) Soient m et n dans $\mathbb{N}$. Établir la formule

$$n(n+1) < L_n, L_m >= m(m+1) < L_m, L_n > .$$

3) En déduire que, pour tout $n \in \mathbb{N}$, la famille $(L_0, ..., L_n)$ est une base orthogonale de $\mathbb{R}_n[X]$.
4) Soit $n \in \mathbb{N}^*$.
   a) Montrer que $L_n \in (\mathbb{R}_{n-1}[X])^\perp$.
   b) Notons $x_1, ..., x_r$ les racines deux à deux distinctes de L_n qui sont dans $]-1, 0[$ et qui sont d'ordre de multiplicité *impair* (avec $r = 0$ s'il n'y en a pas).
   À l'aide de a), montrer qu'on ne peut pas avoir $r \leq n-1$.

c) En déduire que L_n a n racines simples dans $]-1,0[$.

5) Soit $n \in \mathbb{N}$. Après avoir montré qu'il existe $(\lambda_0, ..., \lambda_n) \in \mathbb{R}^{n+1}$ tel que

$$L_n(-X-1) = \lambda_0 L_0 + ... + \lambda_n L_n,$$

établir l'égalité :

$$L_n(-X-1) = (-1)^n L_n(X).$$

Préciser la valeur de $L_n(-1)$.

6) Soit $n \in \mathbb{N}^*$.

a) Après avoir montré qu'il existe $(\mu_0, ..., \mu_{n+1}) \in \mathbb{R}^{n+2}$ tel que

$$(2n+1)L_1 L_n = \mu_0 L_0 + ... + \mu_{n+1} L_{n+1},$$

établir l'égalité :

$$(2n+1)L_1 L_n = (n+1)L_{n+1} + nL_{n-1}.$$

b) En déduire que les racines de L_n s'intercalent entre celles de L_{n+1}, c'est-à-dire que si on note $\alpha_1^{(n)}, ..., \alpha_n^{(n)}$ (respectivement $\alpha_1^{(n+1)}, ..., \alpha_{n+1}^{(n)}$) les racines de L_n (respectivement L_{n+1}) rangées dans l'ordre croissant alors, pour tout $i \in [\![1, n]\!]$, on a $\alpha_i^{(n+1)} \leq \alpha_i^{(n)} \leq \alpha_{i+1}^{(n+1)}$. (On pourra raisonnner par récurrence sur n.)

Partie 3

On considère la fonction f définie sur $\mathbb{R}$ par $f(t) = \dfrac{-1}{\exp(t)+1}$.

1) Montrer que $f(\mathbb{R}) =]-1, 0[$.

Pour tout $n \in \mathbb{N}$, on note F_n la fonction définie par $F_n = L_n \circ f$.

2) Montrer qu'il existe $\beta_n \in \mathbb{R}$ (qu'on déterminera) tel que

$$F_n'' + \beta_n f' F_n = 0.$$

3) Montrer que, pour tout $t \in \mathbb{R}$, on a

$$0 \leq \frac{1}{f'(t)} F_n'^2(t) + n(n+1)F_n^2(t) \leq n(n+1).$$

4) En déduire que, pour tout $t \in \mathbb{R}$, on a $|F_n(t)| \leq 1$ puis que, pour tout $x \in [-1, 0]$, on a $|L_n(x)| \leq 1$.

5) Soit r fixé dans $[-1, 0]$. On considère la série entière $\sum L_n(r)t^n$.

a) Montrer que cette série converge pour tout $t \in]-1, 1[$.
Pour $t \in]-1, 1[$, on note $S_r(t)$ sa somme.

b) Montrer que S_r est solution de l'équation différentielle

$$(1 - 2(1+2r)t + t^2)g'(t) - (1 + 2r - t)g(t) = 0.$$

c) En déduire explicitement S_r.

Ce sujet est constitué d'un problème.

Notations.

$\mathscr{P}$ est un plan euclidien.
Étant donnés deux points distincts A et B du plan $\mathscr{P}$, on note $]AB[$ le segment $[AB]$ privé de ses extrémités.
Si Γ est un cercle de centre Ω, de rayon R, on appellera « intérieur du cercle Γ » et on notera $\mathscr{I}(\Gamma)$ le disque ouvert, de centre Ω, de rayon R qui est limité par Γ.
On a donc $\mathscr{I}(\Gamma) = \{M \in \mathscr{P} \,|\, \Omega M < R\}$.
De même, l'extérieur du cercle Γ, noté $\mathscr{E}(\Gamma)$ est l'ensemble :

$$\mathscr{E}(\Gamma) = \{M \in \mathscr{P} \,|\, \Omega M > R\}$$

Recommandations importantes.

Les sept parties de ce problème sont très largement dépendantes. Il est recommandé de les traiter dans l'ordre, mais on pourra toujours admettre un résultat pour continuer le problème.

Dans ce problème, on demande plusieurs fois de proposer une *construction géométrique* d'une figure ou d'un élément d'une figure. Ceci signifie que l'on demande une suite d'instructions permettant de réaliser de façon théorique cette figure ou cet élément à l'aide de la règle et du compas. *On réalisera effectivement cette construction dans une figure.*

Cependant, on supposera connues, on ne détaillera pas et on pourra utiliser sans explication les constructions géométriques élémentaires classiques suivantes :

- tracé de la médiatrice ou du milieu d'un bipoint ;
- tracé du cercle passant par trois points non alignés ;
- tracé de la parallèle à une droite passant par un point donné ;
- tracé de la perpendiculaire à une droite passant par un point donné.

