Université Abdelmalek Essaadi
ENSAH D'AL-Hoceima
A.P., Première année
Année universitaire 2019/2020

Correction du Devoir Libre 1 du Module AP21 : "Algèbre Linéaire"

Problème 1

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie $n \geq 2$.

Définition 0.1 *On appelle* **transvection** *de E tout automorphisme $\mathcal{T}$ de E différent de id_E possédant les propriétés suivantes :*

P_1 *: Il existe un hyperplan H de E tel que $\forall x \in H$, $\mathcal{T}(x) = x$,*

P_2 *: $\forall x \in E$, $\mathcal{T}(x) - x \in H$.*

1. (a) Montrer que pour tout hyperplan H de E, il existe une forme linéaire ϕ sur E telle que $H = \text{Ker}(\phi)$.
   (b) Que peut-on dire de deux formes linéaires définissant le même hyperplan ?
   (c) Soient H_1 et H_2 deux hyperplans de E distincts,
   montrer que $H_1 + H_2 = E$, puis calculer $\dim(H_1 \cap H_2)$.
2. Soit $\mathcal{T}$ une transvection de E,
   (a) Montrer que l'hyperplan H associé à $\mathcal{T}$ est unique. (**Indication** : *raisonner par l'absurde en prenant H et H′ tels que $H \neq H'$ et considérer $H + H' = E$*).
   *H est appelé hyperplan de transvection de $\mathcal{T}$.
   (b) Montrer que $\text{Ker}(\mathcal{T} - id_E) = H$, puis en déduire qu'il existe une droite $\mathcal{D}$ telle que :
   $$P_3 : \quad \forall x \in E, \quad \mathcal{T}(x) - x \in \mathcal{D}.$$
   (c) Si ϕ est une forme linéaire définissant H, déterminer un vecteur u de E tel que
   $$P_4 : \quad \forall x \in E, \quad \mathcal{T}(x) = x + \phi(x).u.$$
   (d) **Réciproquement**, montrer que si Φ est une forme linéaire non nulle de E et $u \in \text{Ker}(\Phi)\ \{0_E\}$, alors $\mathcal{T} : E \to E$, $x \mapsto \mathcal{T}(x) = x + \Phi(x).u$ est une transvection de E. Déterminer son hyperplan et sa droite.
   (e) Soit $H = \text{Ker}(\Phi)$ un hyperplan de E. On note $\mathbb{T}(H)$ l'ensemble de toutes les transvections sur E d'hyperplan H et $G = \mathbb{T}(H) \cup \{id_E\}$.
      i. Montrer que $(G, \circ)$ est un groupe ou plutôt sous-groupe de $(Aut(E), \circ)$ où $Aut(E) = GL(E)$.
      ii. Soit $\mathscr{L} : (H, +) \to (G, \circ)$, $u \mapsto \mathcal{T}_u$ où $\mathcal{T}_u : E \to E$, $x \mapsto \mathcal{T}_u(x) = x + \Phi(x).u$.
      Montrer que $\mathscr{L}$ est un isomorphisme de groupe, et que $(G, \circ)$ est abélien.
3. (a) Soit $\mathcal{U}$ une involution de E, c'est à dire $\mathcal{U} \in \mathscr{L}(E)$ et $\mathcal{U}^2 = id_E$.
   On pose $E_1(\mathcal{U}) = \text{Ker}(\mathcal{U} - id_E)$ et $E_{-1}(\mathcal{U}) = \text{Ker}(\mathcal{U} + id_E)$.
      i. Montrer que $E = E_1(\mathcal{U}) \oplus E_{-1}(\mathcal{U})$

ii. Dans cette question, on suppose que $\dim(E_1(\mathcal{U})) = 1$.

A. Soit $a \in E$ tel que $E_1(\mathcal{U}) = \mathbb{R}.a$. Montrer qu'il existe $\varphi \in \mathscr{L}(E, \mathbb{R})$ une forme linéaire de E telle que $\mathrm{Ker}(\varphi) = E_{-1}(\mathcal{U})$ et $\varphi(a) = 2$.

B. En déduire qu'il existe $a \in E$ et $\varphi \in \mathscr{L}(E, \mathbb{R})$ tels que $\forall x \in E$, $\mathcal{U}(x) = -x + \varphi(x).a$.

C. Soit $\mathcal{V}$ une autre involution de E telle que $E_1(\mathcal{U}) = E_1(\mathcal{V})$.
*Montrer qu'il existe $\psi \in \mathscr{L}(E, \mathbb{R})$ telle que $\forall x \in E$, $\mathcal{V}(x) = -x + \psi(x).a$.
*En déduire que $\mathcal{U} \circ \mathcal{V}$ est une transvection.

(b) i. Soit une transvection $\mathcal{T}$ et $\sigma \in \mathrm{Aut}(E)$ un automorphisme de E.
Montrer que $\sigma \circ \mathcal{T} \circ \sigma^{-1}$ est une transvection, puis déterminer son hyperplan H et sa droite $\mathcal{D}$.

ii. Prouver que si $\mathcal{T}_1$ et $\mathcal{T}_2$ sont deux transvections, alors il existe $\sigma \in \mathrm{Aut}(E)$ tel que $\mathcal{T}_2 = \sigma \circ \mathcal{T}_1 \circ \sigma^{-1}$

Solution : Considérons un $\mathbb{R}$-espace vectoriel E de dimension finie $n \geq 2$.

Définition 0.2 *On appelle* **transvection** *de E tout automorphisme $\mathcal{T}$ de E différent de* id_E *possédant les propriétés suivantes :*

P_1 *: Il existe un hyperplan H de E tel que $\forall x \in H$, $\mathcal{T}(x) = x$,*

P_2 *: $\forall x \in E$, $\mathcal{T}(x) - x \in H$.*

1. (a) Montrons que pour tout hyperplan H de E, il existe une forme linéaire ϕ sur E telle que $H = \mathrm{Ker}(\phi)$: en effet, soit H un hyperplan de E.
H est un hyperplan de E si et seulement si il existe $a \in E$ avec $a \notin H$ tel que

$$E = H \oplus \mathbb{R}\, a.$$

Soit $x \in E$, alors il existe un unique $h \in H$ et un unique $\lambda \in \mathbb{R}$ tel que $x = h + \lambda\, a$.
On définit l'application $\phi\,:\, E \to \mathbb{R}$, $x \mapsto \phi(x) = \lambda$.
L'application ϕ est linéaire, en effet, soient $x = h + \lambda\, a$ et $x' = h' + \lambda'\, a$ dans E, alors $x + x' = (h + h') + (\lambda + \lambda')\, a$, donc il vient

$$\phi(x + x') = \lambda + \lambda' = \phi(x) + \phi(x')$$

ceci d'une part et d'autre pour $\alpha \in \mathbb{R}$ on a $\alpha\, x = \alpha\, h + (\alpha\, \lambda)\, a$ où $\alpha\, h \in H$, alors

$$\phi(\alpha\, x) = \alpha\, \lambda = \alpha\, \phi(x)$$

d'où ϕ est linéaire.
Montrons que $\mathrm{Ker}(\phi) = H$: en effet, soit $x \in H$, alors $x = x + 0\, a$, donc $\phi(x) = 0$, d'où $x \in \mathrm{Ker}(\phi)$, soit $H \subset \mathrm{Ker}(\phi)$.
Soit $x \in \mathrm{Ker}(\phi)$, alors $x = h + \lambda\, a$ et $\phi(x) = 0 = \lambda$, donc $x = h \in H$,
d'où $\mathrm{Ker}(\phi) \subset H$, finalement $\mathrm{Ker}(\phi) = H$.

(b) Soit H un hyperplan de E, alors $E = H \oplus \mathbb{R}\, a$ avec $a \in E$ et $a \notin H$, et soient ϕ_1 et ϕ_2 deux formes linéaires telles que $\mathrm{Ker}(\phi_1) = \mathrm{Ker}(\phi_2) = H$.
Soit $x \in E$, alors $x = h + \lambda\, a$ où $h \in H$ et $\lambda \in \mathbb{R}$, donc

$$\begin{aligned}
\phi_1(x) &= \phi_1(h) + \lambda\, \phi_1(a) = \lambda\, \phi_1(a) \quad \text{car} \quad h \in H = \mathrm{Ker}(\phi_1) \\
\phi_2(x) &= \phi_2(h) + \lambda\, \phi_2(a) = \lambda\, \phi_2(a) \quad \text{car} \quad h \in H = \mathrm{Ker}(\phi_2)
\end{aligned}$$

or $a \notin H$, alors $\phi_1(a) \neq 0$ et $\phi_2(a) \neq 0$ car sinon ϕ_1 et ϕ_2 seraient nulles, donc

$$\frac{\phi_1(x)}{\phi_1(a)} = \lambda = \frac{\phi_2(x)}{\phi_2(a)}$$

donc $\phi_1(x) = \dfrac{\phi_1(a)}{\phi_2(a)}\,\phi_2(x)$ pour tout $x \in E$, on pose $\kappa = \dfrac{\phi_1(a)}{\phi_2(a)}$, alors

$$\phi_1(x) = \kappa\,\phi_2(x), \quad \forall x \in E$$

d'où ϕ_1 et ϕ_2 sont proportionnelles.
Finalement, si deux formes linéaires ϕ_1 et ϕ_2 définissent le même hyperplan H, alors ϕ_1 et ϕ_2 sont proportionnelles.

(c) Soient H_1 et H_2 deux hyperplans de E tels que $H_1 \neq H_2$.
Montrer que $H_1 + H_2 = E$: en effet, $H_1 \neq H_2$ implique il existe $a \in H_1$ et $a \notin H_2$.
Or H_2 est un hyperplan, alors $E = H_2 \oplus \mathbb{R}\,a$.
Soit $x \in E$, alors $x = h_2 + \lambda\,a$ où $h_2 \in H_2$ et $\lambda \in \mathbb{R}$;
comme $a \in H_1$ et H_1 est un sous-espace vectoriel de E, alors $\lambda\,a \in H_1$, donc $x \in H_2 + H_1$, d'où $E \subset H_2 + H_1$.
Comme H_1 et H_2 sont deux sous-espaces vectoriels de E, alors $H2 + H_1$ est un sous-espace vectoriel de E, soit $H_2 + H_1 \subset E$.
D'où $E = H_2 + H_1$.
On a $\dim(E) = \dim(H_1 + H_2)$, alors $n = \dim(H_1) + \dim(H_2) - \dim(H_1 \cap H_2)$,
or H_1 et H_2 sont deux hyperplans de E, alors $\dim(H_1) = \dim(H_2) = n - 1$,
donc $n = n - 1 + n - 1 - \dim(H_1 \cap H_2)$,
d'où $\dim(H_1 \cap H_2) = 2\,n - 2 - n = n - 2$.

