

DS 7

du 11/02/2026

Tout appareil connecté est interdit. Calculatrices interdites.

Faites attention au soin apporté à votre présentation et à la justesse de votre rédaction.

Vous devez choisir entre le **sujet A** comprenant les exercices **1,2,3A** et le **sujet B** comprenant les exercices **1,2,3B**. Pour ce faire, indiquer clairement sur votre première copie, **vosre nom et numéro du sujet**. Toutes les feuilles doivent être numérotées.

Durée : 4 heures.

EXERCICE 1: THÉORÈME DE WILSON

Le but de cet exercice est de montrer le théorème suivant¹.

Théorème de Wilson.

$n \geq 2$ est premier si et seulement si $1 + (n-1)!$ est divisible par n .

PARTIE A - PREMIERS CAS

- ① Vérifier le théorème de Wilson pour $n = 2, 3, 4$.

Dans la suite, on fixe $n > 4$.

PARTIE B - SENS INDIRECT

On suppose ici qu'il existe $p, q \in \llbracket 2, n-1 \rrbracket$, tels que $n = pq$.

- ② Montrer que n divise $(n-1)!$. On pourra faire une disjonction des cas $p = q$ et $p < q$.
- ③ En déduire que $1 + (n-1)!$ n'est pas divisible par n .
- ④ Montrer alors le sens indirect ($\Leftarrow$) du théorème, proprement.

PARTIE C - SENS DIRECT

On suppose que n est premier. Pour tout $k \in \llbracket 1, n-1 \rrbracket$, on appelle φ_k l'application définie sur $\llbracket 1, n-1 \rrbracket$ et qui à tout entier x associe le reste de la division euclidienne de kx par n .

- ⑤ Montrer que $\forall k \in \llbracket 1, n-1 \rrbracket, \forall x \in \llbracket 1, n-1 \rrbracket, \varphi_k(x) \in \llbracket 1, n-1 \rrbracket$.
On pourra donc considérer φ_k comme une application de $\llbracket 1, n-1 \rrbracket$ dans lui-même.
- ⑥ Montrer que pour tout $k \in \llbracket 1, n-1 \rrbracket$, l'application φ_k est injective.
On écrira explicitement la définition d'injectivité pour φ_k .
- ⑦ (a) Soit $k \in \llbracket 1, n-1 \rrbracket$. Montrer l'existence de $a_0, b_0 \in \mathbb{Z}$ tel que $a_0 n + b_0 k = 1$.
 (b) Donner tous les couples $(a, b) \in \mathbb{Z}^2$ solution de $an + bk = 1$.
 (c) En déduire qu'il existe un $b' \in \llbracket 1, n-1 \rrbracket$ tel que $b'k \equiv 1 \pmod n$.
- ⑧ En déduire que $\forall k \in \llbracket 1, n-1 \rrbracket, \exists! b' \in \llbracket 1, n-1 \rrbracket, \varphi_k(b') = 1$.
- ⑨ Montrer que $\varphi_k(k) = 1 \iff n \mid (k-1)(k+1)$ et en déduire que $\varphi_k(k) = 1 \iff (k = 1 \text{ ou } k = n-1)$.
- ⑩ Justifier que, pour tout $x, y \in \llbracket 2, n-2 \rrbracket, \varphi_y(x) = 1 \iff \varphi_x(y) = 1$.

¹Ce théorème fut énoncé par John Wilson en 1770 selon une conjecture émise par son ex-étudiant Edward Waring. Aucun des deux mathématiciens n'est parvenu à démontrer lui-même ce résultat.

- ⑪ Prenons b' comme dans la question ⑧. En regroupant dans le produit $2 \times 3 \times \dots \times (n-2)$ les facteurs 2 à 2 pour former les produits du type kb' , montrer que $(n-2)!$ peut s'écrire sous la forme $nq+1$, avec $q \in \mathbb{Z}$.
- ⑫ En déduire enfin que $1 + (n-1)!$ est divisible par n .

EXERCICE 2

Soit $n \in \mathbb{N} \setminus \{0\}$. Soit $\mathbb{K}$ un corps.

