2020-2021 **Algèbre L3B**

Examen : Mardi 5 Janvier 2021
Durée de l'épreuve 4h

Tout document et appareil électronique (calculatrice, téléphone portable) est interdit.

Barème indicatif : Cours :

Questions de cours.

1. Démontrer que le groupe $\mathrm{SO}_2(\mathbb{R})$ est isomorphe au groupe $\mathbb{U} = \{z \in \mathbb{C} |\ |z| = 1\}$.
2. Rappeler la définition d'un élément irréductible dans un anneau intègre.
3. Soit A un anneau principal, et $a \in A$ un élément irréductible. Montrer que (a) est un idéal maximal.

Exercice 1.

1. Rappeler la définition d'action transitive. Qu'est-ce que cela signifie sur le nombre d'orbites pour l'action ?
   L'action de G sur X est transitive si pour tout $x, y \in X$, il existe $g \in G$ tel que $g.x = y$. Ceci est équivalent à dire que pour tout $x \in X$, l'orbite de x $\mathcal{O}(x) = X$, autrement dit il n'y a qu'une seule orbite pour l'action.
2. Montrer que $\mathfrak{S}_n$ agit transitivement sur $\{1, \dots, n\}$.
   Soit $i, j \in \{1, \dots, n\}$, alors il existe $\sigma \in \mathfrak{S}_n$ tel que $\sigma(i) = j$. En effet, si $i = j$ on peut prendre $\sigma = \mathrm{id}$, et si $i \neq j$, on peut prendre pour σ la transposition $\sigma = (ij)$.
3. Le sous-groupe engendré par le n-cycle $(1 \cdots n)$ agit-il transitivement sur $\{1, \dots, n\}$?
   Notons $c = (1 \cdots n)$ le n-cycle. Une récurrence simple montre que pour tout $p \geq 0$ et pour tout $i \in \{1, \dots, n\}$, on a $c^p(i) = i + p$ où les indices sont pris modulo n. En effet c'est clair pour $p = 0$ et $p = 1$. Supposons que c'est vrai pour p, alors $c^{p+1}(i) = c \circ c^p(i) = c(p + i) = p + i + 1$. Soit maintenant $i, j \in \{1, \dots, n\}$. Alors si $j \geq i$, on a $c^{j-i}(i) = j$, et si $j \leq i$, alors on a $c^{-(i-j)}(i) = j$. L'action est donc transitive.

Soit G un groupe fini agissant sur un ensemble fini X de cardinal ≥ 2.

4. Montrer que l'application $G \times (X \times X) \to (X \times X)$ définie par
$$g(x,y) := (gx, gy), \ g \in G, \ (x,y) \in X \times X$$
définit une action de groupe de G sur $X \times X$.
On a bien $1_G.(x,y) = (1_G x, 1_G y) = (x,y)$. Par ailleurs on a pour $g, h \in G$ et $(x,y) \in X^2$, on a
$$g.(h.(x,y)) = g.(hx, hy) = (g(hx), g(hy)) = ((gh)x, (gh)y) = gh.(x,y).$$
On a donc bien une action de G sur X^2.

On dit que l'action de G sur X est doublement transitive si
$$\forall x \neq y \in X \ \ \forall x' \neq y' \in X \quad \exists g \in G \text{ tel que } gx = x' \text{ et } gy = y'.$$