2. Soit $\mathcal{T}$ une transvection de E,

(a) Montrons que l'hyperplan H associé à $\mathcal{T}$ est unique : en effet, supposons qu'il existe deux hyperplans distincts H et H' associés à la transvection $\mathcal{T}$ de E.
Soit $x \in E$, alors $x = x_1 + x_2$ où $x_1 \in H$ et $x_2 \in H'$,
donc $\mathcal{T}(x_1) = x_1$ et $\mathcal{T}(x_2) = x_2$, donc

$$\mathcal{T}(x) = \mathcal{T}(x_1) + \mathcal{T}(x_2) = x_1 + x_2 = x \quad \text{ceci pour tout} \quad x \in E$$

d'où $\mathcal{T} = \mathrm{id}_E$, ce qui est absurde puisque par hypothèse la transvection $\mathcal{T}$ est différente de id_E.
Finalement, l'hyperplan H associé à $\mathcal{T}$ est unique. H est appelé hyperplan de transvection de $\mathcal{T}$.

(b) Montrons que $\mathrm{Ker}(\mathcal{T} - \mathrm{id}_E) = H$: en effet, soit H l'hyperplan de E associé à la transvection $\mathcal{T}$, alors $E = H + \mathbb{R}\,a$ où $a \notin H$.
Soit $x \in E$ alors $x = h + \lambda\,a$ où $h \in H$ et $\lambda \in \mathbb{R}$;
comme $h \in H$ alors $\mathcal{T}(h) = h$, donc $\mathcal{T}(x) = \mathcal{T}(h) + \lambda\,\mathcal{T}(a) = h + \lambda\,\mathcal{T}(a)$.
Or $\mathcal{T} \neq \mathrm{id}_E$, alors $\mathcal{T}(a) \neq a$ car sinon on aurait $\mathcal{T}(x) = h + \lambda\,a = x$ pour tout $x \in E$, soit $\mathcal{T} = \mathrm{id}_E$ ce qui ne peut pas avoir lieu.
Si $x \in \mathrm{Ker}(\mathcal{T} - \mathrm{id}_E)$, alors $\mathcal{T}(x) = x$, donc il vient

$$h + \lambda\,\mathcal{T}(a) = h + \lambda\,a \quad \text{c'est à dire} \quad \lambda\,(\mathcal{T}(a) - a) = 0_E,$$

comme $\mathcal{T}(a) \neq a$ alors $\lambda = 0$, donc $x = h + 0\,a = h \in H$, d'où $\mathrm{Ker}(\mathcal{T} - \mathrm{id}_E) \subset H$.
Maintenant, soit $x \in H$, alors $\mathcal{T}(x) = x$, donc $\mathcal{T}(x) - x = (\mathcal{T} - \mathrm{id}_E)(x) = 0_E$, soit $x \in \mathrm{Ker}(\mathcal{T} - \mathrm{id}_E)$, d'où $H \subset \mathrm{Ker}(\mathcal{T} - \mathrm{id}_E)$.
Finalement, on obtient $H = \mathrm{Ker}(\mathcal{T} - \mathrm{id}_E)$.
On a $E = H + \mathbb{R}\,a$ alors $E = \mathrm{Ker}(\mathcal{T} - \mathrm{id}_E) + \mathbb{R}\,a$ avec $a \notin \mathrm{Ker}(\mathcal{T} - \mathrm{id}_E)$, or $a \notin \mathrm{Ker}(\mathcal{T} - \mathrm{id}_E)$ alors $\mathcal{T}(a) - a \neq 0_E$.
Soit $x \in E$, alors $x = h + \lambda\,a$ où $h \in \mathrm{Ker}(\mathcal{T} - \mathrm{id}_E)$ et $\lambda \in \mathbb{R}$, donc $\mathcal{T}(h) = h$, donc $\mathcal{T}(x) = h + \lambda\,\mathcal{T}(a)$, cela entraine que

$$\mathcal{T}(x) - x = h + \lambda\,\mathcal{T}(a) - h - \lambda\,a = \lambda\,(\mathcal{T}(a) - a)$$

on pose $b = \mathcal{T}(a) - a$, alors $b \neq 0_E$, donc les vecteurs $y = \mathcal{T}(x) - x$ et b sont colinéaires. Soit $\mathcal{D}$ la droite engendré par le vecteur directeur $b = \mathcal{T}(a) - a$, d'où

$$P_3 : \quad \forall x \in E, \quad \mathcal{T}(x) - x = \lambda\,(\mathcal{T}(a) - a) \in \mathcal{D}.$$

(c) Soit ϕ est une forme linéaire définissant H, cherchons un vecteur u de E tel que

$$P_4 : \quad \forall x \in E, \quad \mathcal{T}(x) = x + \phi(x).u.$$

En effet, on a $E = H + \mathbb{R}\,a$ où $a \notin H$ et soit $\mathcal{D} =< a >$ la droite engendrée par le vecteur a. D'après ce qui précède on a $H = \mathrm{Ker}(\mathcal{T} - \mathrm{id}_E)$ et $H = \mathrm{Ker}(\phi)$.
Soit $x \in E$, alors $x = h + \lambda\,a$ où $h \in H$ et $\lambda \in \mathbb{R}$, donc

$$\mathcal{T}(x) = \mathcal{T}(h) + \lambda\,\mathcal{T}(a) = h + \lambda\,\mathcal{T}(a) \quad \text{car} \quad \mathcal{T}(h) = h$$

ceci d'une part et d'autre part on a

$$\phi(x) = \phi(h) + \lambda\,\phi(a) = \lambda\,\phi(a) \quad \text{car} \quad \phi(h) = 0$$

on a $\phi(a) \neq 0$ car sinon $\phi(a) = 0$ implique $a \in \mathrm{Ker}(\phi) = H$ ce qui est contradictoire aux hypothèses.
Donc $\lambda = \dfrac{\phi(x)}{\phi(a)}$, en remplaçant λ par son expression il vient

$$\begin{aligned} \mathcal{T}(x) = h + \lambda\,\mathcal{T}(a) &= x - \lambda\,a + \lambda\,\mathcal{T}(a) \\ &= x + \lambda\,(\mathcal{T}(a) - a) \\ &= x + \phi(x)\,\frac{1}{\phi(a)}\,(\mathcal{T}(a) - a) \end{aligned}$$

on pose $u = \dfrac{1}{\phi(a)}\,(\mathcal{T}(a) - a)$, d'où $\mathcal{T}(x) = x + \phi(x)\,u$ qui est le résultat demandé.

(d) **Réciproquement**, montrons que si Φ est une forme linéaire non nulle de E et $u \in \mathrm{Ker}(\Phi)\backslash\{0_E\}$, alors $\mathcal{T} : E \to E$, $x \mapsto \mathcal{T}(x) = x + \Phi(x).u$ est une transvection de E :
en effet, soit Φ est une forme linéaire non nulle de E et soit $u \in \mathrm{Ker}(\Phi)\backslash\{0_E\}$ tel que $\mathcal{T}(x) = x + \Phi(x).u$.
– L'application $\mathcal{T}$ est bien définie car $\mathcal{T}(x) = x + \Phi(x).u \in E$ pour tout $x \in E$ et $u \in \mathrm{Ker}(\Phi)\backslash\{0_E\}$.

- L'application $\mathcal{T}$ est linéaire : en effet, soient x et y dans E et $\alpha \in \mathbb{R}$, alors

$$\begin{array}{rcl} \mathcal{T}(x+\alpha\, y) & = & x+\alpha\, y+\Phi(x+\alpha\, y)\,.u \\ & = & = x+\alpha\, y+\Phi(x)\,.u+\alpha\,\Phi(y)\,.u \\ & = & (x+\Phi(x)\,.u)+\alpha\,(y+\Phi(y)\,.u) \end{array}$$

  donc $\mathcal{T}(x+\alpha\, y) = \mathcal{T}(x)+\alpha\,\mathcal{T}(y)$, d'où $\mathcal{T}$ est linéaire.
- L'application $\mathcal{T}$ est un automorphisme de E : en effet, soit x dans E tel que $\mathcal{T}(x) = x+\Phi(x).u = 0_E$, alors $x = 0_E$:
  si $x \in H = \mathrm{Ker}(\Phi)$, alors $\Phi(x) = 0$ et donc $x+\Phi(x).u = 0_E$ entraine $x+0.u = 0_E$ soit $x = 0_E$,
  si $x \notin H = \mathrm{Ker}(\Phi)$, alors $\Phi(x+\Phi(x).u) = \Phi(0_E) = 0$,
  donc $\Phi(x)+\Phi(x).\Phi(u) = \Phi(x)\,(1+\Phi(u)) = 0$,
  d'où $\Phi(x) = 0$, c'est à dire $x = 0_E$. Finalement $\mathcal{T}$ est injective.
  Comme E est dimension finie, alors $\mathcal{T}$ est surjective, d'où $\mathcal{T}$ est bijective

L'application $\mathcal{T}$ est linéaire et bijective de E dans lui-même, d'où $\mathcal{T}$ est un automorphisme de E.
Déterminons l'hyperplan et la droite de $\mathcal{T}$: en effet, pour $x \in H = \mathrm{Ker}(\Phi)$, alors $\mathcal{T}(x) = x+0\,u = x$.
Soit $x \in E$, alors $\mathcal{T}(x) = x+\Phi(x).u$, donc $\mathcal{T}(x)-x = \Phi(x).u$,
on a $\Phi(\Phi(x).u) = \Phi(x).\Phi(u) = \Phi(x).0 = 0$, alors $\Phi(\mathcal{T}(x)-x) = 0$,
donc $\mathcal{T}(x)-x \in H = \mathrm{Ker}(\Phi)$, d'où $\mathcal{T}$ est une transvection de $H = \mathrm{Ker}(\Phi)$ et sa droite est $\mathcal{D} =< a >$ où $a \notin H$.