- ① Justifier qu'il existe un couple $(P, Q) \in \mathbb{K}[X]$ tels que $(1-X)^n P + X^n Q = 1$.
- ② Montrer qu'il est possible de choisir P, Q de degrés strictement inférieurs à n , et que ce couple est alors unique.
On pensera à écrire toutes les solutions à l'équation. On montrera proprement l'unicité.
 On notera ce couple de degré minimal, (P_0, Q_0) .
- ③ Montrer que $Q_0(X) = P_0(1-X)$. *On pensera à utiliser l'unicité établie*
- ④ Montrer qu'il existe $\lambda \in \mathbb{R}$ tel que $(1-X)P'_0(X) - nP_0(X) = \lambda X^{n-1}$.
 Posons $P_0 = \sum_{k=0}^{n-1} p_k X^k$.
- ⑤ Montrer que $(2n-1)p_{n-1} = \lambda$, que $p_0 = 1$ et que, pour tout $k \in \llbracket 0, n-2 \rrbracket$, $(k+1)p_{k+1} = p_k(n+k)$
- ⑥ En déduire les coefficients de P_0 .
- ⑦ Donner alors les solutions du système de congruence sur $\mathbb{C}(X)$,
$$\begin{cases} A = X^2 + 1 & [X^n], \\ A = X + 2 & [(1-X)^n]. \end{cases}$$

EXERCICE 3A

On pose A le polynôme à coefficients rationnels $A = X^3 - X - 1 \in \mathbb{Q}[X]$

PARTIE A - RACINES DE A

- ① Montrer que le polynôme A possède une seule racine réelle α .
- ② Montrer que si $\frac{p}{q}$ est une racine rationnelle de P , avec p et q premiers entre eux, alors $|p| = |q| = 1$.
- ③ En déduire que $\alpha \notin \mathbb{Q}$.
- ④ Montrer alors que A est un polynôme irréductible sur $\mathbb{Q}$. Le résultat est-il encore vrai sur $\mathbb{R}$? Expliquer.
- ⑤ Soit β une des deux autres racines de A . Donner alors l'autre racine de A en fonction de β .
- ⑥ Exprimer $\operatorname{Re}(\beta)$ et $|\beta|^2$ en fonction de α , en utilisant les relations coefficients racines.

PARTIE B - CORPS QUADRATIQUE

- ⑦ Donner le quotient et le reste de la division euclidienne de $X^5 + 2X^4 - 3X^3$ par $X^3 - X - 1$.
- ⑧ Soit $x = \alpha^5 + 2\alpha^4 - 3\alpha^3$. Montrer que $x = \tilde{R}(\alpha)$, où $R \in \mathbb{Q}_2[X]$ est un polynôme bien choisi.
 On note $\mathbb{Q}[\alpha]$ le sous anneau de $\mathbb{R}$ engendré par $\mathbb{Q} \cup \{\alpha\}$. Donc toutes les sommes et tous les produits de ces éléments sont dans $\mathbb{Q}[\alpha]$.
 Par exemple, $\alpha, 3\alpha - 8, \frac{4}{3}\alpha^4 - \frac{1}{12}\alpha + 10, 2\alpha^8 \in \mathbb{Q}[\alpha]$
- ⑨ Montrer que $\frac{4}{3}\alpha^4 - \frac{1}{12}\alpha + 10 = \frac{4}{3}\alpha^2 + \frac{15}{12}\alpha + 10$.
- ⑩ Montrer que $\mathbb{Q}[\alpha] = \{\tilde{P}(\alpha) \mid P \in \mathbb{Q}_2[X]\}$, où $\mathbb{Q}_2[X]$ désigne l'ensemble des polynômes de $\mathbb{Q}[X]$ de degré ≤ 2 .
*Dans l'ensemble ci-dessus, $|$ est la séparation habituelle, et **ne veut pas dire "divise"**.*

- (11) Soit $B = X^2 + 2X$. Déterminer deux polynômes U et V de $\mathbb{Q}[X]$ tels que $AU + BV = 1$.
Il est normal de trouver des coefficients de U et V dont les dénominateurs sont égaux à 7.
- (12) Montrer que $y = \alpha^2 + 2\alpha$ est inversible dans l'anneau $\mathbb{Q}[\alpha]$ et donner son inverse.
On pourra utiliser l'égalité juste démontrée.
- (13) Montrer, en s'inspirant de l'exemple des deux questions précédentes avec B , que $\mathbb{Q}[\alpha]$ est un corps.
On expliquera proprement chaque étape.
- (14) Quels sont les isomorphismes de ce corps dans lui-même?
On admettra qu'un tel automorphisme laisse invariant les rationnels.

PARTIE C - UNE DÉCOMPOSITION

- (15) Donner la décomposition en élément simples de $\frac{X^3 + 3X^2 - X - 2}{X^3 - X - 1}$ sur $\mathbb{R}$, en fonction de α .
Les relations de la question (6) seront utiles.

EXERCICE 3B: UNE ÉQUATION POLYNÔMIALE

Soient $a, b \in \mathbb{C}$ fixés. Pour tout $P \in \mathbb{C}[X]$, on dit que P est solution de $(*)$ si

$$P(X^2) = P(X + a)P(X + b).$$

Lorsque l'on parle de racines dans ce problème, il s'agit toujours de racines dans $\mathbb{C}$.