Partie I : Puissance d'un point par rapport à un cercle.

Soit Γ un cercle de $\mathscr{P}$, de centre Ω, de rayon $R > 0$.

1. Soit M un point de $\mathscr{P}$, et soit $\mathscr{D}$ une droite passant par M et coupant Γ en deux points T_1 et T_2. On pose
$$p_{[\mathscr{D},\Gamma]}(M) = \overline{MT_1}.\overline{MT_2}$$
Montrer que $p_{[\mathscr{D},\Gamma]}(M) = \Omega M^2 - R^2$ donc que $p_{[\mathscr{D},\Gamma]}(M)$ ne dépend pas de la droite sécante $\mathscr{D}$.
(On pourra, introduire le point H, projeté orthogonal de Ω sur $\mathscr{D}$).
Dans cette situation, on pose $p_\Gamma(M) = p_{[\mathscr{D},\Gamma]}(M)$ (quelle que soit la droite $\mathscr{D}$ passant par M et coupant Γ en deux points) et on appelle cette quantité $p_\Gamma(M)$ *la puissance du point M par rapport au cercle* Γ.
2. Quel rapport y a-t-il entre le signe de la puissance d'un point M par rapport à un cercle Γ et sa position dans le plan ?
3. Quelle est la puissance du centre d'un cercle par rapport à ce cercle ?
4. Soit Γ un cercle et soit $\mathscr{D}_0$ une droite passant par M et tangente au cercle Γ en un point T.
Que peut-on dire du point M si une telle droite $\mathscr{D}_0$ existe ? $\mathscr{D}_0$ est-elle unique ?
Montrer que $p_\Gamma(M) = MT^2$.
5. Soient Γ_1 et Γ_2 deux cercles sécants en deux points A et B. Montrer que la droite (AB) est exactement l'ensemble de tous les points M du plan qui vérifient la relation
$$p_{\Gamma_1}(M) = p_{\Gamma_2}(M)$$

6. Déterminer la nature de l'ensemble des points qui ont la même puissance par rapport à deux cercles lorsque ceux-ci ne sont pas forcément sécants. Que peut-on en dire si les deux cercles sont tangents ?
7. $\mathscr{P}$ est rapporté à un repère orthonormal $\mathscr{R} = (O; \vec{\imath}, \vec{\jmath})$. Soit Γ un cercle dont l'équation cartésienne dans le repère $\mathscr{R}$ est $x^2 + y^2 + ax + by + c = 0$.
Déterminer la puissance du point O (origine du repère) par rapport à ce cercle.

Partie II : Construction d'une Π-droite.

Dans cette partie, $\mathscr{C}$ est un cercle de centre O et de rayon R, et Π le disque ouvert limité par $\mathscr{C}$ et A et B sont deux points distincts de Π.
Le but de cette partie est démontrer qu'en général, pour toute paire $\{A, B\}$ de points du disque ouvert Π, il y a existence et unicité, d'un cercle Γ passant par A et B, et coupant $\mathscr{C}$ en deux points *diamétralement opposés*, tout en proposant une construction géométrique de ce cercle Γ.

1. On suppose que A et B sont situés sur un même diamètre du cercle $\mathscr{C}$. Montrer qu'aucun cercle passant par A et B ne rencontre $\mathscr{C}$ en deux points diamétralement opposés. (On pourra calculer de deux manières la puissance de O par rapport à un cercle Γ qui passerait par A et B et qui couperait $\mathscr{C}$ en deux points diamétralement opposés).
2. On suppose que A et B ne sont pas situés sur un même diamètre et que $OA = OB$. Montrer dans ce cas l'existence et l'unicité d'un cercle Γ qui passe par A et B et qui rencontre $\mathscr{C}$ en deux points diamétralement opposés. Proposer une construction géométrique de ce cercle.
3. On suppose que $OA \neq OB$ et que A et B ne sont pas sur un même diamètre. On suppose qu'il existe un cercle Γ, de centre Ω, qui rencontre $\mathscr{C}$ en deux points diamétralement opposés T_1 et T_2.
   a. Montrer que (AB) rencontre (T_1T_2) en un point unique S.
   b. Comparer $p_{\mathscr{C}}(S)$ et $p_{\Gamma}(S)$.
   c. Soit Γ' un cercle quelconque passant par A et B et rencontrant $\mathscr{C}$ en deux points U_1 et U_2 distincts. Comparer la puissance de S par rapport aux cercles $\mathscr{C}$, Γ et Γ' et en déduire que $S \in (U_1U_2)$.
   d. Lorsqu'on ne connaît pas le cercle Γ, déduire de ce qui précède une construction géométrique du point S, puis du cercle Γ.
   e. Justifier l'existence et l'unicité de Γ.
4. Autre démonstration de l'existence et l'unicité de Γ :
Dans cette question, le plan euclidien $\mathscr{P}$ est rapporté à un repère orthonormal $\mathscr{R} = (O; \vec{\imath}, \vec{\jmath})$ et $\mathscr{C}$ est le cercle de centre O, de rayon $R = 1$.
   a. Montrer qu'un cercle Γ (distinct de $\mathscr{C}$) rencontre $\mathscr{C}$ en deux points diamétralement opposés si et seulement si $p_{\Gamma}(O) = -1$.
   b. En déduire une méthode analytique pour montrer l'existence et l'unicité de Γ en en déterminant une équation cartésienne puis son centre.Comment, dans cette méthode, reconnaît-on que les coordonnées de A et B sont telles qu'on est dans le cas particulier étudié à la question 1. ?

