Devoir à la maison n°10

- Le devoir devra être rédigé sur des copies *doubles*.
- Les copies ne devront comporter ni rature, ni renvoi, ni trace d'effaceur.
- Toute copie ne satisfaisant pas à ces exigences devra être intégralement récrite.

Problème 1

$\boxed{1}$ En développant par rapport à la première ligne, $\det(\mathrm{C_P}) = (-1)^n a_0 = (-1)^n \mathrm{P}(0)$. Ainsi $\mathrm{C_P}$ est inversible si et seulement si $\mathrm{P}(0) \neq 0$.

$\boxed{2}$ Tout d'abord,

$$\chi_{\mathrm{C_P}}(\mathrm{X}) = \begin{vmatrix} \mathrm{X} & \cdots & \cdots & 0 & a_0 \\ -1 & \ddots & & \vdots & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{n-2} \\ 0 & \cdots & 0 & -1 & \mathrm{X}+a_{n-1} \end{vmatrix}$$

Première méthode. En numérotant $\mathrm{L}_0, \dots, \mathrm{L}_{n-1}$ les lignes de ce déterminant et en effectuant l'opération $\mathrm{L}_0 \leftarrow \sum_{k=0}^{n-1} \mathrm{X}^k \mathrm{L}_k$, on obtient

$$\chi_{\mathrm{C_P}}(\mathrm{X}) = \begin{vmatrix} 0 & \cdots & \cdots & 0 & \mathrm{P}(\mathrm{X}) \\ -1 & \ddots & & \vdots & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{n-2} \\ 0 & \cdots & 0 & -1 & \mathrm{X}+a_{n-1} \end{vmatrix}$$

En développant par rapport à la première ligne, on obtient $\chi_{\mathrm{A}}(\mathrm{X}) = \mathrm{P}(\mathrm{X})$.
Deuxième méthode. En développant par le déterminant définissant $\chi_{\mathrm{C_P}}(\mathrm{X})$ par rapport à sa dernière colonne, on obtient

$$\chi_{\mathrm{C_P}}(\mathrm{X}) = \sum_{k=0}^{n-2} (-1)^{n+k+1} a_k \mathrm{D}_k(\mathrm{X}) + (\mathrm{X}+a_{n-1}) \det(\mathrm{XI}_{n-1})$$

avec

$$\mathrm{D}_k(\mathrm{X}) = \left|\begin{array}{ccccc|ccccc} \mathrm{X} & 0 & 0 & \cdots & 0 & & & & & \\ -1 & \mathrm{X} & 0 & \ddots & \vdots & & & & & \\ 0 & -1 & \ddots & \ddots & 0 & & & (\mathbf{0}) & & \\ \vdots & \ddots & \ddots & \ddots & 0 & & & & & \\ 0 & \cdots & 0 & -1 & \mathrm{X} & & & & & \\ \hline & & & & & -1 & \mathrm{X} & 0 & \cdots & 0 \\ & & & & & 0 & -1 & \mathrm{X} & \ddots & \vdots \\ & & (\mathbf{0}) & & & 0 & 0 & \ddots & \ddots & 0 \\ & & & & & \vdots & \ddots & \ddots & \ddots & \mathrm{X} \\ & & & & & 0 & \cdots & 0 & 0 & -1 \end{array}\right|$$

où le bloc supérieur gauche est de taille k et le bloc inférieur droit est de taille $n-1-k$. Comme il s'agit d'un déterminant diagonal par blocs, on obtient $\mathrm{D}_k(\mathrm{X}) = (-1)^{n-1-k}\mathrm{X}^k$ puis

$$\chi_{\mathrm{C_P}}(\mathrm{X}) = \sum_{k=0}^{n-1} a_k \mathrm{X}^k + \mathrm{X}^{n-1}(\mathrm{X}+a_{n-1}) = \mathrm{X}^n + \sum_{k=0}^{n-1} a_k \mathrm{X}^k = \mathrm{P}(\mathrm{X})$$

$\boxed{3}$ S'il existe $A \in \mathcal{M}_n(\mathbb{K})$ telle que $Q = \chi_A$, alors A est unitaire de degré n. Réciproquement, si Q est unitaire de degré n, alors $Q = \chi_{C_Q}$ d'après la question précédente.
Finalement, il existe $A \in \mathcal{M}_n(\mathbb{K})$ telle que $Q = \chi_A$ si et seulement si Q est unitaire de degré n.

$\boxed{4}$ **4.a** De manière générale, si $A \in \mathcal{M}_n(\mathbb{K})$,

$$\chi_A = \det(XI_n - A) = \det((XI_n - A)^\top) = \det(XI_n - A^\top) = \chi_{A^\top}$$

Comme le spectre d'une matrice est l'ensemble des racines du polynôme caractéristique, $\mathrm{Sp}(A) = \mathrm{Sp}(A^\top)$.

4.b Soit $X = \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} \in E_\lambda(C_P^\top)$. On a alors

$$\forall k \in [\![0, n-2]\!],\ x_{k+1} = \lambda x_k$$

puis

$$\forall k \in [\![0, n-1]\!],\ x_k = \lambda^k x_0$$

Ainsi, en posant $X_\lambda = \begin{pmatrix} 1 \\ \lambda \\ \vdots \\ \lambda^{n-1} \end{pmatrix}$,

$$E_\lambda(C_P^\top) \subset \mathrm{vect}(X_\lambda)$$

Notamment $\dim E_\lambda(C_P^\top) \leq 1$. Mais un sous-espace propre n'est pas nul donc $\dim E_\lambda(C_P^\top) \geq 1$. Finalement,

$$\dim E_\lambda(C_P^\top) = 1 = \dim \mathrm{vect}(X_\lambda)$$

L'inclusion précédente garantit alors que $E_\lambda(C_P^\top) = \mathrm{vect}(X_\lambda)$.

