Correction Examen session 1 2021-2022

1 et 2. Questions de cours.

3. Par le théorème de classification des groupes abéliens finis. Un groupe abélien d'ordre 36 se décompose de manière unique comme produit direct d'un groupe abélien d'ordre 9 par un groupe abélien d'ordre 4. Il y a deux groupes abéliens d'ordre 4 : $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. De même il y a deux groupes abéliens d'ordre 9 : $\mathbb{Z}/9\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Il y a donc au total 4 groupes abéliens d'ordre 36 :

$$\begin{array}{ll} \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \end{array}$$

4. Si R est un anneau commutatif unitaire, on sait que l'anneau $R[X]$ est principal si et seulement si R est en fait un corps. En particulier, $\mathbb{C}[X,Y] = (\mathbb{C}[X])[Y]$ n'est pas un anneau principal car $\mathbb{C}[X]$ n'est pas un corps (X n'est pas iversible).

5. Soit R un anneau commutatif unitaire. Le R-module $R[X]$ n'est pas de type fini. En effet, soit $P_1, \cdots, P_n$ une famille finie de $R[X]$, on pose $k = \max\{\deg P_i\}$. Tout élément du sous module de $R[X]$ engendré par les P_i et de degré au plus k. La famille $\{P_i\}$ n'engendre donc pas tout $R[X]$ (les polynômes de degré supérieur à k ne sont pas atteints).

6. Le sous-module de $\mathbb{Z}$ engendré par m et n est donné par

$$M = \{am + bn \mid a, b \in \mathbb{Z}\}$$

Ce sous-module de $\mathbb{Z}$ est égal à $\mathbb{Z}$ tout entier si et seulement si il contient 1. En effet si $M = \mathbb{Z}$, alors $1 \in M$ est évident, et réciproquement si $1 \in M$, alors $M = \mathbb{Z}$ car $\mathbb{Z}$ est engendré par 1 (en tant que groupe abélien).
Par définition, on a $1 \in M$ si et seulement si il existe $a, b \in \mathbb{Z}$ tels que $am + bn = 1$, ce qui par le théorème de Bézout est équivalent à dire que m et n sont premiers entre eux.
On obtient donc que la famille $\{m, n\}$ engendre $\mathbb{Z}$ si et seulement si m et n sont premiers entre eux.

7. Soient R un anneau commutatif unitaire, et $A \subset R$ une partie de R.

- Si A est un sous-module de R, alors A est en particulier un sous-groupe de R par définition d'un sous-module. Ensuite, pour $a \in A, r \in R$, l'élément ra est une combinaison R-linéaire d'éléments de A, donc $ra \in A$ car A est un sous-module, ce qui montre que A est absorbant. A est donc un idéal de R.
- Si A est un idéal de R, alors A est en particulier un sous-groupe de R par définition d'un idéal. Ensuite, pour $a_1, a_2 \in A, r_1, r_2 \in R$, les éléments r_1a_1 et r_2a_2 sont dans A par absorbance. Donc la combinaison linéaire $r_1a_1 + r_2a_2$ appartient aussi à A comme somme d'éléments de A, ceci montre que A est stable par combinaison linéaires dans R. Donc A est un sous-module de R.

8. Hélàs la réponse est non : $R[X]_n$ est bien un sous R-module de $R[X]$, mais ce n'est pas un sous $R[X]$-module de $R[X]$. Par la question précédente, cela revient à dire que $R[X]_n$ n'est pas un idéal de $R[X]$, mais on peut donner une preuve plus directe.
L'ensemble $R[X]_n$ contient le polynôme X^n, or, en prenant $X \in R[X]$, on a

$$X.X^n = X^{n+1} \notin R[X]_n$$

Ce qui montre que $R[X]_n$ n'est pas un sous $R[X]$-module de $R[X]$.

9. On sait que $\mathbb{Q}[X]_n$ est un $\mathbb{Q}$-espace vectoriel de dimension finie et égale à $n+1$. Son dual $\mathbb{Q}[X]_n^*$ est donc lui aussi un $\mathbb{Q}$-espace vectoriel de dimension $n+1$. La famille $\{ev_{\alpha_i}\}_{i \in [\![1, n+1]\!]}$ est une famille de cardinal $n+1$

dans $\mathbb{Q}[X]_n^*$, il suffit donc pour conclure de montrer qu'elle est libre, ou qu'elle est génératrice (on donne deux preuves ici, une seule suffisait bien-sûr).