Partie III : Un problème de lieu géométrique.

Dans cette partie, $\mathscr{C}$ est un cercle de centre O, de rayon R, et A est un point distinct de O, situé dans le disque ouvert Π limité par $\mathscr{C}$. Le but de cette partie est de déterminer le lieu $\mathscr{L}$ des centres des cercles qui passent par A et qui coupent $\mathscr{C}$ selon deux points diamétralement opposés, puis d'en déduire une autre construction du cercle Γ de la partie II.

1. Soit $[T_0T_0']$ le diamètre de $\mathscr{C}$ perpendiculaire à (OA). Soit Γ_0 le cercle circonscrit au triangle $T_0T_0'A$, et Ω_0 son centre. Soit Ω un point de la perpendiculaire Δ à (OA) qui passe par Ω_0. Soit $[T_1T_2]$ le diamètre de $\mathscr{C}$ qui est perpendiculaire à (ΩO).
   a. Montrer que $\Omega T_i = \Omega A$ pour $i = 1, 2$.
   b. En déduire que $\Delta \subset \mathscr{L}$.
2. Montrer l'inclusion réciproque.
3. Déduire de cette étude une nouvelle construction géométrique du cercle Γ qui passe par deux points A et B (non situés sur un même diamètre) du disque Π, et qui coupe $\mathscr{C}$ en deux points diamétralement opposés.

Partie IV : Un « plan » étonnant.

On se place toujours dans un plan euclidien $\mathscr{P}$. On considère l'ensemble $\Pi = \mathscr{I}(\mathscr{C})$, qui est le disque ouvert limité par le cercle $\mathscr{C}$ d'équation $x^2 + y^2 = 1$ dans le repère orthonormal $\mathscr{R} = (O; \vec{\imath}, \vec{\jmath})$. On appelle Π-droite un sous-ensemble de Π qui est d'un des deux types suivants :

- soit c'est l'intersection de Π avec un cercle Γ (distinct de $\mathscr{C}$) qui passe par deux points diamétralement opposés de $\mathscr{C}$.
- soit c'est l'intersection de Π avec un diamètre de $\mathscr{C}$.

Le cercle [respectivement la droite] qui contient tous les points d'une Π-droite est le support de la Π-droite.

1. Justifier que par deux points distincts de Π passe une unique Π-droite.
   L'unique Π-droite passant par les deux points distincts A et B de Π sera notée $((AB))$.
2. Deux Π-droites seront dites Π-parallèles lorsqu'elles sont confondues ou que leur intersection est vide.
   a. Montrer que si les supports de deux Π-droites se coupent en deux points diamétralement opposés de $\mathscr{C}$, alors ces Π-droites sont Π-parallèles.
   b. Soit $U =]T_0T_0'[$ une Π-droite dont le support est un diamètre de $\mathscr{C}$ et soit V une Π-droite dont le support est un cercle Γ qui rencontre $\mathscr{C}$ en deux points diamétralement opposés T_1 et T_2 (non confondus avec T_0 ou T_0').
   En considérant la puissance de O par rapport à Γ, montrer que O est intérieur au cercle Γ puis que la Π-droite $]T_0T_0'[$ rencontre la Π-droite dont le support est Γ en un point unique.
   c. Montrer que si Γ et Γ' sont deux cercles coupant $\mathscr{C}$ en des couples différents de points diamétralement opposés respectivement (T_1, T_2) pour Γ, (T_1', T_2') pour Γ', alors Γ et Γ' se coupent en deux points d'un diamètre de $\mathscr{C}$, dont un seul est dans Π (on pourra considérer des équations cartésiennes de ces cercles).
   d. Montrer que si deux Π-droites non confondues sont Π-parallèles, alors leurs supports se coupent en deux points diamétralement opposés de $\mathscr{C}$.
   e. Montrer que la relation de Π-parallélisme est une relation d'équivalence dans l'ensemble des Π-droites.
3. Montrer que si deux Π-droites ne sont pas Π-parallèles, alors leur intersection est un singleton.
4. Montrer qu'étant donnés un point A de Π et une Π-droite U, il existe une unique Π-droite V qui est Π-parallèle à U et qui passe par A.

   L'ensemble Π vérifie donc deux axiomes classiques d'incidence dans un plan affine.
   Pour compléter l'étude de ce « plan », les parties suivantes vont montrer q'il peut être mis en bijection avec un plan usuel.

Partie V : Grands cercles d'une sphère et droites d'un plan.

Dans cette partie, Π_0 désigne le plan d'équation $z = 1$ dans un espace affine euclidien de dimension 3 rapporté à un repère orthonormal $\mathscr{R}' = \left(O; \vec{\imath}, \vec{\jmath}, \vec{k}\right)$, et $\mathscr{P}$ désigne le plan d'équation $z = 0$; un repère orthonormal du plan $\mathscr{P}$ est donc $\mathscr{R} = (O; \vec{\imath}, \vec{\jmath})$.
Σ désigne la sphère unité, d'équation cartésienne $x^2 + y^2 + z^2 = 1$, et Σ^+ désigne le sous-ensemble de Σ formé des points M dont la troisième coordonnée z dans le repère $\mathscr{R}'$ est strictement positive.

