Devoir surveillé n°07 : corrigé

Solution 1.

1. **a.** On sait que $\phi(x) \equiv 0[q]$ donc $(x-1)\phi(x) \equiv 0[q]$. D'où $x^p - 1 \equiv 0[q]$ i.e. $x^p \equiv 1[q]$. Ainsi $p \in A$.

   b. Puisque $\phi(x) \equiv 0[q]$, il existe $r \in \mathbb{Z}$ tel que $\phi(x) = rq$. Ainsi $1+\sum_{k=1}^{p-1} x^k = rq$ d'où $rq - x\sum_{k=1}^{p-1} x^{k-1} = 1$. Or $\sum_{k=1}^{p-1} x^{k-1} \in \mathbb{Z}$ donc x et q sont premiers entre eux en vertu du théorème de Bézout.

   Remarque. On peut également remarquer que, puisque $x^p \equiv 1[q]$ d'après la question précédente, il existe $r \in \mathbb{Z}$ tel que $x^p - kq = 1$, ce qui permet à nouveau d'affirmer que $x \wedge q = 1$ grâce au théorème de Bézout. ■

   Puisque x est premier avec le nombre premier q, $x^{q-1} \equiv 1[q]$ en vertu du petit théorème de Fermat. Ainsi $q-1 \in A$.

   c. D'après une des deux questions précédentes, A est non vide. Comme c'est une partie de $\mathbb{N}$, A possède un plus petit élément.

   d. Il existe $(k,r) \in \mathbb{N}^2$ tel que $a = km + r$ et $0 \leqslant r \leqslant m-1$. Puisque $a \in A$, $x^a \equiv 1[q]$ i.e. $x^{km+r} \equiv 1[q]$ ou encore $(x^m)^k x^r \equiv 1[q]$. Or $m \in A$ donc $x^m \equiv 1[q]$. Il s'ensuit que $x^r \equiv 1[q]$. On ne peut avoir $r > 0$ sinon r appartiendrait à A et le fait que $r \leqslant m-1$ contredirait la minimalité de m. C'est donc que $r = 0$ et que m divise A.

   e. Raisonnons par l'absurde et supposons $m = 1$. On a donc $x \equiv 1[q]$. Il s'ensuit que $\phi(x) \equiv p[q]$. Or $\phi(x) \equiv 0[q]$ donc $p \equiv 0[q]$. Ainsi q divise p. Comme p est premier, on a donc $q = 1$ (impossible car q est premier) ou $q = p$ (impossible car p et q sont distincts). On aboutit à une contradiction de sorte que $m \neq 1$.

   f. D'après la question **1.a**, $p \in A$. D'après la question **1.d**, m divise p. Or p est premier donc ses seuls diviseurs positifs sont 1 et p. De plus, $m \neq 1$ d'après la question précédente donc $m = p$.

   g. D'après la question **1.b**, $q-1 \in A$ et toujours d'après la question **1.d**, $m = p$ divise $q-1$. Ceci signifie que $q - 1 \equiv 0[p]$ i.e. $q \equiv 1[p]$.

2. **a.** On a clairement $\phi(q_1q_2\dots q_r) \geqslant 2$ donc $\phi(q_1q_2\dots q_r)$ possède un diviseur premier q'. Ainsi $\phi(q_1q_2\dots q_r) \equiv 0[q']$. L'équation $\phi(x) \equiv 0[q']$ possède donc une solution, à savoir $q_1q_2\dots q_r$. Par hypothèse, ceci signifie que q' est l'un des q_i. Il existe donc $i \in [\![1,r]\!]$ tel que

   $$\phi(q_1q_2\dots q_r) \equiv 0[q_i]$$

   b. Tout d'abord, $\phi(q_1q_2\dots q_r) = 1 + \sum_{k=1}^{p-1}(q_1q_2\dots q_r)^k$. De plus, pour $k \in [\![1,p-1]\!]$, $(q_1q_2\dots q_r)^k$ est un multiple de q_i donc $(q_1q_2\dots q_r)^k \equiv 0[q_i]$. Il s'ensuit que $\phi(q_1q_2\dots q_r) \equiv 1[q_i]$. D'après la question précédente, $\phi(q_1q_2\dots q_r) \equiv 0[q_i]$ donc $1 \equiv 0[q_i]$ i.e. q_i divise 1, ce qui est absurde.