1ère preuve : Par la dualité. Dire que $\{ev_{\alpha_i}\}_{i\in[\![1,n+1]\!]}$ est génératrice revient à montrer que Vect $\left(\{ev_{\alpha_i}\}_{i\in[\![1,n+1]\!]}\right)$ est de dimension $n+1$, ce qui est équivalent à montrer que son orthogonal au sens des formes linéaires est réduit à 0. L'orthogonal de Vect $\left(\{ev_{\alpha_i}\}_{i\in[\![1,n+1]\!]}\right)$ est égal à l'orthogonal de la famille $\{ev_{\alpha_i}\}_{i\in[\![1,n+1]\!]}$, lui même égal à l'intersection des noyaux des ev_{α_i}. Calculons Ker ev_{α_i} : on a $P \in$ Ker ev_{α_i} si et seulement si

$$ev_{\alpha_i}(P) = P(\alpha_i) = 0$$

autrement dit, l'orthogonal de la famille $\{ev_{\alpha_i}\}_{i\in[\![1,n+1]\!]}$ est constitué des polynôme admettant chacun des α_i comme racine. Comme les α_i sont distincts deux à deux, un tel polynôme serait un polynôme de degré n admettant $n+1$ racine distinctes, la seule possibilité est $P = 0$. L'orthogonal de $\{ev_{\alpha_i}\}_{i\in[\![1,n+1]\!]}$ est donc réduit à 0 : la famille est génératrice, et il s'agit donc d'une base.

2ème preuve (plus simple) : Les polynômes de Lagrange. Montrons que la famille $\{ev_{\alpha_i}\}_{i\in[\![1,n+1]\!]}$ est libre. Posons, pour $k \in [\![1, n+1]\!]$

$$P_k := \prod_{\substack{i=1\\ i\neq k}}^{n+1} (X - \alpha_i)$$

Il s'agit d'un polynôme de degré n comme produit de n monômes. Par construction, on a $P_k(\alpha_i) = 0$ pour $i \neq k$, et comme les α_i sont distincts deux à deux, on a $P_k(\alpha_k) = \prod_{\substack{i=1\\ i\neq k}}^{n+1}(\alpha_k - \alpha_i) \neq 0$.

Soit une combinaison linéaire nulle de la famille $\{ev_{\alpha_i}\}_{i\in[\![1,n+1]\!]}$:

$$0 = \sum_{i=1}^{n+1} \lambda_i ev_{\alpha_i}$$

Pour $k \in [\![1, n+1]\!]$, on a

$$0 = \sum_{i=1}^{n+1} \lambda_i ev_{\alpha_i}(P_k) = \sum_{i=1}^{n+1} \lambda_i P_k(\alpha_i) = \lambda_k P_k(\alpha_k)$$

et comme $P_k(\alpha_k) \neq 0$, on obtient que λ_k est nul, et ce pour tout k. La famille $\sum_{i=1}^{n+1} \lambda_i ev_{\alpha_i}$ est donc libre, et il s'agit d'une base.

10. Comme on se place dans $\mathbb{R}^2$ muni de sa base canonique, on fera l'identification entre un endomorphisme et sa matrice dans la base canonique. Considérons la matrice

$$M = I_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

son polynôme minimal est clairement égal à $X - 1$ (ce polynôme est annulateur et de degré 1). Et son polynôme caractéristique est égal à $(X-1)^2$ (déterminant d'une matrice diagonale).

11. On sait qu'une matrice compagnon a même polynôme minimal et caractéristique, on considère donc la matrice

$$M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

(il s'agit de la matrice compagnon pour le polynôme $X^2 + 1$). Son polynôme caractéristique est donné par

$$\begin{vmatrix} X & 1 \\ -1 & X \end{vmatrix} = X^2 + 1$$

Ce polynôme est irréductible sur $\mathbb{R}$. Or par le théorème de Cayley-Hamilton, le polynôme minimal doit diviser le polynôme caractéristique, donc le polynôme minimal de M est égal à 1 ou a X^2+1, le premier cas est impossible

(le polynôme minimal doit être annulateur), donc le polynôme minimal et le polynôme caractéristique sont tous deux égaux à X^2+1.