5. Le groupe $\mathfrak{S}_n$ agit-il doublement transitivement sur $\{1, \cdots, n\}$?
Soient $x \neq y$, et $x' \neq y'$ dans $\{1, \dots, n\}$. Alors si x, y, x' et y' sont deux à deux distincts, on pose $\sigma = (xx')(yy')$ et on a bien $\sigma(x) = x'$ et $\sigma(y) = y'$. Si $x = x'$ (rec. $y = y'$) alors on pose $\sigma = (yy')$ (rec. $\sigma(yy')$). Si $x' = y$ alors on pose $\sigma = (xx'y')$ et on a bien $\sigma(x) = x'$ et $\sigma(y) = \sigma(x') = y'$. Enfin si $x = y'$ on pose $\sigma = (xx'y)$ et on a bien $\sigma(x) = x'$, $\sigma(y) = x = y'$. L'action est donc bien doublement transitive.
6. Le sous-groupe engendré par le n-cycle $(1 \cdots n)$ agit-il doublement transitivement sur $\{1, \dots, n\}$?
Si $n \geq 3$, posons $x = 1$, $y = 2$, $x' = 1$ et $y' = 3$. Alors s'il existe $p \in \mathbb{Z}$ tel que $c^p(x) = x'$, on a nécessairement $p = 0$ modulo n. Mais alors $c^p(y) = y \neq y'$. L'action n'est donc pas doublement transitive. Par contre si $n = 2$, alors on a $\mathfrak{S}_2 = \langle c \rangle$, et donc l'action est doublement transitive par la question précédente.
7. Montrer que si l'action est doublement transitive, alors elle est transitive.
Supposons l'action doublement transitive et soient $x, x' \in X$. Comme le cardinal de X est ≥ 2, il existe $y \neq x$, et il existe $y' \neq x'$. L'action étant doublement transitive, il existe $g \in G$ tel que $gx = x'$ et tel que $gy = y'$. Donc l'action est transitive.
8. Montrer que l'action de G sur X est doublement transitive si et seulement l'action de G sur $X \times X$ a exactement 2 orbites. (On pourra introduire le sous-ensemble $\Delta := \{(x,x) \in X^2, x \in X\}$ de X^2 et son complémentaire).
Notons $\Delta := \{(x,x) \in X^2, x \in X\}$. On a alors $X^2 \setminus \Delta = \{(x,y) \in X^2 | x \neq y\}$. Supposons l'action doublement transitive, alors pour tout $(x,y) \in X^2 \setminus \Delta$ et pour tout $(x', y') \in X^2 \setminus \Delta$, il existe $g \in G$ tel que $g.(x,y) = (gx, gy) = (x', y')$. Autrement dit l'ensemble $X^2 \setminus \Delta$ est une orbite pour l'action de G sur X^2. De plus par la question précédente, l'action est transitive et donc si $(x,x) \in \Delta$ et si $(y,y) \in \Delta$, il existe $g \in G$ tel que $gx = y$ autrement dit $g(x,x) = (y,y)$, donc Δ est une orbite.
Réciproquement, supposons que l'action de G sur X^2 a exactement 2 orbites. Soit $(x,x) \in \Delta$, alors $g.(x,x) = (gx, gx)$ est dans Δ. Donc Δ est une union d'orbites. De même pour $X^2 \setminus \Delta$. Donc si l'action a exactement deux orbites, ces deux orbites sont nécessairement Δ et $X^2 \setminus \Delta$ (puisque ces deux ensembles sont non vides). Le fait que $X^2 \setminus \Delta$ soit une orbite signifie exactement que l'action est doublement transitive.

9. Pour $g \in G$, on note $\mathrm{Fix}(g) := \{x \in X \mid gx = x\}$ l'ensemble des points fixés par g. En utilisant la formule de Burnside pour l'action de G sur $X \times X$, montrer que si l'action est doublement transitive on a
$$2|G| = \sum_{g \in G} |\mathrm{Fix}(g)|^2.$$
Soit G agissant sur un ensemble Y, la formule de Burnside dit que le nombre d'orbites pour l'action de G sur Y est donné par
$$\frac{1}{|G|} \sum_{g \in G} |\{y \in Y| \; g.y = y\}|.$$
Appliquons cette formule pour l'action de G sur X^2 dans le cas où l'action est doublement transitive. Le nombe d'orbites est alors égal à deux par la question précédente, et on a donc
$$2 = \frac{1}{|G|} \sum_{g \in G} |\{(x,y) \in X^2 | g.(x,y) = (x,y)\}|.$$
Or on a $g.(x,y) = (x,y)$ si et seulement si $gx = x$ et $gy = y$. Donc un couple (x,y) est dans l'ensemble $\{(x,y) \in X^2 | g.(x,y) = (x,y)\}$ si et seulement si $x \in \mathrm{Fix}(g)$ et $y \in \mathrm{Fix}(g)$. Autrement dit on a
$$\{(x,y) \in X^2 | g.(x,y) = (x,y)\} = \mathrm{Fix}(g) \times \mathrm{Fix}(g).$$
On a donc $|\{(x,y) \in X^2 | g.(x,y) = (x,y)\}| = |\mathrm{Fix}(g)|^2$ et on obtient la formule voulue.

Exercice 2. Soit A un anneau commutatif. On considère l'anneau produit $A^2 = A \times A$ muni des lois $(a,b) + (a',b') = (a + a', b + a')$ et $(a,b).(a',b') = (aa', bb')$. On note p_1 (resp. p_2) la projection de A^2 sur A définie par $p_1(x,y) = x$ (resp. $p_2(x,y) = y$)). On rappelle que ce sont des morphismes d'anneaux.