3. D'après la question précédente, il existe un nombre infini de nombres premiers q tels que l'équation $\phi(x) \equiv 0[q]$ admette une solution. Il existe donc évidemment une infinité de nombres premiers q *distincts de* p tels que l'équation $\phi(x) \equiv 0[q]$ admette une solution. La question **1** montre alors que $q \equiv 1[p]$ i.e. q est de la forme $1+kp$ avec $k \in \mathbb{N}^*$ (on ne peut avoir $k \leqslant 0$ car $q \geqslant 2$ en tant que nombre premier).

Solution 2.

1. Clairement $F \subset E$. La suite nulle est clairement 4-périodique. Enfin, une combinaison linéaire de suites 4-périodiques est bien 4-périodique. Ainsi F est bien un sous-espace vectoriel de E.

2. Soit $(u_n) \in G$. Alors pour tout $n \in \mathbb{N}$,
   $$u_{n+4} = u_{n+2} = u_n$$
   Donc $(u_n) \in F$.
   De même, si $(u_n) \in H$. Alors pour tout $n \in \mathbb{N}$,
   $$u_{n+4} = -u_{n+2} = u_n$$
   Donc $(u_n) \in F$.
   G et H sont bien inclus dans F.

3. On prouve sans difficulté qu'en posant pour tout $n \in \mathbb{N}$,

$$a_n = 1 \qquad b_n = (-1)^n \qquad c_n = \cos(n\pi/2) \qquad d_n = \sin(n\pi/2)$$

alors

$$G = \text{vect}((a_n), (b_n)) \qquad H = \text{vect}((c_n), (d_n))$$

Ainsi G et H sont bien des sous-espaces vectoriels de F et les familles $((a_n), (b_n))$ et $((c_n), (d_n))$ engendrent respectivement G et H.

4. Soit $(u_n) \in G \cap H$. Alors pour tout $n \in \mathbb{N}$, $u_{n+2} = u_n = -u_n$ de sorte que la suite (u_n) est nulle. Ainsi $F \cap G = \{0_E\}$. F et G sont bien en somme directe.
Puisque G et H sont inclus dans F, $G \oplus H \subset F$. Réciproquement, soit $(u_n) \in F$ et posons $v_n = \frac{u_n+u_{n+2}}{2}$ et $w_n = \frac{u_n-u_{n+2}}{2}$ pour tout $n \in \mathbb{N}$. Alors, on a clairement $(u_n) = (v_n) + (w_n)$.
Remarquons tout d'abord que $u_{n+4} = u_n$ pour tout $n \in \mathbb{N}$ puisque $(u_n) \in H$. Alors pour tout $n \in \mathbb{N}$,

$$v_{n+2} - v_n = \frac{u_{n+2} + u_{n+4}}{2} - \frac{u_n + u_{n+2}}{2} = 0$$
$$w_{n+2} + w_n = \frac{u_{n+2} - u_{n+4}}{2} + \frac{u_n - u_{n+2}}{2} = 0$$

Ainsi $(v_n) \in G$ et $(w_n) \in H$, puis $(u_n) \in G \oplus H$ de sorte que $F \subset G \oplus H$. Par double inclusion, $F = G \oplus H$.

5. Puisque

$$F = G \oplus H = \text{vect}((a_n), (b_n)) \oplus \text{vect}((c_n), (d_n)) = \text{vect}((a_n), (b_n), (c_n), (d_n))$$

la famille $((a_n), (b_n), (c_n), (d_n))$ engendre F.

Solution 3.

1. On trouve sans peine que $F = \text{vect}((1, 1, 0), (0, 1, 1))$ donc F est bien un sous-espace vectoriel de E.
Par ailleurs,

$$\begin{cases} x + y - z = 0 \\ x - y - z = 0 \end{cases} \iff \begin{cases} y = 0 \\ x = z \end{cases}$$

donc $G = \text{vect}((1, 0, 1))$. Ainsi G est bien un sous-espaces vectoriel de E.

2. Une résolution de système montre que $F \cap G = \{(0, 0, 0)\}$. Par ailleurs, la question précédente montre que $\dim F = 2$ et $\dim G = 1$ puisque les familles $((1, 1, 0), (0, 1, 1))$ et $((1, 0, 1))$ sont clairement libres. Ainsi $\dim F + \dim G \dim E$ donc F et G sont bien supplémentaires dans E.

