Répondez directement sur l'énoncé en **détaillant vos calculs** et **justifiant vos raisonnements**.

Nom: **CORRIGÉ**

1. Soit $\mathbf{F}_{16}$ le corps à 16 éléments obtenu en adjoignant à $\mathbf{F}_2$ un élément α tel que $\alpha^4 = \alpha + 1$, vu comme un espace vectoriel sur $\mathbf{F}_2$. En travaillant par rapport à la base $\mathcal{B} = (1,\, \alpha,\, \alpha^2,\, \alpha^3)$, donner la représentation matricielle de l'application linéaire $\psi(x) = x^2 + x$ et en déduire les solutions dans $\mathbf{F}_{16}$ de l'équation $x^2 + x + 1 = 0$.

Tout élément $x \in \mathbf{F}_{16}$ s'écrit uniquement sous la forme

$$x = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3, \qquad (a_0,\, a_1,\, a_2,\, a_3) \in (\mathbf{F}_2)^4;$$

en d'autres termes, les coordonnées de x par rapport à la base $\mathcal{B}$ sont $\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$. On calcule alors

$$\begin{aligned} \psi(x) = x^2 + x &= (a_0 + a_1\alpha^2 + a_2\alpha^4 + a_3\alpha^6) + (a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3) \\ &= a_2 + (a_1 + a_2)\alpha + (a_1 + a_2 + a_3)\alpha^2 \end{aligned}$$

en utilisant les relations $\alpha^4 = \alpha + 1$ et $\alpha^6 = \alpha^2 \cdot \alpha^4 = \alpha^3 + \alpha$. Donc

$${}_{\mathcal{B}}\big[\psi(x)\big] = \begin{bmatrix} 0 \\ a_1 + a_2 \\ a_1 + a_2 + a_3 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Ou alors, de façon équivalente, on calcule $\psi(1) = 0$, $\psi(\alpha) = \alpha + \alpha^2$, $\psi(\alpha^2) = 1 + \alpha + \alpha^2$, $\psi(\alpha^3) = \alpha^2$ et on dispose les coordonnées en colonnes.

Pour résoudre l'équation $x^2 + x + 1 = 0$: on ne peut *pas* ici utiliser la formule usuelle (pourquoi ?), mais on peut très bien résoudre le système d'équations linéaires $\psi(x) = 1$ et effectuant de la réduction gaussienne sur la matrice augmentée

$$\left[\begin{array}{cccc|c} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right] \sim \left[\begin{array}{cccc|c} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

qui nous dit que la solution générale s'écrit

$$x = a_0 + \alpha + \alpha^2, \quad a_0 \in \mathbf{F}_2.$$

En d'autres termes : les solutions sont $\alpha + \alpha^2$ et $1 + \alpha + \alpha^2$.

Remarque : Si on note β l'une ou l'autre de ces solutions, on remarque que $\mathbf{F}_2(\beta)$ avec $\beta^2 = \beta + 1$ est une copie de $\mathbf{F}_4$ réalisée comme sous-corps de $\mathbf{F}_{16}$.

2. Donner une formule pour le terme général de la suite $(x_n)_{n=0}^{\infty}$ de nombres réels définie par

$$x_0 = 0, \quad x_1 = 1 \quad \text{et} \quad x_n = x_{n-1} + 2\,x_{n-2} + 1 \quad (n \geqslant 2).$$

Bonne pratique : on peut observer les premiers termes pour référence future :

$$(0, 1, 2, 5, 10, 21, 42, 85, 170, 341, \ldots)$$

Il s'agit d'une équation de récurrence linéaire d'ordre 2 à coefficients constants :

- Solution générale de l'équation homogène $x_n = x_{n-1} + 2\,x_{n-2}$ $(n \geqslant 2)$. Si on cherche une solution géométrique, posant $x_n = \lambda^n$ on voit que λ doit satisfaire l'équation algébrique

$$\lambda^2 = \lambda + 2, \qquad \text{soit} \qquad \lambda^2 - \lambda - 2 = (\lambda - 2)(\lambda + 1) = 0$$

  dont les solutions sont $\lambda = 2$ et $\lambda = -1$.

  On sait donc que la solution générale de l'équation homogène s'écrit

$$x_n = A \cdot 2^n + B \cdot (-1)^n,$$

  où A et B sont des constantes à déterminer.

- Solution particulière de l'équation avec second membre : celui-ci étant constant on peut chercher une solution particulière de même forme et on trouve $x_n = -\frac{1}{2}$.

- Par superposition linéaire, la solution générale de l'équation avec second membre s'écrit

$$x_n = A \cdot 2^n + B \cdot (-1)^n - \frac{1}{2}.$$

- En imposant les conditions initiales $x_0 = 0$ et $x_1 = 1$, on trouve les valeurs des constantes $A = \frac{2}{3}$ et $B = -\frac{1}{6}$, d'où la réponse finale

$$x_n = \frac{2}{3} \cdot 2^n - \frac{1}{6} \cdot (-1)^n - \frac{1}{2} = \frac{3 \cdot 2^{n+1} + (-1)^{n+1} - 3}{6} \qquad (n \geqslant 0).$$