(e) Soit $H = \mathrm{Ker}(\Phi)$ un hyperplan de E. On note $\mathbb{T}(H)$ l'ensemble de toutes les transvections sur E d'hyperplan H et $G = \mathbb{T}(H) \cup \{\mathrm{id}_E\}$.

  i. Montrons que $(G,\circ)$ est un groupe ou plutôt sous-groupe de $(Aut(E),\circ)$: en effet, soient $\mathcal{T}_1$ et $\mathcal{T}_2$ deux transvections de E, d'abord la composée $\mathcal{T}_1\circ\mathcal{T}_2$ est un automorphisme car $\mathcal{T}_1$ et $\mathcal{T}_2$ sont tous deux automorphismes de E.
  Montrons que $\mathcal{T}_1\circ\mathcal{T}_2$ est une transvection sur E :
  - Soit $x \in H$, alors $\mathcal{T}_1(x) = x$ et $\mathcal{T}_2(x) = x$, donc

$$\mathcal{T}_1\circ\mathcal{T}_2(x) = \mathcal{T}_1(\mathcal{T}_2(x)) = \mathcal{T}_1(x) = x.$$

  - Soit $x \in E$ où $\mathcal{T}_1(x)-x \in H$ et $\mathcal{T}_2(x)-x \in H$, alors

$$\begin{array}{rcl} \mathcal{T}_1\circ\mathcal{T}_2(x)-x & = & \mathcal{T}_1(\mathcal{T}_2(x))-x \\ & = & \mathcal{T}_1(\mathcal{T}_2(x))-\mathcal{T}_1(x)+\mathcal{T}_1(x)-x \\ & = & \mathcal{T}_1(\mathcal{T}_2(x)-x)+\mathcal{T}_1(x)-x \end{array}$$

  comme $\mathcal{T}_2(x)-x \in H$, alors $\mathcal{T}_1(\mathcal{T}_2(x)-x) = \mathcal{T}_2(x)-x$, donc

$$\mathcal{T}_1\circ\mathcal{T}_2(x)-x = \underbrace{(\mathcal{T}_2(x)-x)}_{\in H}+\underbrace{(\mathcal{T}_1(x)-x)}_{\in H} \in H$$

  car la somme de deux éléments de H est un élément de H.
  d'où $\mathcal{T}_1\circ\mathcal{T}_2$ est une transvection sur E, c'est à dire $\circ$ laisse stable $\mathbb{T}(H)$.
  Soit $\mathcal{T} \in \mathbb{T}(H)$, on a $\mathcal{T}$ est un automorphisme alors $\mathcal{T}^{-1}$ est un automorphisme

de E. A-t-on $\mathcal{T}^{-1} \in \mathbb{T}(H)$?
Pour $x \in H$ alors on a $\mathcal{T}(x) = x$, donc $\mathcal{T}^{-1} \circ \mathcal{T}(x) = \mathcal{T}^{-1}(x)$, d'où $x = \mathcal{T}^{-1}(x)$.
Pour $x \in E$, on a $\mathcal{T}(x) - x \in H$, alors on applique $\mathcal{T}^{-1}$ il vient

$$\mathcal{T}^{-1}(\mathcal{T}(x) - x) = \mathcal{T}(x) - x$$

donc $\mathcal{T}^{-1} \circ \mathcal{T}(x) - \mathcal{T}^{-1}(x) = \mathcal{T}(x) - x$, donc $x - \mathcal{T}^{-1}(x) = \mathcal{T}(x) - x$,
d'où $\mathcal{T}^{-1}(x) - x = -(\mathcal{T}(x) - x) \in H$, ce qui prouve que $\mathcal{T}^{-1} \in \mathbb{T}(H)$ est une transvection.

ii. Soit $\mathscr{L} : (H, +) \to (G, \circ)$, $u \mapsto \mathcal{T}_u$ où $\mathcal{T}_u : E \to E$, $x \mapsto \mathcal{T}_u(x) = x + \Phi(x).u$.
Montrons que $\mathscr{L}$ est un isomorphisme de groupe : en effet, soient u et v dans H, on a $\mathscr{L}(u + v) = \mathcal{T}_{u+v}$. On a aussi

$$\begin{aligned} \mathcal{T}_u \circ \mathcal{T}_v(x) &= \mathcal{T}_u(\mathcal{T}_v(x)) = \mathcal{T}_u(x + \Phi(x).v) \\ &= x + \Phi(x).v + \Phi(x + \Phi(x).v).u \\ &= x + \Phi(x).v + (\Phi(x) + \Phi(x).\Phi(v)).u \\ &= x + \Phi(x).v + \Phi(x).u \end{aligned}$$

car $\Phi(v) = 0$, alors $\mathcal{T}_u \circ \mathcal{T}_v(x) = x + \Phi(x).(v + u)$, donc

$$\mathscr{L}(u) \circ \mathscr{L}(v) = \mathcal{T}_{u+v} = \mathscr{L}(u + v)$$

ce qui prouve que $\mathscr{L}$ est un homomorphisme de groupes.
Montrons que $\mathscr{L}$ est injectif : soeint u et v dans H tel que $\mathscr{L}(u) = \mathscr{L}(v)$, alors pour tout $x \in E$ on a $\mathcal{T}_u(x) = \mathcal{T}_v(x)$,
donc $x + \Phi(x).u = x + \Phi(x).v$, soit $\Phi(x)(u - v) = 0_E$,
or $\Phi(x) \neq 0$, alors $u - v = 0_E$, donc $u = v$, d'où $\mathscr{L}$ est injectif. L'application $\mathscr{L}$ est évidement surjective, d'où $\mathscr{L}$ est un isomorphisme de groupes.
Comme $(H, +)$ est un groupe abélien et que $(H, +)$ et $(G, \circ)$ sont isomorphes, alors $(G, \circ)$ est un groupe abélien.

3. (a) Soit $\mathcal{U}$ une involution de E, c'est à dire $\mathcal{U} \in \mathscr{L}(E)$ et $\mathcal{U}^2 = \mathrm{id}_E$.
On pose $E_1(\mathcal{U}) = \mathrm{Ker}(\mathcal{U} - \mathrm{id}_E)$ et $E_{-1}(\mathcal{U}) = \mathrm{Ker}(\mathcal{U} + \mathrm{id}_E)$.

i. Montrons que $E = E_1(\mathcal{U}) \oplus E_{-1}(\mathcal{U})$: en effet, soit $x \in E$, alors d'une part on a

$$x = \frac{1}{2}(\mathcal{U}(x) + x) + \frac{1}{2}(x - \mathcal{U}(x)) = x_1 + x_2$$

où $x_1 = \frac{1}{2}(\mathcal{U}(x) + x)$ et $x_2 = \frac{1}{2}(x - \mathcal{U}(x))$, et d'autre part

$$\mathcal{U}(\mathcal{U}(x) + x) = \mathcal{U}^2(x) + \mathcal{U}(x) = x + \mathcal{U}(x),$$

donc $\mathcal{U}(x + \mathcal{U}(x)) - (x + \mathcal{U}(x)) = 0_E$, donc $x + \mathcal{U}(x) \in \mathrm{Ker}(\mathcal{U} - \mathrm{id}_E) = E_1(\mathcal{U})$,
d'où $x_1 = \frac{1}{2}(\mathcal{U}(x) + x) \in E_1(\mathcal{U})$,
on a aussi $\mathcal{U}(x - \mathcal{U}(x)) = \mathcal{U}(x) - \mathcal{U}^2(x) = \mathcal{U}(x) - x$,
alors $\mathcal{U}(x - \mathcal{U}(x)) + (x - \mathcal{U}(x)) = 0_E$, donc $x - \mathcal{U}(x) \in \mathrm{Ker}(\mathcal{U} + \mathrm{id}_E) = E_{-1}(\mathcal{U})$,
d'où $x_2 = \frac{1}{2}(x - \mathcal{U}(x)) \in E_{-1}(\mathcal{U})$,
d'où $x = x_1 + x_2$ où $x_1 \in E_1(\mathcal{U})$ et $x_2 \in E_{-1}(\mathcal{U})$, d'où $E = E_1(\mathcal{U}) + E_{-1}(\mathcal{U})$.
Soit $x \in E_1(\mathcal{U}) \cap E_{-1}(\mathcal{U})$, alors $x \in E_{-1}(\mathcal{U})$ et $x \in E_1(\mathcal{U})$, donc il vient

$$x - \mathcal{U}(x) = 0_E \quad \text{et} \quad x + \mathcal{U}(x) = 0_E$$

en faisant la somme des deux équations, il vient $x - \mathcal{U}(x) + x + \mathcal{U}(x) = 0_E$, donc $2\,x = 0_E$, d'où $x \in \{0_E\}$, soit $E_1(\mathcal{U}) \cap E_{-1}(\mathcal{U}) \subset \{0_E\}$.
Comme $E_1(\mathcal{U})$ et $E_{-1}(\mathcal{U})$ sont deux sous-espaces vectoriels de E, alors $0_E \in E_1(\mathcal{U})$ et $0_E \in E_{-1}(\mathcal{U})$, donc $\{0_E\} \subset E_1(\mathcal{U}) \cap E_{-1}(\mathcal{U})$.
D'où $E_1(\mathcal{U}) \cap E_{-1}(\mathcal{U}) = \{0_E\}$. Finalement, on obtient $E = E_1(\mathcal{U}) \oplus E_{-1}(\mathcal{U})$.

ii. Supposons que $\dim(E_1(\mathcal{U})) = 1$.

A. Soit $a \in E$ tel que $E_1(\mathcal{U}) = \mathbb{R}.a$. Montrons qu'il existe $\varphi \in \mathscr{L}(E, \mathbb{R})$ une forme linéaire de E telle que $\mathrm{Ker}(\varphi) = E_{-1}(\mathcal{U})$ et $\varphi(a) = 2$:
en effet, comme $\dim(E_1(\mathcal{U})) = 1$ alors $E_1(\mathcal{U})$ est une droite vectorielle, donc il existe $a \in E$ et $a \neq 0_E$ tel que $E_1(\mathcal{U}) = \mathbb{R}\,a$,
d'où $E = \mathbb{R}\,a \oplus E_{-1}(\mathcal{U})$, soit $\dim(E_{-1}(\mathcal{U})) = n - 1$; ce qui prouve que $E_{-1}(\mathcal{U})$ est un hyperplan de E.
Pour $x \in E$, on a $x = y + \lambda\,a$ où $y \in E_{-1}(\mathcal{U})$. On pose $\varphi(x) = 2\lambda$, on a alors $a = 0 + 1\,a$, donc $\varphi(a) = 2 * 1 = 2$ et $\mathrm{Ker}(\varphi) = E_{-1}(\mathcal{U})$.

B. D'après ii-A), pour $x = x_1 + \lambda\,a \in E$ où $x_1 \in E_{-1}(\mathcal{U})$ et $\lambda \in \mathbb{R}$, on a $\varphi(x) = 2\,\lambda$.

$$\begin{aligned} x_1 \in E_{-1}(\mathcal{U}) \quad &\Leftrightarrow \quad \mathcal{U}(x_1) + x_1 = 0_E \\ &\Leftrightarrow \quad \mathcal{U}(x_1) = -x_1 \end{aligned}$$

et

$$\begin{aligned} a \in E_1(\mathcal{U}) = \mathbb{R}\,a \quad &\Leftrightarrow \quad \mathcal{U}(a) - a = 0_E \\ &\Leftrightarrow \quad \mathcal{U}(a) = a \end{aligned}$$

donc $\mathcal{U}(x) = \mathcal{U}(x_1) + \mathcal{U}(\lambda\,a) = -x_1 + \lambda\,\mathcal{U}(a) = -x_1 + \lambda\,a$;
or $-x_1 = -x + \lambda\,a$, alors $\mathcal{U}(x) = -x + \lambda\,a + \lambda\,a = -x + 2\,\lambda\,a$,
donc $\mathcal{U}(x) = -x + \varphi(x)\,a$,
d'où on déduit qu'il existe $a \in E$ et $\varphi \in \mathscr{L}(E, \mathbb{R})$ tels que $\forall x \in E$, $\mathcal{U}(x) = -x + \varphi(x)\,a$.