On rappelle q'un grand cercle d'une sphère est l'intersection d'un plan passant par le centre de la sphère avec cette sphère.
$\mathscr{C}$ désigne le cercle du plan $\mathscr{P}$ qui a pour centre O et pour rayon 1. $\mathscr{C}$ est donc aussi un grand cercle de Σ.

1. Montrer que l'intersection de deux grands cercles non confondus de Σ consiste toujours en deux points diamétralement opposés pour Σ.
2. Soit $\mathscr{Q}$ un plan passant par O, distinct de $\mathscr{P}$. Quelle est l'intersection de $\mathscr{Q}$ avec Σ ? Et avec Σ^+ ? Et avec $\mathscr{C}$?
3. Montrer qu'on définit correctement une application φ entre Π_0 et Σ^+ en associant à chaque point M de Π_0 le point d'intersection M' de la droite (OM) avec Σ^+. Montrer que φ est une bijection entre Π_0 et Σ^+.
4. Montrer que l'image d'une droite affine de Π_0 par φ est un « demi-grand-cercle » de Σ. Définir avec précision cette notion de « demi-grand-cercle ».
   Caractériser analytiquement l'image par φ d'une droite d'équations cartésiennes dans $\mathscr{R}'$:
   $$\begin{cases} ax + by + c = 0 \\ z = 1 \end{cases} \quad \text{avec } (a, b) \neq (0, 0)$$

Partie VI : Une autre correspondance entre sphère et plan.

Les notations sont les mêmes que dans la partie V. Σ^* désigne la sphère Σ privée de son « pôle sud », c'est-à-dire du point S de coordonnées $(0, 0, -1)$.

1. Montrer q'on définit correctement une application ψ entre Σ^* et $\mathscr{P}$ en associant à chaque point M de Σ^* le point d'intersection M' de la droite (SM) avec $\mathscr{P}$. ψ est-elle bijective ?
2. Soit M un point de Σ^* de coordonnées (x, y, z) (dans $\mathscr{R}'$). Déterminer en fonction de (x, y, z) les coordonnées (x', y', z') de $M' = \psi(M)$.
3. Soit N un point de $\mathscr{P}$ de coordonnées (x, y) dans $\mathscr{R}$. Déterminer en fonction de (x, y) les coordonnées (X, Y, Z) de l'antécédent éventuel M de N par ψ.
4. Montrer qu'un grand cercle de Σ peut être caractérisé par un système d'équations du type :
   $$\begin{cases} ax + by + cz = 0 \\ x^2 + y^2 + z^2 = 1 \end{cases} \quad \text{avec } (a, b, c) \neq (0, 0, 0).$$
5. Montrer que l'image par ψ d'un grand cercle de Σ ne passant pas par S est un cercle de $\mathscr{P}$.
   Quelle est l'image par ψ de l'intersection avec Σ^* d'un grand cercle de Σ passant par S ?
6. Soit $\mathscr{D}$ un grand cercle de Σ et soit $\mathscr{D}^* = \mathscr{D} \cap \Sigma^*$. Que peut-on dire de l'intersection de $\psi(\mathscr{D}^*)$ avec $\mathscr{C}$?
7. On appelle ψ^+ la restriction de ψ à Σ^+. Montrer que ψ^+ réalise une bijection de Σ^+ vers le disque ouvert Π limité par $\mathscr{C}$.

8. Montrer que l'image d'un « demi-grand-cercle » (voir V.3) par ψ^+ est une Π-droite (voir partie IV).

Partie VII : Synthèse et Application.

Les notations sont celles des parties précédentes.

1. Démontrer l'existence d'une bijection h du plan affine Π_0 vers l'ensemble Π induisant une bijection entre l'ensemble des droites de Π_0 et l'ensemble des Π-droites et conservant le parallélisme (en ce sens que deux droites parallèles de Π_0 sont transformées en deux Π-droites Π-parallèles).
2. Donner des formules analytiques de h, c'est-à-dire un système exprimant les coordonnées (x', y') dans le repère $\mathscr{R}$ de l'image $h(M)$ d'un point M en fonction de ses coordonnées $(x, y, 1)$ dans $\mathscr{R}'$.
3. Inverser le système précédent pour obtenir en fonction des coordonnées d'un point M celles de $h^{-1}(M)$.
4. Voici une *Définition du Π-milieu de deux points de Π.*
   Soient A et B deux points de Π. Soit C un point quelconque de Π, non situé sur $((AB))$. On considère le point D, intersection de la Π-droite qui passe par B et qui est π-parallèle à $((AC))$ et de la Π-droite qui passe par A et qui est π-parallèle à $((BC))$. On appelle Π-milieu de la paire $\{A, B\}$ le point I intersection des π-droites $((AB))$ et $((CD))$.

   En utilisant la bijection h, démontrer que cette définition est correcte : on vérifiera que les Π-droites $((AB))$ et $((CD))$ ne sont pas Π-parallèles, et que cette définition ne dépend pas du point C arbitrairement choisi.
5. Soit A le point de Π de coordonnées $\left(0, \frac{1}{2}\right)$ et B le point de coordonnées $\left(\frac{1}{4}, 0\right)$. Donner une construction géométrique détaillée du Π-milieu I de $\{A, B\}$ (On fera une figure en prenant 8 cm comme unité).
6. Donner les coordonnées des points $A' = h^{-1}(A)$, $B' = h^{-1}(B)$ et $I' = h^{-1}(I)$. En déduire les coordonnées de I dans le repère $\mathscr{R}$.