1. Soit I un idéal de A, montrer que
$$B = \{(a,b) \in A^2 | \; a - b \in I\}$$
est un sous-anneau de A.
Soient $(a,b) \in B$ et $(a',b') \in B$. Alors on a $(a,b) - (a',b') = (a - a', b - b')$. Par ailleurs, $(b - b') - (a - a') = (b - a) - (b' - a')$. Les éléments $b - a$ et $b' - a'$ sont dans I qui est un idéal donc un sous-groupe, donc $(b - b') - (a - a')$ est dans I et donc $(a,b) - (a',b'))$ est dans I, et $(B, +)$ est un sous-groupe de $(A^2, +)$.
On a de plus $(a,b).(a',b') = (aa', bb')$ et on a
$$bb' - aa' = bb' - ba' + ba' - aa' = b(b' - a') + (b - a)a'.$$
Comme $b' - a'$ est dans I et que $(b - a)$ est dans I, $bb' - aa'$ est aussi dans I, et donc $(a,b).(a',b')$ est dans B.
Enfin $1_{A^2} = (1_A, 1_A)$ est dans B car $1_A - 1_A = 0_A$ est dans I. Donc $B(+,.)$ est un sous-anneau de A^2.

2. Soient I_1 et I_2 deux idéaux de A, montrer que $I_1 \times I_2$ est un idéal de A^2, et qu'on a un isomorphisme d'anneaux $A^2/I_1 \times I_2 \simeq A/I_1 \times A/I_2$.

   Comme I_1 et I_2 sont des sous-groupes, alors $I_1 \times I_2$ est un sous-groupe de A^2. Soit $(a, b) \in I_1 \times I_2$ et $(x, y) \in A^2$, alors il est clair que $(a, b).(x, y) = (ax, by)$ est dans $I_1 \times I_2$. L'ensemble $I_1 \times I_2$ est donc un idéal de A^2.

   Considérons maintenant l'application $A \times A \to A/I_1 \times A/I_2$ envoyant (a, b) sur $(\bar{a}, \bar{b})$ où $\bar{a}$ est la classe de a modulo I_1 et $\bar{b}$ celle de b modulo I_2. C'est un morphisme d'anneaux qui est surjectif. Un élément (x, y) est dans le noyau de cette application si et seulement si $\bar{x} = \bar{0}$ et $\bar{y} = \bar{0}$ c'est-à-dire si et seulement si $x \in I_1$ et $y \in I_2$. Le noyau de cette application est donc égal à $I_1 \times I_2$. Par le théorème de factorisation, on a donc un isomorphisme $A^2/I_1 \times I_2 \simeq A/I_1 \times A/I_2$.

3. Soit J un idéal de A^2.

   (a) Montrer que $J_1 = p_1(J)$ et $J_2 = p_2(J)$ sont des idéaux de A.

   J est un sous-groupe de A^2, et p_1 est un morphisme de groupe donc $J_1 = p_1(J)$ est un sous-groupe de A. Soit $a \in A$ et $x \in J_1$, alors on a $x = p_1(x, y)$ avec $(x, y) \in J$. On peut alors écrire $ax = p_1(ax, y) = p_1((a, 1_A).(x, y))$. Comme (x, y) est dans J, alors $(a, 1).(x, y)$ est aussi dans J et donc ax est dans $p_1(J) = J_1$. J_1 est donc un idéal de A. De même pour J_2.

   (b) Montrer que J est inclus dans $J_1 \times J_2$.

   Soit $(x, y) \in J$, alors $p_1(x, y) = x \in p_1(J) = J_1$ et $p_2(x, y) = y \in p_2(J) = J_2$. Donc $(x, y) \in J_1 \times J_2$.

   (c) Montrer que si $x \in J_1$, alors $(x, 0_A)$ est dans J.

   Soit $x \in J_1$, alors il existe $y \in A$ tel que $(x, y) \in J$. Mais alors $(1_A, 0_A).(x, y) = (x, 0_A)$ est dans J.

   (d) Montrer que $J = J_1 \times J_2$.

   Soit $(x, y) \in J_1 \times J_2$. Alors par la question précédente, $(x, 0_A)$ est dans J et de même $(0_A, y)$ est aussi dans J. On a alors $(x, y) = (x, 0) + (0, y)$ est dans J.