C. Soit $\mathcal{V}$ une autre involution de E telle que $E_1(\mathcal{U}) = E_1(\mathcal{V})$.
*Montrons qu'il existe $\psi \in \mathscr{L}(E, \mathbb{R})$ telle que $\forall x \in E$, $\mathcal{V}(x) = -x + \psi(x).a$:
en effet, il existe $a \in E_{-1}(\mathcal{U})$ et $\varphi \in \mathscr{L}(E, \mathbb{R})$ tels que $\forall x \in E$, $\mathcal{U}(x) = -x + \varphi(x)\,a$ et $\varphi(a) = 2$
d'après ii-A), il existe $b \in E_1(\mathcal{V})$ et $\psi_1 \in \mathscr{L}(E, \mathbb{R})$ tels que $\forall x \in E$, $\mathcal{V}(x) = -x + \psi_1(x)\,b$,
or $b \in E_1(\mathcal{V}) = E_1(\mathcal{U}) = \mathbb{R}\,a$, alors il existe $\alpha \in \mathbb{R}$ tel que $b = \alpha\,a$, donc $\mathcal{V}(x) = -x + \alpha\,\psi_1(x)\,a$. On pose $\psi(x) = \alpha\,\psi_1(x)$,
d'où $\mathcal{V}(x) = -x + \psi(x)\,a$
*On a $\mathcal{U}(x) = -x + \varphi(x)\,a$ et $\mathcal{V}(x) = -x + \psi(x)\,a$, alors

$$\begin{aligned} \mathcal{U} \circ \mathcal{V}(x) &= \mathcal{U}(\mathcal{V}(x)) = \mathcal{U}(-x + \psi(x)\,a) \\ &= -\mathcal{U}(x) + \psi(x)\,\mathcal{U}(a) = -\mathcal{U}(x) + \psi(x)\,a \\ &= x - \varphi(x)\,a + \psi(x)\,a \\ &= x + (\psi(x) - \varphi(x))\,a \end{aligned}$$

donc $\mathcal{U} \circ \mathcal{V}(x) - x = (\psi(x) - \varphi(x))\, a$. On pose $g(x) = \psi(x) - \varphi(x)$, alors g est une forme linéaire non nulle sur E, donc $H = \mathrm{Ker}(g)$ est un hyperplan de E.

– Soit $x \in H$, alors $g(x) = 0$, donc $\psi(x) - \varphi(x) = 0$, d'où $\mathcal{U} \circ \mathcal{V}(x) = x \in H$.

– Soit $x \in E$, alors $\mathcal{U} \circ \mathcal{V}(x) - x = (\psi(x) - \varphi(x))\, a$ et on a

$$\begin{aligned} g((\psi(x) - \varphi(x))\, a) &= (\psi(x) - \varphi(x))\, g(a) \\ &= (\psi(x) - \varphi(x))\, (\psi(a) - \varphi(a)) \\ &= (\psi(x) - \varphi(x))\, 0 = 0 \end{aligned}$$

donc $\mathcal{U} \circ \mathcal{V}(x) - x = (\psi(x) - \varphi(x))\, a \in \mathrm{Ker}(g) = H$

d'où $\mathcal{U} \circ \mathcal{V}$ est une transvection de E.

(b) i. Soit une transvection $\mathcal{T}$ et $\sigma \in \mathrm{Aut}(E)$ un automorphisme de E.
Montrons que $\sigma \circ \mathcal{T} \circ \sigma^{-1}$ est une transvection : en effet, on pose $\tilde{\mathcal{T}} = \sigma \circ \mathcal{T} \circ \sigma^{-1}$, alors $\tilde{\mathcal{T}}$ est une application linéaire bijective de E dans lui-même.

– On a $\tilde{\mathcal{T}}(x) = x$ est équivalent à $\sigma \circ \mathcal{T} \circ \sigma^{-1}(x) = x$,

$$\begin{aligned} \sigma \circ \mathcal{T} \circ \sigma^{-1}(x) = x \quad &\Leftrightarrow \quad \mathcal{T} \circ \sigma^{-1}(x) = \sigma^{-1}(x) \quad \text{car } \sigma \text{ est bijectif} \\ &\Leftrightarrow \quad \mathcal{T} \circ \sigma^{-1}(x) - \sigma^{-1}(x) = 0_E \\ &\Leftrightarrow \quad \sigma^{-1}(x) \in \mathrm{Ker}(\mathcal{T} - \mathrm{id}_E) \\ &\Leftrightarrow \quad x \in \sigma(\mathrm{Ker}(\mathcal{T} - \mathrm{id}_E)) \end{aligned}$$

on pose $H = \sigma(\mathrm{Ker}(\mathcal{T} - \mathrm{id}_E))$. On a $\mathcal{T}$ est une transvection de E, alors $\mathrm{Ker}(\mathcal{T} - \mathrm{id}_E)$ est un hyperplan de E ; et comme σ est un automorphisme de E, alors $H = \sigma(\mathrm{Ker}(\mathcal{T} - \mathrm{id}_E))$ est un hyperplan de E.

– Soit $x \in E$, on a $\sigma \circ \mathcal{T} \circ \sigma^{-1}(x) - x = \sigma\left(\mathcal{T} \circ \sigma^{-1}(x) - \sigma^{-1}(x)\right)$
or $\mathcal{T} \circ \sigma^{-1}(x) - \sigma^{-1}(x) \in \mathrm{Ker}(\mathcal{T} - \mathrm{id}_E)$, alors

$$\sigma\Big(\mathcal{T} \circ \sigma^{-1}(x) - \sigma^{-1}(x)\Big) \in H = \sigma(\mathrm{Ker}(\mathcal{T} - \mathrm{id}_E))$$

d'où $\sigma \circ \mathcal{T} \circ \sigma^{-1}(x) - x = \tilde{\mathcal{T}}(x) - x \in H$.

ce qui prouve que $\tilde{\mathcal{T}} = \sigma \circ \mathcal{T} \circ \sigma^{-1}$ est une transvection de E d'hyperplan $H = \sigma(\mathrm{Ker}(\mathcal{T} - \mathrm{id}_E))$.

Soit $\mathcal{D}$ la droite de $\mathcal{T}$, alors il existe $u \in E$ tel que $u \neq 0_E$ et $\mathcal{D} = \mathbb{R}\, u$,
donc pour tout $x \in E$ on a $\mathcal{T}(x) - x = \varphi(x)\, u$, donc

$$\begin{aligned} \sigma \circ \mathcal{T} \circ \sigma^{-1}(x) - x &= \sigma\Big(\mathcal{T} \circ \sigma^{-1}(x) - \sigma^{-1}(x)\Big) \\ &= \sigma\Big(\varphi(\sigma^{-1}(x))\, u\Big) \\ &\quad \text{car} \quad \mathcal{T}(\sigma^{-1}(x)) - \sigma^{-1}(x) = \varphi(\sigma^{-1}(x))\, u \\ &= \varphi(\sigma^{-1}(x))\, \sigma(u) \end{aligned}$$

donc $\sigma \circ \mathcal{T} \circ \sigma^{-1}(x) - x = \varphi \circ \sigma^{-1}(x)\, \sigma(u)$,
d'où la droite $\tilde{\mathcal{D}}$ de $\tilde{\mathcal{T}} = \sigma \circ \mathcal{T} \circ \sigma^{-1}$ est engendrée par le vecteur $\sigma(u)$,
finalement $\tilde{\mathcal{D}} = \sigma(\mathcal{D})$.

ii. Prouvons que si $\mathcal{T}_1$ et $\mathcal{T}_2$ sont deux transvections, alors il existe $\sigma \in \mathrm{Aut}(E)$ tel que $\mathcal{T}_2 = \sigma \circ \mathcal{T}_1 \circ \sigma^{-1}$: en effet, soient $\mathcal{T}_1$ et $\mathcal{T}_2$ deux transvections de E. On considère Φ l'application de $\mathrm{Aut}(E)$ définie pour tout $\sigma \in \mathrm{Aut}(E)$ par $\Phi(\sigma) = \sigma \circ \mathcal{T} \circ \sigma^{-1}$ où $\mathcal{T}$ est une tranvection de E, montrons que Φ est injective. Soient σ_1 et σ_2 dans $\mathrm{Aut}(E)$ tels que $\Phi(\sigma_1) = \Phi(\sigma_2)$, alors

$$\sigma_1 \circ \mathcal{T} \circ \sigma_1^{-1} = \sigma_2 \circ \mathcal{T} \circ \sigma_2^{-1}$$

donc les transvections $T_1 = \sigma_1 \circ \mathcal{T} \circ \sigma_1^{-1}$ et $T_2 = \sigma_2 \circ \mathcal{T} \circ \sigma_2^{-1}$ ont le même hyperplan H et la même droite $\mathcal{D}$, c'est à dire que $\sigma_1(H) = \sigma_2(H)$ et $\sigma_1(u) = \sigma_2(u)$ où $E = H \oplus \mathbb{R}\,u$ et $u \notin H$ avec $u \neq 0_E$, donc $\sigma_1 = \sigma_2$,
d'où Φ est injectif.
D'après 3.(b)-i, pour toute tranvection $\mathcal{T}$ de E et tout automorphisme σ, on a $\sigma \circ \mathcal{T} \circ \sigma^{-1}$ est une transvection de E, d'où $\sigma^{-1}\Phi(\sigma)\sigma = \mathcal{T}$ est une tranvection, ce qui prouve que Φ est sujectif.
D'où Φ est bijectif, ce qui prouve que pour toutes tranvections $\mathcal{T}_1$ et $\mathcal{T}_2$, il existe $\sigma \in \mathrm{Aut}(E)$ tel que $\mathcal{T}_2 = \sigma \circ \mathcal{T}_1 \circ \sigma^{-1}$ où bien $\mathcal{T}_2 \circ \sigma = \sigma \circ \mathcal{T}_1$.