12. Comme E est de dimension 3, le polynôme minimal de f est de degré 3. Notons $P = X^3 + aX^2 + bX + c$ le polynôme caractéristique de l'endomorphisme f, il s'agit en particulier d'un polynôme annulateur de f.
Montrons par récurrence que pour $k \geqslant 3$, on a $f^k(u) \in \text{Vect}(u, f(u), f^2(u))$.
Pour $k = 3$, comme P est annulateur de f, on a

$$f^3(u) + af^2(u) + bf(u) + cu = 0 \Rightarrow f^3(u) = -af^2(u) - bf(u) - cu \in \text{Vect}(u, f(u), f^2(u))$$

Pour l'hérédité, on a

$$f^{k+1}(u) = f^3(f^{k-2}(u)) = -af^2(f^{k-2}(u)) - bf(f^{k-2}(u)) - cf^{k-2}u = -af^k(u) - bf^{k-1}(u) - cf^{k-2}(u)$$

ce dernier élément appartenant à $\text{Vect}(u, f(u), f^2(u))$ par hypothèse de récurrence, on a bien $f^{k+1}(u) \in \text{Vect}(u, f(u), f^2(u))$ comme annoncé.

13. D'après la question précédente, la famille $(u, f(u), f^2(u))$ est une famille génératrice de E, en effet on a vu qu'elle engendrait toute la famille $\{f^i(u) \mid i \in \mathbb{N}\}$ qui est génératrice par hypothèse. Comme E est supposé de dimension 3, et que la famille $(u, f(u), f^2(u))$ est de cardinal 3, on obtient bien qu'il s'agit d'une base de E.

14. On a vu dans la question 12 que $f(f^2(u)) = f^3(u) = -af^2(u) - bf(u) - cu$, ensuite, on a évidemment $f(u) = f(u)$ et $f(f(u)) = f^2(u)$, d'où la matrice suivante :

$$M = \begin{pmatrix} 0 & 0 & -c \\ 1 & 0 & -b \\ 0 & 1 & -a \end{pmatrix}$$

Comme il s'agit d'une matrice de l'endomorphisme f dans une certaine base, le polynôme caractéristique de M est le même que celui de f, c'est à dire $X^3 + aX^2 + bX + c$. On pouvait bien-sûr le calculer à la main, mais ça nous ferait perdre un peu de temps ;)

15.**1ere preuve : Théorème de Cayley-Hamilton.** Soit f un endomorphisme de $\mathbb{R}^3$ ayant trois valeurs propres distinctes. On sait que les valeurs propres de f sont toutes des racines de son polynôme minimal, le polynôme minimal de f a donc 3 racines distinctes, il est au moins de degré 3. Par le thèorème de Cayley-Hamilton, le polynôme minimal de f divise le polynôme caractéristique de f, ce dernier étant de degré 3 également (et unitaire comme le polynôme minimal), les polynômes minimaux et caractéristiques de f sont égaux, ce qui montre que f est cyclique.

2eme preuve : Preuve directe. Dans le doute (je ne suis pas sur que cet argument soit acceptable dans la mesure ou je ne sais pas s'il faisait partie du cours), montrons directement que f est cyclique, d'après la définition donnée à la question 12. Soient α, β, γ les trois valeurs propres de f, et x, y, z des vecteurs propres respectifs pour ces valeurs propres, on pose $u = x + y + z$, et on a

$$f(u) = \alpha x + \beta y + \gamma z, f^2(u) = \alpha^2 x + \beta^2 y + \gamma^2 z$$

On sait que x, y, z forme une base de $\mathbb{R}^3$ (base de diagonalisation pour f), la matrice de passage de la base x, y, z vers la famille $u, f(u), f^2(u)$ est donnée par

$$\begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix}$$

on reconnait une matrice de Vandermonde, dont le déterminant est non nul car α, β, γ sont distincts deux à deux. La famille $(u, f(u), f^2(u))$ est donc une base de $\mathbb{R}^3$ et f est cyclique.