Pour tout $P \in \mathbb{C}[X]$, on note $\bar{P}$ le polynôme dont les coefficients sont les conjugués de ceux de P .

On admet que pour tous $P, Q \in \mathbb{C}[X]$,

$$\overline{P + Q} = \bar{P} + \bar{Q}, \quad \overline{PQ} = \bar{P}\bar{Q}, \quad \overline{P \circ Q} = \bar{P} \circ \bar{Q}.$$

PARTIE A - GÉNÉRALITÉS

- (1) Déterminer les solutions constantes de $(*)$.
 On note désormais $\mathcal{E}$ l'ensemble des solutions non constantes.
- (2) Montrer que tout élément de $\mathcal{E}$ est unitaire.

PARTIE B - CAS OÙ $a = b$

On suppose dans cette question que $a = b$.

- (3) Soit $P \in \mathcal{E}$. Montrer que 0 est la seule racine de P .
On pourra prendre une racine non nulle α , et arriver à une contradiction, en comparant le nombre de racines distinctes de $P(X + a)^2$ et le nombre de racines distinctes de $P(X^2)$.
- (4) En déduire, en fonction de a , une description explicite de $\mathcal{E}$.

PARTIE C - UNICITÉ DES SOLUTIONS DE MÊME DEGRÉ

Soient $P, Q \in \mathcal{E}$ de même degré. On pose

$$D(X) = P(X) - Q(X), \quad R(X) = P(X + a)D(X + b) + D(X + a)Q(X + b).$$

- (5) Montrer que $D(X^2) = R(X)$ et que, si $P \neq Q$, $\deg R = \deg P + \deg D$.
- (6) Justifier que $\deg D < \deg P$.
- (7) En déduire que $P = Q$.
- (8) Déduire du résultat précédent que si a et b sont réels, alors $\mathcal{E} \subset \mathbb{R}[X]$.

PARTIE D - CAS $a = 0$ ET $b = -1$

On suppose dans cette question que $a = 0$ et $b = -1$. Soit $P \in \mathcal{E}$.

- (9) Montrer que si α est une racine de P , alors α^{2^n} est racine de P pour tout $n \in \mathbb{N}$.
- (10) En déduire que toute racine α de P vérifie $\alpha = 0$ ou $|\alpha| = 1$.
- (11) Montrer que 0 n'est pas racine de P .
- (12) Montrer que pour toute racine α de P , on a $|\alpha + 1| = 1$.
- (13) Montrer qu'il existe $n \in \mathbb{N}^*$ tel que $P = (X^2 + X + 1)^n$.
- (14) En déduire une description explicite de $\mathcal{E}$.

PARTIE E - FORME DE L'ENSEMBLE $\mathcal{E}$

La suite du problème suppose désormais $\mathcal{E}$ non vide.

- (15) Montrer que $\mathcal{E}$ est stable par produit.
- (16) Soient $A, B \in \mathbb{C}[X]$ et $n \in \mathbb{N}^*$. On pose $U = A^n - B^n$, et $V = \prod_{k=0}^{n-1} \left(A - e^{\frac{2ik\pi}{n}} B \right)$.
Montrer que $U = V$.
- (17) En déduire que pour tout polynôme unitaire P et tout $n \geq 1$, $P^n \in \mathcal{E} \implies P \in \mathcal{E}$.
- (18) Justifier l'existence d'un unique polynôme M de degré minimal dans $\mathcal{E}$.
On note $\lambda_1, \dots, \lambda_r$ les racines distinctes de M et $m_1, \dots, m_r$ leurs multiplicités respectives, de sorte que $M = \prod_{i=1}^r (X - \lambda_i)^{m_i}$.
- (19) Soit $P \in \mathcal{E}$. On note $d = \deg(P) \wedge \deg(M)$.
 - (a) Justifier l'existence s, t premiers entre eux tels que $\deg(P) = ds$ et $\deg(M) = dt$.
 - (b) Montrer que $P^t = M^s$, puis que $P = \prod_{i=1}^r (X - \lambda_i)^{p_i}$ pour certains $p_1, \dots, p_r \in \mathbb{N}^*$.
On pose alors $Q = \prod_{i=1}^r (X - \lambda_i)^{m_i \wedge p_i}$.
 - (c) Montrer que $P = Q^s$ et $M = Q^t$, puis que P est une puissance de M .
- (20) Dédire des questions (15), (18), (19) l'ensemble $\mathcal{E}$.