Problème 2

On considère l'espace vectoriel $\mathbb{C}[X]$ ainsi le sous-ensemble $\mathbb{C}_n[X]$ des polynômes de degré inférieur ou égal à n avec $n \in \mathbb{N}^*$.

1. Montrer que $\mathbb{C}_n[X]$ est un sous-espace vectoriel de $\mathbb{C}[X]$. Que peut-on en déduire ?
2. Montrer que l'application $\mathcal{D} : \mathbb{C}[X] \to \mathbb{C}[X]$ définie par :

$$\forall P \in \mathbb{C}[X], \quad \mathcal{D}(P) = P' \ : \text{ la dérivée de } P$$

est linéaire.

3. Soit $B_n = \{U_p \,:\, p \in \{0, 1, \ldots, n\}\}$ la base de $\mathbb{C}_n[X]$ formée par les polynômes

$$U_p = X^p(1-X)^{n-p} \quad \text{où} \quad p \in \{0, 1, \ldots, n\}.$$

(a) Rappeler la formule du binôme $(a+b)^p$, puis montrer que $1 = \sum_{k=0}^{p} \mathrm{C}_p^k X^{p-k}(1-X)^k$.

(b) Montrer que $\forall 0 \leq p \leq n$, on a $X^{n-p} = \sum_{k=0}^{p} \mathrm{C}_p^k U_{n-k}$, où $\mathrm{C}_p^k = \frac{p!}{k!(p-k)!}$.

(c) Soit $B = \{1, X, X^2, \ldots, X^n\}$ la base canonique de $\mathbb{C}_n[X]$, déterminer la matrice de passage T de B à B_n. Exprimer la matrice T lorsque $n = 2$, puis calculer la matrice inverse T^{-1}.

4. On considère l'application β qui à tout élément $Q \in \mathbb{C}[X]$ associe le polynôme

$$\beta(Q) = \sum_{p=0}^{n} Q\left(\frac{p}{n}\right) \mathrm{C}_n^p U_p$$

(a) Montrer que β est une application linéaire de $\mathbb{C}[X]$ dans $\mathbb{C}_n[X]$.

(b) Montrer que $\beta(1) = 1$.

5. (a) Montrer que $\forall\, 0 \leq p \leq n$, on a

$$\frac{X(1-X)}{n}\mathcal{D}(U_p) = \frac{p}{n}U_p - XU_p.$$

Traiter les cas $p = 0$ et $p = n$ à part.

(b) Montrer, en utilisant la linéarité de l'application $\mathcal{D}$, que :

$$\forall k \in \mathbb{N}^* \; : \quad \mathcal{D}(\beta(X^k)) = \sum_{k=0}^{p} \left(\frac{p}{n}\right)^k \mathrm{C}_n^p \mathcal{D}(U_p)$$

(c) Déduire, en utilisant 4-a), que : $\forall k \in \mathbb{N}$ on a

$$\frac{X(1-X)}{n}\mathcal{D}(\beta(X^k)) = \beta(X^{k+1}) - X\beta(X^k).$$

6. (a) Soit $Q = \sum_{k=0}^{m} \lambda_k X^k$, montrer que $\beta(XQ) = \sum_{k=0}^{m} \lambda_k \beta(X^{k+1})$.

(b) Déduire, grâce à la linéarité de $\mathcal{D}$ et β, et d'après ce qui précède que :

$$\forall Q \in \mathbb{C}[X] \quad \beta(XQ) = \frac{X(1-X)}{n}\, \mathcal{D}(\beta(Q)) + X\beta(Q)$$

(c) Calculer $\beta(X)$ et $\beta(X^2)$.

Solution : Considère l'espace vectoriel $\mathbb{C}[X]$ et le sous-ensemble $\mathbb{C}_n[X]$ des polynômes de degré inférieur ou égal à n avec $n \in \mathbb{N}^*$.

1. Montrons que $\mathbb{C}_n[X]$ est un sous-espace vectoriel de $\mathbb{C}[X]$: D'abord $\mathbb{C}_n[X] \neq \emptyset$ car le polynôme nul est un élément dans $\mathbb{C}_n[X]$. Soient P et Q deux éléments dans $\mathbb{C}_n[X]$ et λ et γ deux scalaires complexes, on a

$$P = \sum_{i=0}^{n} a_i\, X^i \quad \text{et} \quad Q = \sum_{j=0}^{n} b_j\, X^j$$

alors

$$\lambda\, P + \gamma\, Q = \sum_{i=0}^{n} (\lambda\, a_i + \gamma\, b_i)\, X^i = \sum_{i=0}^{n} c_i\, X^i \quad \text{où} \quad c_i = \lambda\, p_i + \gamma\, q_i$$

donc $\lambda\, P + \gamma\, Q \in \mathbb{C}_n[X]$, d'où $\mathbb{C}_n[X]$ est un $\mathbb{C}$-espace vectoriel de $\mathbb{C}[X]$.
On en déduit que $\dim_{\mathbb{C}}(\mathbb{C}_n[X]) = n + 1$.

2. Montrons que l'application $\mathcal{D} : \mathbb{C}[X] \to \mathbb{C}[X]$ définie par :

$$\forall P \in \mathbb{C}[X], \quad \mathcal{D}(P) = P' \qquad \text{est linéaire}$$

Soient P et Q deux éléments dans $\mathbb{C}_n[X]$ et λ et γ deux scalaires complexes, on a

$$P = \sum_{i=0}^{n} a_i\, X^i \quad \text{et} \quad Q = \sum_{j=0}^{n} b_j\, X^j$$

alors

$$\begin{aligned}\mathcal{D}(\lambda\, P+\gamma\, Q) &= (P+Q)' = \left(\sum_{i=0}^{n}(\lambda\, a_i+\gamma\, b_i)\, X^i\right)' = \sum_{i=1}^{n} i\,(\lambda\, a_i+\gamma\, b_i)\, X^{i-1}\\ &= \lambda\sum_{i=1}^{n} i\, a_i\, X^{i-1}+\gamma\sum_{i=1}^{n} i\, b_i\, X^{i-1} = \lambda\left(\sum_{i=0}^{n} a_i\, X^i\right)'+\gamma\left(\sum_{i=0}^{n} b_i\, X^i\right)'\end{aligned}$$

donc $\mathcal{D}(\lambda\, P+\gamma\, Q) = \lambda\, P'+\gamma\, Q' = \lambda\,\mathcal{D}(P)+\gamma\,\mathcal{D}(Q)$, d'où la linéarité de $\mathcal{D}$.

3. Soit $B_n = \{U_p \,:\, p\in\{0,1,\ldots,n\}\}$ la base de $\mathbb{C}_n[X]$ formée par les polynômes

$$U_p = X^p(1-X)^{n-p} \quad \text{où} \quad p\in\{0,1,\ldots,n\}.$$

(a) La formule du binôme $(a+b)^p$: soient a et b deux réels, alors $a\,b = b\,a$, donc il vient

$$(a+b)^p = \sum_{k=0}^{p} \mathrm{C}_p^k\, a^{p-k}\, b^k.$$

Pour $a = 1-X$ et $b = X$, alors $(a+b)^p = (1-X+X)^p = 1^p = 1$, donc

$$1 = \sum_{k=0}^{p} \mathrm{C}_p^k\, X^{p-k}(1-X)^k.$$

(b) Montrons que $\forall 0\le p\le n$, on a $X^{n-p} = \sum_{k=0}^{p}\mathrm{C}_p^k U_{n-k}$, où $\mathrm{C}_p^k = \frac{p!}{k!(p-k)!}$.

Pour tout $0\le p\le n$, on a

$$\begin{aligned}\sum_{k=0}^{p}\mathrm{C}_p^k U_{n-k} &= \sum_{k=0}^{p}\mathrm{C}_p^k X^{n-k}(1-X)^k = \sum_{k=0}^{p}\mathrm{C}_p^k X^{n-p}\, X^{p-k}(1-X)^k\\ &= X^{n-p}\sum_{k=0}^{p}\mathrm{C}_p^k X^{p-k}(1-X)^k\\ &= X^{n-p}\,(X+1-X)^p\end{aligned}$$

d'où $\sum_{k=0}^{p}\mathrm{C}_p^k U_{n-k} = X^{n-p}$.

(c) Soit $B = \{1, X, X^2, \ldots, X^n\}$ la base canonique de $\mathbb{C}_n[X]$,

– La matrice de passage T de B à B_n : on a $\sum_{k=0}^{p}\mathrm{C}_p^k U_{n-k} = X^{n-p}$, alors

pour $p = n$, on a $1 = \sum_{k=0}^{n}\mathrm{C}_n^k U_{n-k}$,

on pose $h = n-k$, alors $1 = \sum_{h=0}^{n}\mathrm{C}_n^{n-h} U_h$ et comme $\mathrm{C}_n^{n-h} = \mathrm{C}_n^h$ alors

$$1 = \sum_{h=0}^{n}\mathrm{C}_n^h U_h = \mathrm{C}_n^0 U_0+\mathrm{C}_n^1 U_1+\ldots+\mathrm{C}_n^n U_n.$$

De même, $\sum_{k=0}^{p} \mathrm{C}_p^k U_{n-k} = X^{n-p}$, on pose $h = n - p$, alors $p = n - h$, donc

$$X^h = \sum_{k=0}^{n-h} \mathrm{C}_{n-h}^k U_{n-k}$$

or on a $0 \leq k \leq n - h$, alors $h \leq n - k \leq n$, on pose $j = n - k$, donc

$$X^h = \sum_{j=h}^{n} \mathrm{C}_{n-h}^{n-j} U_j$$

pour $h = 1$, on a $X = \mathrm{C}_{n-1}^0 U_1 + \mathrm{C}_{n-1}^1 U_2 + \mathrm{C}_{n-1}^2 U_3 + \ldots + \mathrm{C}_{n-1}^{n-1} U_n$,
pour $h = 2$, on a $X^2 = \mathrm{C}_{n-2}^0 U_2 + \mathrm{C}_{n-2}^1 U_3 + \mathrm{C}_{n-2}^2 U_4 + \ldots + \mathrm{C}_{n-2}^{n-2} U_n$,
pour $h = n - 1$, on a $X^{n-1} = \mathrm{C}_1^1 U_{n-1} + \mathrm{C}_1^0 U_n$,
pour $h = n$, on a $X^n = \mathrm{C}_0^0 U_n$,
d'où la matrice de passage T de B à B_n est

$$T = \begin{bmatrix} \mathrm{C}_n^0 & 0 & 0 & \ldots & 0 \\ \mathrm{C}_n^1 & \mathrm{C}_{n-1}^0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \mathrm{C}_n^{n-1} & \mathrm{C}_{n-1}^{n-2} & \ldots & \mathrm{C}_1^0 & 0 \\ \mathrm{C}_n^n & \mathrm{C}_{n-1}^{n-1} & \ldots & \mathrm{C}_1^1 & \mathrm{C}_0^0 \end{bmatrix}$$