4. Montrer que si A est non nul (c'est-à-dire n'est pas réduit à $\{0_A\}$), alors A^2 n'est pas intègre.

   Si A est non nul, alors $1_A \neq 0_A$, et donc $(0_A, 1_A).(1_A, 0_A) = (0_A, 0_A)$. On a donc des diviseurs de zéro, car $(0_A, 1_A) \neq (0_A, 0_A) = 0_{A^2}$.

5. En déduire que les idéaux premiers de A^2 sont de la forme $A \times I$, ou $I \times A$ avec I idéal premier de A.

   Soit J un idéal premier de A^2. Alors J est de la forme $J_1 \times J_2$ par la question 3. Le quotient A^2/J est isomorphe au quotient $A/J_1 \times A/J_2$. Si J_1 et J_2 sont des idéaux stricts, alors par la question précédente A/J n'est pas intègre. Donc si J est premier, un des idéaux (disons J_1) est égal à A. On aura alors A^2/J est isomorphe à $\{0\} \times A/J_2$ qui est canoniquement isomorphe à A/J_2. Donc si J est premier, A/J_2 est intègre, et donc J_2 est premier.

   Réciproquement, si I est premier, alors A/I est intègre. Et donc $\{0\} \times A/I \simeq A/A \times A/I \simeq A^2/(A \times I)$ est intègre, autrement dit $A \times I$ est intègre.

Exercice 3. Soit A un anneau principal, et $a, b \in A$ non nuls. On considère l'ensemble

$$E_{(a,b)} = \{(u, v) \in A^2 \mid au + bv = 1_A\}.$$

1. A quelle condition sur a et b a-t-on $E_{(a,b)} \neq \emptyset$?
   D'après le cours, l'ensemble $E_{(a,b)}$ est non vide si et seulement si le pgcd de a et b est égal à 1, autrement dit si a et b sont premiers entre eux.
2. On suppose maintenant que $E_{(a,b)} \neq \emptyset$. Soit $(u_0, v_0) \in E_{(a,b)}$. Montrer que

   $$(u, v) \in E_{(a,b)} \Leftrightarrow \exists w \in A \text{ tel que } u - u_0 = bw \text{ et } v_0 - v = aw.$$

   Soit (u, v) dans $E_{(a,b)}$, alors on a $au + bv = 1$. Mais on a aussi $au_0 + bv_0 = 1$. En faisant la différence on obtient

   $$a(u - u_0) + b(v - v_0) = 0_A$$

   On obtient donc que b divise $a(u - u_0)$. Comme a et b sont premiers entre eux, par le lemme de Gauss on obtient que b divise $u - u_0$, c'est-à-dire qu'il existe $w \in A$ avec $u - u_0 = bw$. En remplaçant dans l'équation on obtient

   $$abw + b(v - v_0) = 0_A.$$

   Puisque A est principal, il est intègre et donc on peut simplfier par b, et on obtient $v - v_0 = -aw$. Réciproquement si il existe w tel que $u - u_0 = bw$ et $v_0 - v = aw$ alors on a

   $$au + bv = a(bw + u_0) + b(v_0 - aw) = au_0 + bv_0 = 1_A$$

   donc (u, v) est dans $E_{(a,b)}$.
3. **Application :** On prend maintenant $A = \mathbb{R}[X]$. Décrire l'ensemble $E_{(a,b)}$ où $a = (X + 1)^2$ et $b = (X - 1)^2$.
   On effectue l'agorithme d'Euclide pour obtenir un couple de Bezout. On obtient

   $$X^2 + 2X + 1 = (X^2 - 2X + 1) + 4X \text{ et } X^2 - 2X + 1 = 4X\frac{X_2}{4} + 1.$$

   On obtient alors

   $$1 = (X-1)^2 - \frac{X-2}{4}(4X) = (X-1)^2 - \frac{(X-2}{4}((X+1)^2 - (X-1)^2) = \frac{X+2}{4}(X-1)^2 + \frac{2-X}{4}(X+1)^2,$$

   c'est-à-dire $u_0 = \frac{2-X}{4}$ et $v_0 = \frac{X+2}{4}$. On a alors

   $$E_{(a,b)} = \{(\frac{2-X}{4} + (X+1)^2 P, \frac{X+2}{4} + (X-1)^2 P) | P \in \mathbb{R}[X]\}.$$

Exercice 4. Soit $P = X^4 - 2X^3 - 3X^2 + 4X + 4 \in \mathbb{C}[X]$. On considère un endomorphisme f de $E = \mathbb{C}^4$ annulé par P.