Ce sujet est constitué de deux problèmes totalement indépendants.

PROBLÈME N°1

Ce problème est constitué de 5 parties. La partie III est indépendante des autres.

Dans tout ce problème, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$ et E un $\mathbb{K}$-espace vectoriel de dimension finie $n \geq 2$.

Notations et conventions

- $\mathscr{L}(E)$: le $\mathbb{K}$-espace vectoriel des endomorphismes de E
- le vecteur nul de chaque espace vectoriel considéré par la suite sera invariablement noté 0.

Pour $f \in \mathscr{L}(E)$, on désigne par

- P_f le polynôme caractéristique de f
- π_f le polynôme minimal de f

et on convient que $f^0 = id_E$ (l'application identité de E).

Pour $P(X), Q(X)$ dans $\mathbb{K}[X]$, le fait que $P(X)$ divise $Q(X)$ sera noté $P|Q$ et $ppcm(P,Q)$ (respectivement $pgcd(P,Q)$) désignera le seul ppcm (respectivement pgcd) unitaire de $P(X)$ et $Q(X)$ dans $\mathbb{K}[X]$.

Définitions

Soient f un endomorphisme de E et x un élément de E.

On note alors $\mathbb{K}[f]$ le sous-espace vectoriel de $\mathscr{L}(E)$ défini par

$$\mathbb{K}[f] = \{Q(f); Q(X) \in \mathbb{K}[X]\},$$

$E_{f,x}$ le sous-espace vectoriel de E défini par

$$E_{f,x} = Vect(f^k(x); k \in \mathbb{N}),$$

$I_{f,x}$ la partie de $\mathbb{K}[X]$ définie par

$$I_{f,x} = \{P(X); P(f)(x) = 0\},$$

et pour $p \in \mathbb{N}^*$, $B(x,p)$ la famille

$$B(x,p) = (x, f(x), ..., f^{p-1}(x)).$$

On dit que f est un endomorphisme *cyclique* de E s'il existe $x \in E$ tel que $E_{f,x} = E$.

I Étude de $\mathbb{K}[f]$

Soit $f \in \mathscr{L}(E)$. On note s le degré du polynôme π_f.

1) Montrer que pour tout polynôme $Q(X) \in \mathbb{K}[X]$, il existe $(a_0, ..., a_{s-1}) \in \mathbb{K}^s$ tel que

$$Q(f) = \sum_{i=0}^{s-1} a_i f^i$$

(on pourra effectuer la division euclidienne de $Q(X)$ par $\pi_f(X)$).

2) Montrer que la famille $(id_E, f, ..., f^{s-1})$ est une base de $\mathbb{K}[f]$ et en déduire la dimension de $\mathbb{K}[f]$.

II Étude de $E_{f,x}$

1) Propriétés générales

Soient $f \in \mathscr{L}(E)$ et $x \in E$.

1) a) Montrer que $E_{f,x}$ est égal à $\{Q(f)(x); Q(X) \in \mathbb{K}[X]\}$ et que $E_{f,x}$ est un sous- espace vectoriel de E stable par f et contenant x.

b) Montrer que $E_{f,x}$ est *le plus petit* sous-espace vectoriel de E stable par f et contenant x.

2) À quelle condition sur $\dim E_{f,x}$ le vecteur x est-il un vecteur propre de f ?

3) Montrer que f est une homothétie si et seulement si pour tout $y \in E\backslash\{0\}$ on a $\dim E_{f,y} = 1$.

4) a) Montrer que $I_{f,x}$ est un idéal non nul de $\mathbb{K}[X]$.

b) En déduire qu'il existe un et un seul polynôme unitaire, qu'on notera $P_{f,x}(X)$, dans $\mathbb{K}[X]$ tel que pour tout $Q(X) \in \mathbb{K}[X]$, on ait : $Q(X) \in I_{f,x} \iff P_{f,x}|Q$.

On en déduit en particulier que $P_{f,x}(f)(x) = 0$.

5) On note p le degré de $P_{f,x}$.

a) Montrer que pour tout polynôme $Q(X) \in \mathbb{K}[X]$, il existe $(a_0, ..., a_{p-1}) \in \mathbb{K}^p$ tel que

$$Q(f)(x) = \sum_{i=0}^{p-1} a_i f^i(x).$$

b) Montrer que $B(x, p)$ est une base de $E_{f,x}$ et en déduire la dimension de $E_{f,x}$.

6) Montrer que $P_{f,x}|\pi_f$.

2) Démonstration d'un lemme

Soit $f \in \mathscr{L}(E)$.

Le but de cette partie est de démontrer le lemme suivant :

$$(*)\ \textit{il existe } x \in E \textit{ tel que } P_{f,x} = \pi_f.$$

On considère la décomposition de π_f en produit de polynômes irréductibles unitaires dans $\mathbb{K}[X]$:

$$\pi_f(X) = P_1^{\alpha_1}(X)...P_k^{\alpha_k}(X),$$

où $k \in \mathbb{N}^*$, $\alpha_1, ..., \alpha_k \in \mathbb{N}^*$ et $P_1, ..., P_k$ sont irréductibles unitaires dans $\mathbb{K}[X]$ et deux à deux distincts.

1) **Cas où $k = 1$ et $\alpha_1 = 1$:** on a $\pi_f = P_1$.