– La matrice T pour $n = 2$: on a

$$T = \begin{bmatrix} \mathrm{C}_2^0 & 0 & 0 \\ \mathrm{C}_2^1 & \mathrm{C}_1^0 & 0 \\ \mathrm{C}_2^1 & \mathrm{C}_1^0 & \mathrm{C}_0^0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

– La matrice inverse T^{-1} de T est

$$T^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 1 & -1 & 1 \end{bmatrix}.$$

4. Considère l'application β qui à tout élément $Q \in \mathbb{C}[X]$ associe le polynôme

$$\beta(Q) = \sum_{p=0}^{n} Q\left(\frac{p}{n}\right) \mathrm{C}_n^p U_p$$

   (a) Montrons que β est une application linéaire de $\mathbb{C}[X]$ dans $\mathbb{C}_n[X]$: soit Q dans $\mathbb{C}[X]$ alors pour tout $0 \leq p \leq n$ on a $Q\left(\frac{p}{n}\right) \mathrm{C}_n^p \in \mathbb{C}$ et que

$$\mathrm{d}^o U_p = \mathrm{d}^o(X^p(1-X)^{n-p}) = n \quad \text{donc} \quad \mathrm{d}^o \beta(Q) \leq n$$

   d'où pour tout Q dans $\mathbb{C}[X]$ on a $\mathrm{d}^o \beta(Q) \leq n$, soit $\beta(Q) \in \mathbb{C}_n[X]$ c'est à dire que β est bien défini de $\mathbb{C}[X]$ dans $\mathbb{C}_n[X]$.
   Soient P et Q deux éléments dans $\mathbb{C}[X]$ et λ un scalaire complexe, alors

$$\beta(\lambda Q) = \sum_{p=0}^{n} (\lambda Q)\left(\frac{p}{n}\right) \mathrm{C}_n^p U_p = \lambda \sum_{p=0}^{n} Q\left(\frac{p}{n}\right) \mathrm{C}_n^p U_p = \lambda \beta(Q)$$

$$\beta(P+Q)=\sum_{p=0}^{n}(P+Q)\left(\frac{p}{n}\right)\mathrm{C}_n^pU_p=\sum_{p=0}^{n}P\left(\frac{p}{n}\right)\mathrm{C}_n^pU_p+\sum_{p=0}^{n}Q\left(\frac{p}{n}\right)\mathrm{C}_n^pU_p$$

donc $\beta(P+Q)=\beta(P)+\beta(Q)$, d'où la linéarité de β.

(b) Montrons que $\beta(1)=1$: on a $\beta(Q)=\sum_{p=0}^{n}Q\left(\frac{p}{n}\right)\mathrm{C}_n^pU_p$, alors pour $Q=1$ il ;vient

$$\beta(1)=\sum_{p=0}^{n}1\,\mathrm{C}_n^pU_p=\sum_{p=0}^{n}\mathrm{C}_n^pX^p(1-X)^{n-p}=(X+1-X)^n=1.$$

5. (a) Montrons que $\forall\, 0\leq p\leq n$, on a

$$\frac{X(1-X)}{n}\mathcal{D}(U_p)=\frac{p}{n}U_p-XU_p.$$

Pour $0\leq p\leq n$, on a

$$\begin{aligned}\frac{X(1-X)}{n}\mathcal{D}(U_p) &= \frac{X(1-X)}{n}\left(X^p(1-X)^{n-p}\right)'\\ &= \frac{X(1-X)}{n}\Big(p\,X^{p-1}\,(1-X)^{n-p}-(n-p)\,X^p\,(1-X)^{n-p-1}\Big)\\ &= \frac{X(1-X)}{n}\,X^{p-1}\;(1-X)^{n-p-1}\,(p\,(1-X)-(n-p)\,X)\\ &= \frac{1}{n}\,X^p\;(1-X)^{n-p}\,(p-n\,X)\end{aligned}$$

donc $\frac{X(1-X)}{n}\mathcal{D}(U_p)=\frac{p}{n}\,X^p\;(1-X)^{n-p}-X\,X^p\;(1-X)^{n-p}=\left(\frac{p}{n}-X\right)\,U_p$.
Pour $p=0$, on a $U_0=X^0(1-X)^{n-0}=(1-X)^n$, alors $\mathcal{D}(U_0)=-n\,(1-X)^{n-1}$, donc

$$\frac{X(1-X)}{n}\mathcal{D}(U_0)=-X\,(1-X)^n=-X\,U_0$$

et pour $p=n$ on a $U_n=X^n(1-X)^{n-n}=X^n$, alors $\mathcal{D}(U_n)=n\,X^{n-1}$, donc

$$\frac{X(1-X)}{n}\mathcal{D}(U_n)=(1-X)\,X^n=(1-X)\,U_n.$$

(b) Montrons, en utilisant la linéarité de l'application $\mathcal{D}$, que :

$$\forall k\in\mathbb{N}^*\ :\quad \mathcal{D}(\beta(X^k))=\sum_{k=0}^{p}\left(\frac{p}{n}\right)^k\mathrm{C}_n^p\mathcal{D}(U_p).$$

Soit $k\in\mathbb{N}^*$, pour $Q=X^k$ on a $\beta(X^k)=\sum_{p=0}^{n}\left(\frac{p}{n}\right)^k\mathrm{C}_n^pU_p$, alors

$$\mathcal{D}(\beta(X^k))=\mathcal{D}\left(\sum_{k=0}^{p}\left(\frac{p}{n}\right)^k\mathrm{C}_n^pU_p\right)=\left(\sum_{k=0}^{p}\left(\frac{p}{n}\right)^k\mathrm{C}_n^pU_p\right)'$$

comme $\mathcal{D}$ est linéaire alors

$$\mathcal{D}(\beta(X^k)) = \sum_{k=0}^{p} \left(\frac{p}{n}\right)^k \mathrm{C}_n^p \,(U_p)'$$

d'où le résultat $\mathcal{D}(\beta(X^k)) = \displaystyle\sum_{k=0}^{p} \left(\frac{p}{n}\right)^k \mathrm{C}_n^p \mathcal{D}(U_p)$.

(c) D'après la question 5-a), on a $\dfrac{X(1-X)}{n}\mathcal{D}(U_p) = \dfrac{p}{n}U_p - XU_p$, alors en replaçant U_p par $\beta(X^k)$ il vient

$$\begin{aligned}\frac{X(1-X)}{n}\mathcal{D}(\beta(X^k)) &= \frac{p}{n}\beta(X^k) - X\beta(X^k)\\ &= \frac{p}{n}\sum_{p=0}^{n}\left(\frac{p}{n}\right)^k \mathrm{C}_n^p U_p - X\beta(X^k)\\ &= \sum_{p=0}^{n}\left(\frac{p}{n}\right)^{k+1} \mathrm{C}_n^p U_p - X\beta(X^k)\end{aligned}$$

d'où on déduit que $\dfrac{X(1-X)}{n}\mathcal{D}(\beta(X^k)) = \beta(X^{k+1}) - X\beta(X^k)$.

6. (a) Soit $Q = \displaystyle\sum_{k=0}^{m} \lambda_k X^k$, montrons que $\beta(XQ) = \displaystyle\sum_{k=0}^{m} \lambda_k \beta(X^{k+1})$. En effet, on a

$$X\,Q = X\,\sum_{k=0}^{m}\lambda_k X^k = \sum_{k=0}^{m}\lambda_k X^{k+1}$$

alors

$$\beta(X\,Q) = \beta\left(\sum_{k=0}^{m}\lambda_k X^{k+1}\right) = \sum_{p=0}^{n}\sum_{k=0}^{m}\lambda_k\left(\frac{p}{n}\right)^{k+1}\mathrm{C}_n^p U_p$$

donc, en faisant intervertir les signes somme, il vient

$$\beta(X\,Q) = \sum_{k=0}^{m}\lambda_k\left(\sum_{p=0}^{n}\left(\frac{p}{n}\right)^{k+1}\mathrm{C}_n^p U_p\right)$$

d'où $\beta(X\,Q) = \displaystyle\sum_{k=0}^{m}\lambda_k\beta(X^{k+1})$.

(b) D'après la question 5-(c) on a $\dfrac{X(1-X)}{n}\mathcal{D}(\beta(X^k)) = \beta(X^{k+1}) - X\beta(X^k)$, alors

$$\lambda_k\,\frac{X(1-X)}{n}\mathcal{D}(\beta(X^k)) = \lambda_k\,\beta(X^{k+1}) - \lambda_k\,X\beta(X^k)$$

comme $\beta(X\,Q) = \displaystyle\sum_{k=0}^{m}\lambda_k\beta(X^{k+1})$ et $\beta(Q) = \displaystyle\sum_{k=0}^{m}\lambda_k\beta(X^k)$ alors d'après la linéarité de $\mathcal{D}$ il vient

$$\mathcal{D}(\beta(Q)) = \sum_{k=0}^{m}\lambda_k\,\mathcal{D}\left(\beta(X^k)\right)$$

donc

$$\begin{aligned}
\frac{X(1-X)}{n}\,\mathcal{D}\left(\beta(X^k)\right) &= \sum_{k=0}^{m}\lambda_k\,\frac{X(1-X)}{n}\mathcal{D}(\beta(X^k))\\
&= \sum_{k=0}^{m}\lambda_k\,\left(\beta(X^{k+1})-X\beta(X^k)\right)\\
&= \sum_{k=0}^{m}\lambda_k\,\beta(X^{k+1})-X\,\sum_{k=0}^{m}\lambda_k\,\beta(X^k)\\
&= \beta(X\,Q)-X\,\beta(Q)
\end{aligned}$$

car $\beta(X\,Q)=\sum_{k=0}^{m}\lambda_k\beta(X^{k+1})$ et $\beta(Q)=\sum_{k=0}^{m}\lambda_k\beta(X^k)$, d'où on déduit que

$$\forall Q\in\mathbb{C}[X]\quad \text{on a}\quad \beta(XQ)=\frac{X(1-X)}{n}\,\mathcal{D}(\beta(Q))+X\beta(Q)$$

(c) Calculons $\beta(X)$ et $\beta(X^2)$: en effet,
pour $Q=1$ on a $\mathcal{D}(1)=0$, alors d'après la question 6-(b) il vient

$$\beta(X)=\frac{X(1-X)}{n}\,\mathcal{D}(\beta(1))+X\beta(1)=\frac{X(1-X)}{n}\,\mathcal{D}(1)+X$$

donc $\beta(X)=X$,
et pour $Q=X$, on a $\beta(X^2)=\frac{X(1-X)}{n}\,\mathcal{D}(\beta(X))+X\beta(X)$, donc

$$\beta(X^2)=\frac{X(1-X)}{n}\,\mathcal{D}(X)+X^2=\frac{X(1-X)}{n}+X^2$$

d'où $\beta(X^2)=\frac{n-1}{n}\,X^2+\frac{1}{n}\,X$.
On peut continuer les calculs pour $Q=X^3$ on trouve

$$\beta(X^2)=\frac{n^2-3\,n+2}{n^2}\,X^3+\frac{n^2+2\,n-3}{n^2}\,X^2+\frac{1}{n^2}\,X.$$

Problème 3

Soient $P=X^3-X-1$ et $Q=X^3+X^2-1$ deux polynômes.