1. Faire la division euclidienne de P par $(X-2)^2$, et en déduire la décomposition de P en irréductibles.

   On trouve $P = (X-2)^2(X+1)^2$.

2. Montrer que
$$E = \mathrm{Ker}(f - 2\mathrm{Id}_E)^2 \oplus \mathrm{Ker}(f + \mathrm{Id}_E)^2.$$

   Les polynômes $P_1 = (X+1)^2$ et $P_2 = (X-2)^2$ sont premiers entre eux. Par le lemme de décompositions des noyaux appliqué à f on obtient donc
$$\mathrm{Ker}(P(f)) = \mathrm{Ker}(P_1(f)) \oplus \mathrm{Ker}(P_2(f)).$$

   Par ailleurs P est annulateur de f donc $P(f) = 0_{\mathcal{L}(E)}$ et donc $\mathrm{Ker}P(f) = E$. On obtient donc l'égalité voulue.

3. Quels sont les polynômes minimaux μ_f possibles pour f ? Pour lesquels f est-il diagonalisable ? Donner les formes diagonales possibles (à permutation des coefficients diagonaux près).

   Tout polynôme annulateur est un multiple du polynôme minimal. Les polynômes minimaux possibles sont donc les diviseurs de P qui sont :
$$X+1,\ X-2,\ (X+1)^2,\ (X-2)^2,\ (X+1)(X-2),\ (X+1)^2(X-2),\ (X+1)(X-2)^2,\text{ et } (X+1)^2(X-2)^2.$$

   L'endomorphisme f est diagonalisable si et seulement son polynôme minimal est scindé à racines simples. Donc f est diagonalisable si et seulement si son polynôme minimal est
$$X-1,\ X-2,\ \text{ et } (X+1)(X-2).$$

   On obtient alors les matrices diagonales
$$\begin{pmatrix}-1&&&\\&-1&&\\&&-1&\\&&&-1\end{pmatrix},\begin{pmatrix}-1&&&\\&-1&&\\&&-1&\\&&&2\end{pmatrix},\begin{pmatrix}-1&&&\\&-1&&\\&&2&\\&&&2\end{pmatrix},\begin{pmatrix}-1&&&\\&2&&\\&&2&\\&&&2\end{pmatrix},\begin{pmatrix}2&&&\\&2&&\\&&2&\\&&&2\end{pmatrix}$$

On suppose maintenant que le polynôme caractéristique de f est P.

4. Quelles sont les dimensions de $\mathrm{Ker}(f - 2\mathrm{Id}_E)^2$ et $\mathrm{Ker}(f + \mathrm{Id}_E)^2$?

   D'après le cours, la dimension de $\mathrm{Ker}(f + \mathrm{Id}_E)^2 = \mathrm{Ker}P_1(f)$ est égale à 2 qui est la multiplicité du polynôme P_1 dans χ_f. De même $\mathrm{Ker}(f - 2\mathrm{Id}_E)$ est de dimension 2.

5. Donner trois exemples de matrices non diagonalisables et non semblables deux à deux dont le polynôme caractéristique est P. (On justifiera bien pourquoi elles ne sont pas diagonalisable et pourquoi elles ne sont pas deux à deux semblables).

   Considérons les matrices triangulaires supérieures suivantes
$$A = \begin{pmatrix}-1&1&0&0\\&-1&0&0\\&&2&0\\&&&2\end{pmatrix}, B = \begin{pmatrix}-1&1&0&0\\&-1&0&0\\&&2&1\\&&&2\end{pmatrix}, C = \begin{pmatrix}-1&1&0&0\\&-1&0&0\\&&2&1\\&&&2\end{pmatrix}$$

Pour montrer qu'elles ne sont pas diagonalisables, et qu'elles ne sont pas semblables deux à deux, on va calculer la dimension de leur sous-espaces propres. Il est facile de voir que

$$\dim V_{-1}(A) = 1, \dim V_2(A) = 2, \dim V_{-1}(B) = 2, \dim V_2(B) = 1, \dim V_{-1}(C) = 1, \dim V_2(C) = 1.$$

Ces matrices ne sont donc pas semblables. Par ailleurs la somme des sous-espaces propres n'est jamais égale à E, donc aucune n'est diagonalisable.