À l'aide de II.1)6., démontrer $(*)$.

2) **Cas où $k = 1$ et $\alpha_1 \geq 1$:** on a $\pi_f = P_1^{\alpha_1}$.

Soit $B = (e_1, ..., e_n)$ une base de E.

a) Montrer que, pour tout $i \in [\![1,n]\!]$, il existe $\beta_i \leq \alpha_1$ tel que $P_{f,e_i} = P_1^{\beta_i}$.

On note β le maximum de $\{\beta_1, ..., \beta_n\}$.

b) Montrer que $P_1^{\beta}(f) = 0$. (On rappelle que pour tout $x \in E$, on a $P_{f,x}(f)(x) = 0$.)

c) En déduire que $\beta = \alpha_1$ et conclure.

3) **Cas général :** on a $\pi_f(X) = P_1^{\alpha_1}(X)...P_k^{\alpha_k}(X)$.

Pour tout $j \in [\![1,k]\!]$, on pose $E_j = \ker P_j^{\alpha_j}(f)$.

a) Montrer que $E = E_1 \oplus ... \oplus E_k$.

b) Montrer que, pour tout $j \in [\![1,k]\!]$, E_j est stable par f.

On note alors f_j la restriction de f à E_j.

c) Montrer que, pour tout $j \in [\![1,k]\!]$, $\pi_{f_j} | P_j^{\alpha_j}$ et en déduire qu'il existe $\gamma_j \leq \alpha_j$ tel que $\pi_{f_j} = P_j^{\gamma_j}$.

d) On pose $P(X) = P_1^{\gamma_1}(X)...P_k^{\gamma_k}(X)$.

i) Montrer que, pour tout $p \in [\![1,k]\!]$ et tout $x \in E_p$, on a $P(f)(x) = 0$

ii) Montrer que $P(f) = 0$ et en déduire que, pour tout $j \in [\![1,k]\!]$, on a $\gamma_j = \alpha_j$.

e) Des questions c) et d) on déduit que, pour tout $j \in [\![1,k]\!]$, on a $\pi_{f_j} = P_j^{\alpha_j}$.
À l'aide de 2., en déduire que, pour tout $j \in [\![1,k]\!]$, il existe $x_j \in E_j$ tel que

$$P_{f_j,x_j} = P_j^{\alpha_j}.$$

f) Montrer que pour tout $j \in [\![1,k]\!]$ on a $P_{f_j,x_j} = P_{f,x_j}$.
Ainsi, pour tout $j \in [\![1,k]\!]$, il existe $x_j \in E_j$ tel que

$$P_{f,x_j} = P_j^{\alpha_j}.$$

g) On pose $x = x_1 + ... + x_k$.

i) Soit $P \in I_{f,x}$.

Montrer que $\sum_{j=1}^{k} P(f)(x_j) = 0$ puis que, pour tout $j \in [\![1,k]\!]$, on a $P(f)(x_j) = 0$ (utiliser II.2)3.a) et b)).

ii) En déduire que, pour tout $P \in I_{f,x}$ et tout $j \in [\![1,k]\!]$, P_{f,x_j} divise P, puis que π_f divise P.

iii) Montrer que $\pi_f = P_{f,x}$.

III Étude de quelques endomorphismes cycliques

1) a) Dans cette question seulement, on considère $E = \mathbb{K}_{n-1}[X]$ l'espace vectoriel des polynômes dans $\mathbb{K}[X]$ de degré inférieur ou égal à $n-1$.

i) Soit f l'endomorphisme de E défini, pour tout $Q(X) \in E$, par $f(Q(X)) = Q'(X)$ (polynôme dérivé de $Q(X)$).
Montrer que f est un endomorphisme cyclique et nilpotent de E.

ii) Soit g l'application définie par $g : E \longrightarrow \mathbb{K}[X], Q(X) \longmapsto Q(X+1) - Q(X)$.
Montrer que g est un endomorphisme de E et qu'il est cyclique et nilpotent.

b) Cas général : Montrer que si f est un endomorphisme nilpotent de E, alors f est cyclique si et seulement si son indice de nilpotence est égal à n.

2) Dans cette question seulement, on considère $\mathbb{K} = \mathbb{R}$ et $\dim E = 2$.

Soit $f \in \mathscr{L}(E)$ tel qu'il existe $p \in \mathbb{N} \setminus \{0, 1, 2\}$ tel que $f^p = id_E$ et pour tout entier k tel que $0 < k < p$, $f^k \neq id_E$.

Soit B une base quelconque de E et A la matrice de f dans B.

a) Montrer que A est diagonalisable dans $\mathscr{M}_2(\mathbb{C})$.

b) i) Montrer que si λ est une valeur propre réelle de A alors $\lambda = \pm 1$.

ii) En déduire que A n'a pas de valeur propre réelle.

iii) Montrer que, pour tout vecteur non nul y de E, la famille $C = (y, f(y))$ est une base de E.

c) i) Montrer que les valeurs propres de A sont deux nombres complexes conjugués λ_1 et λ_2, et que, plus précisément, il existe k premier avec p tel que $\lambda_1 = e^{2ik\pi/p}$ et $\lambda_2 = e^{-2ik\pi/p}$.

ii) Soit un vecteur non nul y de E et $C = (y, f(y))$ la base de E ainsi construite. Montrer que la matrice de f dans C est $\begin{pmatrix} 0 & -1 \\ 1 & 2\cos(2k\pi/p) \end{pmatrix}$.