I) Soit $B=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_1X+a_0\in\mathbb{Z}[X]$.

1. Montrer que si un nombre rationel $\frac{p}{q}\in\mathbb{Q}$, ($p\in\mathbb{N}$, $q\in\mathbb{Z}^*$, p et q sont premiers entre eux), est une racine de B, alors :

$$a_np^n+a_{n-1}p^{n-1}q+\ldots+a_1pq^{n-1}+a_0q^n=0.$$

2. En déduire que p divise a_0 et q divise a_n.
3. Déduire de ce qui précède que les polynômes P et Q ne possèdent aucune racine dans $\mathbb{Q}$.

II) Par la suite, on désigne par ω l'unique racine réelle de P.

1. En utilisant le fait que $\omega \notin \mathbb{Q}$, montrer que P n'est pas divisible par aucun polynôme non constant de $\mathbb{Q}[X]$ de degré ≤ 2.
2. Soit $D = r_0X^2 + r_1X + r_2 \in \mathbb{Q}[X]$ un polynôme de degré 2. On suppose que ω est une racine de D.
   a. Montrer que : $\omega^3 = \omega + 1 = -\frac{r_1}{r_0}\omega^2 - \frac{r_2}{r_0}\omega$.
   b. En déduire que $r_1 \neq 0$ et que $\frac{r_0}{r_1} + \frac{r_2}{r_1} = \frac{r_1}{r_0}$ et $\frac{r_0}{r_1} = \frac{r_2}{r_0}$. (**Indication** : *pour cela écrire ω^2 de deux façons différentes*).
   c. Montrer que $\frac{r_0}{r_1}$ est alors une racine de Q, et en déduire que ω ne peut être une racine de D.
3. Déduire de ce qui précède que P est premier, dans $\mathbb{R}[X]$, avec tout polynôme de $\mathbb{Q}[X]$ de degré 1 ou 2.
4. Montrer que les nombres réels 1, ω et ω^2 sont linéairement indépendants dans $\mathbb{R}$ considéré comme espace vectoriel sur $\mathbb{Q}$.
5. On désigne par F l'ensemble des nombres réels de la forme $\mathrm{R}(\omega)$ où $\mathrm{R}(X)$ est un polynôme de $\mathbb{Q}[X]$; $F = \{\mathrm{R}(\omega) \,/\, \mathrm{R}(X) \in \mathbb{Q}[X]\}$.
   a. Montrer que F est un sous-espace vectoriel de $\mathbb{R}$ considéré comme espace vectoriel sur $\mathbb{Q}$.
   b. Montrer par récurrence sur n que :
   $$\forall n \in \mathbb{N}, \quad \exists q_0, q_1, q_2 \in \mathbb{Q} \quad \text{tel que} \quad \omega^n = q_0 + q_1\omega + q_2\omega^2.$$
   c. En déduire que $\{1, \omega, \omega^2\}$ est une base du sous-espace vectoriel F.

Solution : Soient $P = X^3 - X - 1$ et $Q = X^3 + X^2 - 1$ deux polynômes.

I) Soit $B = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$.

1. Montrons que si un nombre rationel $\dfrac{p}{q} \in \mathbb{Q}$, ($p \in \mathbb{N}$, $q \in \mathbb{Z}^*$, p et q sont premiers entre eux), est une racine de B, alors :
$$a_np^n + a_{n-1}p^{n-1}q + \ldots + a_1pq^{n-1} + a_0q^n = 0.$$
le nombre rationel $\dfrac{p}{q} \in \mathbb{Q}$ est une racine de B, alors $B\left(\dfrac{p}{q}\right) = 0$, donc
$$B\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\left(\frac{p}{q}\right) + a_0 = 0$$
soit $a_n\left(\dfrac{p^n}{q^n}\right) + a_{n-1}\left(\dfrac{p^{n-1}}{q^{n-1}}\right) + \ldots + a_1\left(\dfrac{p}{q}\right) + a_0 = 0$, donc
$$\frac{a_n\,p^n + a_{n-1}\,p^{n-1}\,q + \ldots + a_1\,p\,q^{n-1} + a_0\,q^n}{q^n} = 0$$
on multiplie l'équation fois q^n, il vient
$$q^n\frac{a_n\,p^n + a_{n-1}\,p^{n-1}\,q + \ldots + a_1\,p\,q^{n-1} + a_0\,q^n}{q^n} = q^n\,0 = 0$$
d'où $a_n\,p^n + a_{n-1}\,p^{n-1}\,q + \ldots + a_1\,p\,q^{n-1} + a_0\,q^n = 0$.

2. Le nombre p divise a_0 et q divise a_n : en effet, on a

$$a_n\, p^n + a_{n-1}\, p^{n-1}\, q + \ldots + a_1\, p\, q^{n-1} + a_0\, q^n = 0,$$

alors $p\, \left(a_n\, p^{n-1} + a_{n-1}\, p^{n-2}\, q + \ldots + a_1\, q^{n-1}\right) = -a_0\, q^n$, donc p divise $a_0\, q^n$, comme p et q sont premiers entre eux, alors $p \wedge q^n = 1$,
donc on déduit que p divise a_0.
De même, on a $-a_n\, p^n = q\, \left(a_{n-1}\, p^{n-1} + \ldots + a_1\, p\, q^{n-2} + a_0\, q^{n-1}\right)$,
alors q divise $a_n\, p^n$, et comme $p \wedge q^n = 1$ donc on déduit que q divise a_n.

3. Soient $P = X^3 - X - 1$ et $Q = X^3 + X^2 - 1$, alors $P \in \mathbb{Z}[X]$ et $Q \in \mathbb{Z}[X]$.
Pour les deux polynômes P et Q on a $a_n = 1$ et $a_0 = -1$.
Si le nombre rationel $\dfrac{p}{q} \in \mathbb{Q}$ est une racine de P et de Q, alors

$$P\left(\frac{p}{q}\right) = 0 \quad \text{et} \quad Q\left(\frac{p}{q}\right) = 0$$

donc $P\left(\dfrac{p}{q}\right) = 0 \quad \Leftrightarrow \quad p$ divise -1, d'où $p = 1$ où bien $p = -1$,
et de même, $Q\left(\dfrac{p}{q}\right) = 0 \quad \Leftrightarrow \quad q$ divise 1, d'où $q = 1$ où bien $q = -1$,
d'où $\dfrac{p}{q} = 1$ où bien $\dfrac{p}{q} = -1$,
or $P\,(1) = 1^3 - 1 - 1 = -1 \neq 0$, $P\,(-1) = (-1)^3 - (-1) - 1 = -1 \neq 0$, $Q\,(1) = 1^3 + 1^2 - 1 = 1 \neq 0$ et $Q\,(-1) = (-1)^3 + (-1)^2 - 1 = -1 \neq 0$, alors
-1 et 1 ne sont pas des racines de P et Q, d'où les polynômes P et Q ne possèdent pas de racines dans $\mathbb{Q}$.

II) On désigne par ω l'unique racine réelle de P avec $\omega \notin \mathbb{Q}$.

1. Montrons que P n'est pas divisible par aucun polynôme non constant de $\mathbb{Q}[X]$ de degré ≤ 2 : en effet, on a ω l'unique racine réelle de P, alors $X - \omega$ divise le polynôme P et par une division euclidienne il vient

$$P = (X - \omega)(X^2 + \omega\, X + \omega^2 - 1),$$

comme $\omega \notin \mathbb{Q}$, alors $X^2 + \omega\, X + \omega^2 - 1 \notin \mathbb{Q}[X]$, donc P n'est divisible par aucun polynôme de degré égal à 2 dans $\mathbb{Q}[X]$.

2. On prend $D = r_0 X^2 + r_1 X + r_2 \in \mathbb{Q}[X]$ un polynôme de degré 2. Supposons que ω est une racine de D.

   a. Montrons que : $\omega^3 = \omega + 1 = -\dfrac{r_1}{r_0}\,\omega^2 - \dfrac{r_2}{r_0}\,\omega$: en effet, ω est une racine de P, alors $P(\omega) = \omega^3 - \omega - 1 = 0$, donc $\omega^3 = \omega + 1$.
   De même, ω est une racine de D, alors $D(\omega) = r_0\, \omega^2 + r_1\, \omega + r_2 = 0$,
   comme $r_0 \neq 0$, alors $\omega^2 + \dfrac{r_1}{r_0}\,\omega + \dfrac{r_2}{r_0} = 0$, donc $\omega^2 = -\dfrac{r_1}{r_0}\,\omega - \dfrac{r_2}{r_0}$, donc

$$\omega^3 = -\frac{r_1}{r_0}\,\omega^2 - \frac{r_2}{r_0}\,\omega$$

   d'où le résultat $\omega^3 = \omega + 1 = -\dfrac{r_1}{r_0}\,\omega^2 - \dfrac{r_2}{r_0}\,\omega$

b. Si $r_1 = 0$, alors $\omega^3 = \omega + 1 = -\dfrac{r_2}{r_0}\,\omega$, donc

$$\left(1 + \frac{r_2}{r_0}\right)\omega = -1 \quad \text{d'où} \quad \omega = -\frac{r_0}{r_0 + r_2}$$

soit $\omega \in \mathbb{Q}$ ce qui est absurde puisque ω n'est pas un rationel, d'où on déduit que $r_1 \neq 0$.
D'une part on a $\omega + 1 = -\dfrac{r_1}{r_0}\,\omega^2 - \dfrac{r_2}{r_0}\,\omega$, alors

$$\frac{r_1}{r_0}\,\omega^2 = -\left(1 + \frac{r_2}{r_0}\right)\omega - 1, \quad \text{d'où} \quad \omega^2 = -\left(\frac{r_0}{r_1} + \frac{r_2}{r_1}\right)\omega - \frac{r_0}{r_1}$$

et d'autre part, on a $\omega^2 + \dfrac{r_1}{r_0}\,\omega + \dfrac{r_2}{r_0} = 0$, alors