Exercice 5. Soit E un $\mathbb{C}$-espace vectoriel de dimension finie. Soit f un endomorphisme diagonalisable de E. On note $\chi_f = \prod_{i=1}^{r}(X - \lambda_i)^{m_i}$ son polynôme caractéristique. Pour $i = 1, \ldots, r$, on note V_{λ_i} le sous-espace propre de f associé à la valeur propre λ_i.
On considère l'ensemble

$$\mathrm{Comm}(f) = \{g \in \mathcal{L}(E) | f \circ g = g \circ f\}.$$

1. Montrer que $\mathrm{Comm}(f)$ est un sous-espace vectoriel de $\mathcal{L}(E)$.
   Soient $g_1, g_2 \in \mathrm{Comm}(f)$ et $\mu_1, \mu_2 \in \mathbb{C}$. Alors on a

   $$f \circ (\mu_1 g_1 + \mu g_2) = \mu_1 f \circ g_1 + \mu_2 f \circ g_2 = \mu_1 g_1 \circ f + \mu_2 g_2 \circ f = (\mu_1 g_1 + \mu_2 g_2) \circ f,$$

   donc $\mu_1 g_1 + \mu g_2$ est dans $\mathrm{Comm}(f)$ qui est un sous-espace vectoriel de $\mathcal{L}(E)$.
2. (Question de cours) Soit $g \in \mathrm{Comm}(f)$.
   (a) Montrer que pour tout $i = 1 \ldots, r$ le sous-espace V_{λ_i} est stable par g.
   Soit $x \in V_{\lambda_i}$, alors on a $f(x) = \lambda_i x$. Donc
   $f(g(x)) = f \circ g(x) = g \circ f(x) = g(\lambda_i x) = \lambda_i g(x)$ donc $g(x)$ est dans V_{λ_i}, autrement dit V_{λ_i} est stable par g.
   (b) On note g_i l'endomorphisme g restreint à V_{λ_i}. Montrer que si g est diagonalisable alors g_i est diagonalisable.
   Comme g est diagonalisable, son polynôme minimal μ_g est scindé à racines simples. Alors μ_g annule g_i qui est donc diagonalisable.
   (c) Montrer que si g est diagonalisable, alors il existe une base $\mathcal{B}$ telle que les matrices de f et g dans $\mathcal{B}$ sont diagonales.
   Soit $\mathcal{B}^i$ une base de V_{λ_i} qui diagonalise g_i. Comme f est diagonalisable, E est la somme des sous-espaces propres et donc l'union des bases $\mathcal{B}^i$ forme une base de E. Soit $v \in \mathcal{B}^i$. Alors v est un vecteur propre de g_i, donc un vecteur propre de g. Par ailleurs, $v \in V_{\lambda_i}$, donc v est un vecteur propre pour f. La base $\mathcal{B}$ est donc formée de vecteurs propres pour f et pour g, c'est donc une base de diagonalisation pour f et pour g.
3. Soit $g \in \mathcal{L}(E)$ tel que pour tout $i = 1, \ldots, r$, le sous-espace V_{λ_i} est stable par g. Montrer que $g \in \mathrm{Comm}(f)$.

Soit $x \in E$, alors comme f est diagonalisable, x peut s'écrire $x = x_1 + \cdots + x_r$ avec $x_i \in V_{\lambda_i}$. Comme V_{λ_i} est stable par g, on a alors $g(x_i) \in V_{\lambda_i}$. On peut alors écrire

$$g \circ f(x) = \sum_i g \circ f(x_i) = \sum_i g(\lambda_i x_i) = \sum_i \lambda_i g(x_i).$$

Par ailleurs

$$f \circ g(x) = \sum_i f(g(x_i)) = \sum_i \lambda_i g(x_i).$$

On a donc $f \circ g = g \circ f$.

4. En déduire la dimension de l'espace vectoriel $\mathrm{Comm}(f)$ en fonction des m_i.

   D'après les questions précédentes, un endomorphisme g est dans $\mathrm{Comm}(f)$ si et seulement si pour tout i V_{λ_i} est stable par g. Autrement dit g commute à f si et seulement si sa matrice est diagonale par bloc dans une base adaptée à la décomposition de E en somme de sous-espaces propres. La dimension de V_{λ_i} est m_i, donc la dimension de $\mathcal{L}(V_{\lambda_i}$ est m_i^2. Et la dimension de $\mathrm{Comm}(f)$ est alors $\sum_{i=1}^r m_i^2$.