IV Caractérisations des endomorphismes cycliques

1) Matrices compagnons

Pour tout polynôme unitaire $P(X) = p_0 + p_1 X + ... + p_{k-1}X^{k-1} + X^k$ de $\mathbb{K}[X]$, on note $C(P)$ et on appelle *matrice compagnon de* $P(X)$ la matrice

$$C(P) = \begin{pmatrix} 0 & \dots & \dots & 0 & -p_0 \\ 1 & 0 & \dots & 0 & -p_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -p_{k-2} \\ 0 & \dots & 0 & 1 & -p_{k-1} \end{pmatrix} \in \mathscr{M}_k(\mathbb{K}).$$

1) Montrer que le polynôme caractéristique de $C(P)$ est égal à $(-1)^k P(X)$.

2) Soient $k \in \mathbb{N}^*$, $(p_0, ..., p_{k-1}) \in \mathbb{K}^k$, $P(X) = p_0 + ... + p_{k-1}X^{k-1} + X^k \in \mathbb{K}[X]$ et $A = C(P) \in \mathscr{M}_k(\mathbb{K})$. On appelle f l'endomorphisme de $\mathbb{K}^k$ canoniquement associé à A et on note $B = (e_1, ..., e_k)$ la base canonique de $\mathbb{K}^k$. Notons p le degré du polynôme π_f.

a) Supposons que $p < k$. Écrivons $\pi_f(X) = q_0 + ... + q_{p-1}X^{p-1} + X^p$, avec $q_0, ..., q_{p-1} \in \mathbb{K}$. Montrer que, pour tout $i \in [\![1, k-1]\!]$, on a $f^i(e_1) = e_{i+1}$ puis $q_0 e_1 + ... + q_{p-1}\, e_p + e_{p+1} = 0$. Conclure sur p.

b) Montrer que

$$\pi_f(X) = (-1)^k P_f(X) = P(X).$$

2) Caractérisations

Dans cette partie, le lemme démontré dans la partie II.2) pourra être utile.

Soit $f \in \mathscr{L}(E)$.

1) Montrer que f est cyclique si et seulement si il existe $x \in E$ tel que $B(x, n)$ soit une base de E.

2) Montrer que f est cyclique si et seulement si il existe $x \in E$ tel que $\deg(P_{f,x}) = n$.

3) Montrer que f est cyclique si et seulement si il existe une base B de E telle que la matrice de f dans B soit égale à $C((-1)^n P_f)$.

4) Montrer que f est cyclique si et seulement si $\pi_f(X) = (-1)^n P_f(X)$.

5) Montrer que f est cyclique si et seulement si il existe une base B de E telle que la matrice de f dans B soit égale à $C(\pi_f)$.

V Cyclicité et diagonalisabilité

Dans cette partie, la propriété énoncée dans IV.2)4. pourra être utile.

1) On suppose f *diagonalisable*. On appelle p le nombre de ses valeurs propres distinctes et on note celles-ci $\lambda_1, ..., \lambda_p$.

   a) Montrer que $\pi_f(X) = \prod_{i=1}^{p}(X - \lambda_i)$.

   b) En déduire que f est cyclique si et seulement si $n = p$.

2) On suppose f *cyclique*.
Montrer que f est diagonalisable si et seulement si f a n valeurs propres distinctes.

PROBLÈME N°2

Dans tout le problème n désigne un nombre entier supérieur ou égal à 2.

Le but de ce problème est d'étudier le groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Notations et conventions

- Les anneaux considérés seront tous commutatifs.
- Les anneaux considérés seront tous unitaires, c'est-à-dire muni d'un élément unité, noté 1, pour leur produit.
- Pour un anneau $(A, +, \times)$, on note $U(A)$ l'ensemble de ses éléments inversibles, *i.e.*

$$U(A) = \{a \in A; \exists b \in A, ab = 1\}.$$

- $[\![1, n]\!]$ désigne l'ensemble des nombres entiers compris entre 1 et n.
- Pour $i, j \in \mathbb{Z}$, $i \wedge j$ désigne le *plus grand diviseur positif commun* à i et j.
- Pour une partie finie A d'un ensemble E, le cardinal de A sera noté $Card(A)$.
- $\varphi(n)$ désigne le cardinal $Card(U(\mathbb{Z}/n\mathbb{Z}))$.
- $\mathbb{P}$ désigne l'ensemble des nombres premiers dans $\mathbb{N}$, $\mathbb{N}^*$ l'ensemble des nombres entiers non nuls.
- Si deux éléments i et j de $\mathbb{Z}$ sont tels que i divise j, alors on le notera $i|j$.
- Sauf mention contraire, la classe de congruence d'un entier relatif x dans $\mathbb{Z}/n\mathbb{Z}$ est notée $\overline{x}$.
- Dans un groupe G, pour tout élément a on note $< a >$ le sous-groupe de G engendré par a. Si $< a >$ est fini, on notera $o(a)$ et on appellera *ordre de* a le nombre $o(a) = Card(< a >)$.

I Calcul de $\varphi(n)$

1) Soient a et b deux entiers supérieurs ou égaux à 2. *On suppose que* $a \wedge b = 1$.