$$\omega^2 = -\frac{r_1}{r_0}\,\omega - \frac{r_2}{r_0}$$

donc il vient

$$-\frac{r_1}{r_0}\,\omega - \frac{r_2}{r_0} = -\left(\frac{r_0}{r_1} + \frac{r_2}{r_1}\right)\omega - \frac{r_0}{r_1} \quad \Leftrightarrow \quad \left(\frac{r_0}{r_1} + \frac{r_2}{r_1} - \frac{r_1}{r_0}\right)\omega = \frac{r_0}{r_1} - \frac{r_2}{r_0}$$

c'est à dire que $\dfrac{r_0}{r_1} + \dfrac{r_2}{r_1} - \dfrac{r_1}{r_0} = 0$ et $\dfrac{r_0}{r_1} - \dfrac{r_2}{r_0} = 0$, car sinon

$$\omega = \frac{\dfrac{r_0}{r_1} - \dfrac{r_2}{r_0}}{\dfrac{r_0}{r_1} + \dfrac{r_2}{r_1} - \dfrac{r_1}{r_0}} = \frac{r_0^2 - r_1\,r_2}{r_0^2 + r_0\,r_2 - r_1^2} \quad \text{serait un rationel ce qui est absurde}$$

d'où on déduit que $\dfrac{r_1}{r_0} = \dfrac{r_0}{r_1} + \dfrac{r_2}{r_1}$ et $\dfrac{r_2}{r_0} = \dfrac{r_0}{r_1}$

c. Montrons que $\frac{r_0}{r_1}$ est alors une racine de Q : en effet, on a $\dfrac{r_1}{r_0} = \dfrac{r_0}{r_1} + \dfrac{r_2}{r_1}$ et $r_0^2 = r_1\,r_2$, alors

$$\frac{r_2}{r_1} = \frac{r_0^2}{r_1^2} = \left(\frac{r_0}{r_1}\right)^2 \quad \text{donc} \quad \frac{r_1}{r_0} = \frac{r_0}{r_1} + \left(\frac{r_0}{r_1}\right)^2$$

on multiplie l'équation fois $\dfrac{r_0}{r_1}$, il vient

$$1 = \left(\frac{r_0}{r_1}\right)^2 + \left(\frac{r_0}{r_1}\right)^3 \quad \text{soit} \quad \left(\frac{r_0}{r_1}\right)^3 + \left(\frac{r_0}{r_1}\right)^2 - 1 = 0$$

d'où $Q\left(\dfrac{r_0}{r_1}\right) = 0$, ce qui prouve que $\dfrac{r_0}{r_1}$ est une racine de Q.
On a $\dfrac{r_0}{r_1} \in \mathbb{Q}$ est une racine rationel de Q et comme Q ne peut pas avoir de racine dans $\mathbb{Q}$, d'où l'hypothèse ω est une racine de D est fausse. D'où on déduit que ω ne peut être une racine de D.

3. On a $P = X^3 - X - 1$, soit $D \in \mathbb{Q}[X]$ un polunôme de degré $\mathrm{d}^o D \leq 2$. Soit $R \in \mathbb{R}[X]$ un diviseur commun de P et D.

- Si $d^o R = 1$, alors R admet une racine réelle, notée ω_0 ; et comme R divise P alors $\omega_0 = \omega$ puisque P admet ω comme l'unique racine réelle, donc ω est une racine de D car R divise D, donc $D(\omega) = 0$ ce qui est absurde car d'après $\mathrm{II}-2)$ on a $D \in \mathbb{Q}[X]$. D'où R n'est pas de degré 1.
- Si $d^o R = 2$, alors R divise D et $d^o D = 2$, donc il existe un sclaire λ non nul tel que $R = \lambda\, D$, donc $D = \dfrac{1}{\lambda}\, R$ appartient à $\mathbb{Q}[X]$ ce qui est faux. D'où R n'est pas de degré 2.

D'où $d^o R = 0$, d'où on déduit que R est constant, soit $P \wedge D = 1$

4. Soit $\mathbb{R}$ un espace vectoriel sur $\mathbb{Q}$, soit r_0, r_1 et r_2 des scalaires dans $\mathbb{Q}$ tels que $r_0\,\omega^2 + r_1\,\omega + r_2 = 0$, alors ω est la racine de $D = r_0\,X^2 + r_1\,X + r_2$ dans $\mathbb{Q}[X]$.
Si $r_0 \neq 0$, alors d'après $\mathrm{II}-2)$, D ne peut avoir ω comme racine, donc $r_0 = 0$.
Si $r_1 \neq 0$, alors $r_1\,\omega + r_2 = 0$ implique $\omega = -\dfrac{r_2}{r_1} \in \mathbb{Q}$ ce qui est absurde d'après $\mathrm{II}-2)$, donc $r_1 = 0$, d'où $r_2 = 0$.
Finalement $r_0 = r_1 = r_2 = 0$, ce qui prouve que le système $\{1, \omega, \omega^2\}$ est libre dans $\mathbb{R}$ comme espace vectoriel sur $\mathbb{Q}$.
5. Soit $F = \{\mathrm{R}(\omega)\,/\,\mathrm{R}(X) \in \mathbb{Q}[X]\}$ l'ensemble des nombres réels de la forme $\mathrm{R}(\omega)$ où $\mathrm{R}(X)$ est un polynôme de $\mathbb{Q}[X]$; .
   a. Montrons que F est un sous-espace vectoriel de $\mathbb{R}$ considéré comme espace vectoriel sur $\mathbb{Q}$: en effet, d'abord $F \neq \emptyset$ car $\omega^2 - 1 \in F$ avec $R(X) = X^2 - 1$. Soient α et β dans $\mathbb{Q}$ et R_1 et R_2 dans $\mathbb{Q}[X]$, alors

   $$\alpha\, R_1(\omega) + \beta\, R_2(\omega) \in F \quad \text{car} \quad \alpha\, R_1 + \beta\, R_2 \in \mathbb{Q}[X]$$

   d'où F est un sous-espaace vectoriel de $\mathbb{R}$ considéré comme espace vectoriel sur $\mathbb{Q}$.
   b. Montrons par récurrence sur n que :

   $$\forall n \in \mathbb{N}, \quad \exists q_0, q_1, q_2 \in \mathbb{Q} \quad \text{tel que} \quad \omega^n = q_0 + q_1\omega + q_2\omega^2$$

   en effet,
   - pour $n = 0$, on a $\omega^0 = q_0 + q_1\,\omega + q_2\,\omega^2$, alors

   $$\begin{aligned}
   \omega^0 = q_0 + q_1\,\omega + q_2\,\omega^2 \quad & \Rightarrow \quad q_0 - 1 + q_1\,\omega + q_2\,\omega^2 = 0 \\
   & \Rightarrow \quad (q_0 - 1)\omega + q_1\,\omega^2 + q_2\,\omega^3 = 0 \\
   & \qquad\ \ \text{en multipliant fois} \quad \omega \\
   & \Rightarrow \quad (q_0 - 1)\omega + q_1\,\omega^2 + q_2\,(\omega + 1) = 0 \\
   & \qquad\ \ \text{car} \quad \omega^3 = \omega + 1 \\
   & \Rightarrow \quad q_2 + (q_0 + q_2 - 1)\omega + q_1\,\omega^2 = 0
   \end{aligned}$$

   or le système $\{1, \omega, \omega^2\}$ est libre dans $\mathbb{R}$ comme espace vectoriel sur $\mathbb{Q}$, alors $q_2 = 0$, $q_1 = 0$ et $q_0 + q_2 - 1 = 0$, d'où $q_2 = q_1 = 0$ et $q_0 = 1$, ce qui prouve que l'égalité $0\,\omega^2 + 0\,\omega + 1 = 1 = \omega^0$ est vraie pour $n = 0$.
   - Supposons que l'équation est vraie jusqu'à l'ordre n, c'est à dire que pour n on a $\omega^n = q_0 + q_1\,\omega + q_2\,\omega^2$. Montrons que l'équation reste encore vraie

pour l'ordre $n+1$. On a $\omega^n = q_0 + q_1\,\omega + q_2\,\omega^2$, alors en multipliant cette équation fois ω, il vient

$$\omega^{n+1} = q_0\,\omega + q_1\,\omega^2 + q_2\,\omega^3$$

or $\omega^3 = \omega + 1$, alors $\omega^{n+1} = q_0\,\omega + q_1\,\omega^2 + q_2\,(\omega+1) = q_2 + (q_0+q_2)\,\omega + q_1\,\omega^2$, donc il existe $\tilde{q}_0 = q_2$, $\tilde{q}_1 = q_0 + q_2$ et $\tilde{q}_2 = q_1$ tels que $\omega^{n+1} = \tilde{q}_0 + \tilde{q}_1\,\omega + \tilde{q}_2\,\omega^2$, d'où la propriété est encore vraie pour l'ordre $n+1$.

– D'après la propriété de récurrence, $\forall n \in \mathbb{N}, \quad \exists q_0, q_1, q_2 \in \mathbb{Q}$ tels que $\omega^n = q_0 + q_1\omega + q_2\omega^2$

c. Le système $\{1, \omega, \omega^2\}$ est libre dans F. Il reste à montrer qu'elle est génératrice. Soit P dans $\mathbb{Q}[X]$ avec $P = \sum_{k=0}^{n} \lambda_k\, X^k$, alors

$$P(\omega) = \sum_{k=0}^{n} \lambda_k\, \omega^k$$

or pour tout $k \in \mathbb{N}$, il existe α_k, β_k et γ_k dans $\mathbb{Q}$ tels que $\omega^k = \alpha_k + \beta_k\,\omega + \gamma_k\,\omega^2$, alors

$$\begin{aligned} P(\omega) &= \sum_{k=0}^{n} \lambda_k\, \left(\alpha_k + \beta_k\,\omega + \gamma_k\,\omega^2\right) \\ &= \left(\sum_{k=0}^{n} \lambda_k\,\alpha_k\right) + \left(\sum_{k=0}^{n} \lambda_k\,\beta_k\right)\,\omega + \left(\sum_{k=0}^{n} \lambda_k\,\gamma_k\right)\,\omega^2 \end{aligned}$$

donc $P(\omega) = \rho + \eta\,\omega + \theta\,\omega^2$ où $\rho = \sum_{k=0}^{n} \lambda_k\,\alpha_k$, $\eta = \sum_{k=0}^{n} \lambda_k\,\beta_k$ et $\theta = \sum_{k=0}^{n} \lambda_k\,\gamma_k$, ce qui montre que la famille $\{1, \omega, \omega^2\}$ engendre F, d'où $\{1, \omega, \omega^2\}$ est une base du sous-espace vectoriel F.
Finalement, on déduit la dimension de F : $\dim_{\mathbb{Q}}(F) = 3$.