3. On remarque que $(1, 2, 3) = (0, 2, 2) + (1, 0, 1)$. On vérifie sans peine que $(0, 2, 2) \in F$ et que $(1, 0, 1) \in G$. Ainsi $(0, 2, 2)$ est le projeté de $(1, 2, 3)$ sur F parallélement à G tandis que $(1, 0, 1)$ est le projeté de $(1, 2, 3)$ sur G parallélement à F.

Solution 4.

1. Clairement $F \subset E$. Soient $(y_1, y_2) \in F^2$ et $(\lambda, \mu) \in \mathbb{R}^2$. Alors pour tout $x \in \mathbb{R}$,

$$(\lambda y_1 + \mu y_2)''(x) = \lambda y_1''(x) + \mu y_2''(x) = \lambda(1 + x^2)y_1(x) + \mu(1 + x^2)y_2(x) = (1 + x^2)(\lambda y_1 + \mu y_2)(x)$$

Donc $\lambda y_1 + \mu y_2$ est solution de $(\mathcal{E})$ et appartient donc à F. Ainsi F est un sous-espace vectoriel de E.

2. f est clairement de classe $\mathcal{C}^2$ sur $\mathbb{R}$ et

$$\forall x \in \mathbb{R}, f'(x) = xe^{\frac{x^2}{2}} = xf(x)$$

puis

$$\forall x \in \mathbb{R}, f''(x) = f(x) + xf'(x) = f(x) + x^2 f(x) = (1 + x^2)f(x)$$

Ainsi $f \in F$.
Puisque la fonction $\varphi\colon t \mapsto e^{-t^2}$ est continue sur $\mathbb{R}$, le théorème fondamental de l'analyse permet d'affirmer que $\psi\colon x \mapsto \int_0^x e^{-t^2}\,dt$ est une primitive de φ sur $\mathbb{R}$. Puisque $g = f\psi$, g est de classe $\mathcal{C}^1$ et

$$g' = f'\psi + f\psi' = f'\psi + f\varphi$$

On en déduit que g' est elle-même de classe $\mathcal{C}^1$ (donc g est de classe $\mathcal{C}^2$) et que

$$g'' = f''\psi + f'\psi' + f'\varphi + f\varphi' = f''\psi + 2f'\varphi + f\varphi'$$

Alors pour tout $x \in \mathbb{R}$,

$$g''(x) = f''(x)\psi(x) + 2f'(x)\varphi(x) + f(x)\varphi'(x) = (1+x^2)f(x)\psi(x) + 2xf(x)\varphi(x) - 2xf(x)\varphi(x) = (1+x^2)g(x)$$

g appartient donc bien à F.

3. Soit $(v, w) \in F^2$. Alors pour tout $x \in \mathbb{R}$,

$$(v'w - vw')'(x) = v''(x)w(x) - v(x)w''(x) = (1+x^2)v(x)w(x) - (1+x^2)v(x)w(x) = 0$$

La fonction $v'w - vw'$ est donc constante sur $\mathbb{R}$.

4. Conformément à l'indication de l'énoncé, on calcule la dérivée de h/f.

$$(h/f)' = \frac{h'f - hf'}{f^2}$$

Puisque h et f appartiennent à F, la question précédente montre que $h'f - hf'$ est constante. Notons β cette constante réelle. Ainsi $(h/f)' = \frac{\beta}{f^2}$. Autrement dit, pour tout $x \in \mathbb{R}$,

$$(h/f)'(x) = \beta e^{-x^2} = \beta\varphi(x) = \beta\psi'(x)$$

Il existe donc une constante réelle α telle que

$$h/f = \beta\psi + \alpha$$

On en déduit que

$$h = \beta f\psi + \alpha f = \alpha f + \beta g$$

5. Puisque f et g appartient au sous-espace vectoriel F, $\text{vect}(f, g) \subset F$. La question précédente montre l'inclusion réciproque. Ainsi $F = \text{vect}(f, g)$.

6. La famille (f, g) engendre F. Montrons que cette famille est libre. Soit donc $(\alpha, \beta) \in \mathbb{R}^2$ tel que $\alpha f + \beta g = 0$. En évaluant en 0, on obtient $\alpha = 0$. On a donc $\beta g = 0$. En dérivant et en évaluant en 0, on obtient $\beta g'(0) = 0$. Or

$$g'(0) = f'(0)\psi(0) + f(0)\varphi(0) = 1$$

de sorte que $\beta = 0$. La famille (f, g) est donc également libre : c'est donc une base de F de sorte que $\dim F = 2$.