   Pour tout $x \in \mathbb{Z}$, on note $\overline{x}$ (respectivement $\overline{\overline{x}}$ et $\dot{x}$) la classe de congruence de x dans $\mathbb{Z}/a\mathbb{Z}$ (respectivement $\mathbb{Z}/b\mathbb{Z}$ et $\mathbb{Z}/ab\mathbb{Z}$).

   a) Soient x et y dans $\mathbb{Z}$ tels que $\dot{x} = \dot{y}$. Montrer qu'on a $\overline{x} = \overline{y}$ et $\overline{\overline{x}} = \overline{\overline{y}}$.

   b) La question précédente permet de définir l'application

$$f : \mathbb{Z}/ab\mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, \dot{x} \longmapsto (\overline{x}, \overline{\overline{x}}).$$

   i) Montrer que f est un morphisme d'anneaux.

   ii) Montrer que f est injectif.

   iii) En déduire que f est un isomorphisme d'anneaux.

   Ainsi les anneaux $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ sont isomorphes.

2) Soient $k \in \mathbb{N}^*$ et $a_1, ..., a_k$ k entiers deux à deux premiers entre eux.
   Montrer que les anneaux $\mathbb{Z}/(a_1...a_k)\mathbb{Z}$ et $\mathbb{Z}/a_1\mathbb{Z} \times ... \times \mathbb{Z}/a_k\mathbb{Z}$ sont isomorphes.

3) Soient $k \in \mathbb{N}^*$ et $A_1, ..., A_k$ k anneaux.
   Montrer qu'on a $U(A_1 \times ... \times A_k) = U(A_1) \times ... \times U(A_k)$.

4) a) Soit un anneau $(A, +, \times)$. Montrer que $(U(A), \times)$ est un groupe.

b) Soient A, B deux anneaux. Montrer que s'il existe un isomorphisme d'anneaux f de A sur B, alors la restriction $\widetilde{f}$ de f à $U(A)$ induit un isomorphisme de groupes de $U(A)$ sur $U(B)$.

Ainsi les groupes $U(A)$ et $U(B)$ sont isomorphes.

5) Montrer que
$$U(\mathbb{Z}/n\mathbb{Z}) = \{\overline{x}; x \in [\![1, n]\!] \text{ et } x \wedge n = 1\}.$$

6) On suppose (dans cette question seulement) que n est de la forme $n = p^k$ avec $p \in \mathbb{P}$ et $k \in \mathbb{N}^*$.

a) Soit $x \in \mathbb{Z}$. Montrer : $\overline{x} \notin U(\mathbb{Z}/n\mathbb{Z}) \iff p|x$.

b) En déduire que $\varphi(p^k) = p^k - p^{k-1}$.

7) Soit la décomposition de n en produit de nombres premiers : $n = p_1^{\alpha_1}...p_s^{\alpha_s}$, où $s \in \mathbb{N}^*, (p_1, ..., p_s) \in \mathbb{P}^s, (\alpha_1, ..., \alpha_s) \in (\mathbb{N}^*)^s$ et pour tous $i, j \in [\![1, s]\!]$ distincts, $p_i \neq p_j$. Déduire de tout ce qui précède la valeur de $\varphi(n)$.

II Étude de $U(\mathbb{Z}/2^k\mathbb{Z})$

1) Préliminaire

Soient $(G, \times)$ un groupe commutatif d'élément neutre noté e et A et B deux sous-groupes de G.

On appelle AB la partie de G égale à $\{ab; a \in A, b \in B\}$.

1) Montrer que AB est un sous-groupe de G.

2) On suppose que $AB = G$ et $A \cap B = \{e\}$. Montrer que l'application
$$f : A \times B \longrightarrow G, (a, b) \longmapsto ab$$
est un isomorphisme de groupes du groupe produit $A \times B$ sur le groupe G.

Ainsi les groupes $A \times B$ et G sont isomorphes.

3) On suppose que G est fini et de cardinal pair. Écrivons $Card(G) = 2m$ avec $m \in \mathbb{N}^*$. On suppose en outre qu'il existe a et b dans G tels que $o(a) = m$ et $o(b) = 2$ et tels que b n'appartient pas à $< a >$.

a) Soient $i, j \in [\![1, m]\!]$. Montrer que $a^i = a^j$ si, et seulement si, $i = j$.

b) Calculer
$$Card(\{a^i; i \in [\![1, m]\!]\} \cup \{a^i b; i \in [\![1, m]\!]\}).$$

c) En déduire que $G =< a >< b >$.

d) Montrer que les groupes $< a > \times < b >$ et G sont isomorphes.

2) Application

k désigne ici un élément de $\mathbb{N}^*$. On note désormais G_k le groupe $U(\mathbb{Z}/2^k\mathbb{Z})$.

1) Expliciter G_1, G_2 et G_3.

On suppose désormais $k \geq 3$.

2) Montrer que $\overline{5}$ appartient à G_k.

3) a) Soient $i \in \mathbb{N}$ et $x \in \mathbb{Z}$.
Montrer que
$$(1 + 2^{i+2} + x2^{i+3})^2 \equiv 1 + 2^{i+3} + x2^{i+4} \text{ modulo } 2^{2i+4}.$$

b) Montrer que pour tout $i \in \mathbb{N}$, on a

$$5^{2^i} \equiv 1 + 2^{i+2} \text{ modulo } 2^{i+3}.$$

4) En déduire que $o(\overline{5}) = 2^{k-2}$ dans G_k.

5) Montrer que $\overline{-1}$ n'appartient pas au sous-groupe de G_k engendré par $\overline{5}$.

6) Montrer que le groupe G_k est isomorphe à $\mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.