4.c Supposons P simplement scindé sur $\mathbb{K}$. Puisque $\chi_{C_P^\top} = \chi_{C_P} = P$, $C_P^\top$ est diagonalisable.

Réciproquement, supposons $C_P^\top$ diagonalisable. Alors $\chi_{C^\top} = P$ est sindé sur $\mathbb{K}$. La question précédente montre que tous les sous-espaces propres de $C_P^\top$ sont de dimension 1. Comme $C_P^\top$ est diagonalisable, les multilplicités des valeurs propres dans le polynôme caractéristique sont égales aux dimensions des sous-espaces propres associés. Ainsi toutes les racines de P sont simples. P est bien simplement scindé sur $\mathbb{K}$.

4.d P est alors scindé à racines simples. D'après la question **4.c**, $C_P^\top$ est diagonalisable. Avec les notations de la question **4.b**, $(X_{\lambda_1}, \dots, X_{\lambda_n})$ est une base de $\mathbb{C}^n$ formée de vecteurs propres de $C_P^\top$. Ces vecteurs sont les colonnes du déterminant de Vandermonde de l'énoncé, qui est donc non nul.

Remarque. La notion de déterminant de Vandermonde figure dans le programme de MPSI. On sait que le déterminant de l'énoncé vaut $\prod_{1 \leq i < j \leq n} (\lambda_j - \lambda_i)$. Ce déterminant est clairement non nul si et seulement si les λ_i sont deux à deux distincts. Mais il s'agit de retrouver ce résultat dans cette question.

$\boxed{5}$ **5.a** On pose $P = X^{2002} - X^{2001} - X^{2000} - 1999$. Ce polynôme P est bien unitaire et on peut lui associer sa matrice compagnon $A = C_P \in \mathcal{M}_{2002}(\mathbb{R})$. Alors $\chi_A = P$ et le théorème de Cayley-Hamilton permet de conclure que $P(A) = 0$ i.e. $A^{2002} = A^{2001} + A^{2000} + 1999I_{2002}$.

5.b Comme $f^{n-1} \neq 0$, $\mathrm{Ker} f^{n-1} \subsetneq E$. Soit alors $x \in E \setminus \mathrm{Ker} f^{n-1}$. On vérifie que $\mathcal{B} = (x, f(x), \dots, f^{n-1}(x))$ est bien une base de E. Comme $\dim E = n$, il suffit de vérifier que cette famille est libre. Soit alors $(\lambda_0, \dots, \lambda_{n-1}) \in \mathbb{K}^n$ tel que $\sum_{k=0}^{n-1} \lambda_k f^k(x) = 0_E$. En appliquant successivement f^{n-1}, f^{n-2}, etc... à cette égalité, on trouve $\lambda_{n-1} = \lambda_{n-2} = \dots = \lambda_0 = 0$. La famille $\mathcal{B}$ est bien libre et c'est donc une base de E. La matrice de f dans cette base est alors bien une matrice compagnon. Plus précisément, c'est la matrice $C_{X^n} = \left(\begin{array}{c|c} 0 & 0 \\ \hline I_{n-1} & 0 \end{array}\right)$.

$\boxed{6}$ Soit $i \in [\![1, n]\!]$. Alors $(AX)_i = \lambda X_i$ i.e.

$$\lambda x_i = \sum_{j=1}^n a_{i,j} x_j$$

Par inégalité triangulaire

$$|\lambda x_i| \leq \sum_{j=1}^n |a_{i,j}||x_j| \leq \sum_{j=1}^n |a_{i,j}| \|X\|_\infty = r_i \|X\|_\infty$$

7 On reprend les notations de la question précédente. Il existe alors $i_0 \in [\![1,n]\!]$ tel que $|x_{i_0}| = \|X\|_\infty$. Ainsi $|\lambda|\|X\|_\infty \leq r_{i_0}\|X\|_\infty$. Comme X est un vecteur propre, $X \neq 0$ puis $\|X\|_\infty > 0$. On en déduit que $|\lambda| \leq r_{i_0}$. Ainsi $\lambda \in D_{i_0} \subset \bigcup_{i=1}^{n} D_i$.
Par conséquent, $\mathrm{Sp}(A) \subset \bigcup_{i=1}^{n} D_i$.

8 L'ensemble des racines de P est le spectre de C_P. Avec les notations des questions précédentes, $r_1 = |a_0|$ et $r_i = 1 + |a_i|$ pour $i \in [\![2,n]\!]$. Ainsi $D_i \subset D(0,R)$ pour tout $i \in [\![1,n]\!]$. D'après la question précédente, $\mathrm{Sp}(C_P) \subset D(0,R)$. Les racines de P sont donc toutes dans le disque $D(0,R)$.

9 On cherche les racines du polynôme $P = X^a + X^b - X^c - X^d$ dans $\mathbb{N} \setminus \{0,1\}$. Comme les entiers a, b, c, d sont distincts et non nuls, on a $R = 2$ avec les notations de la question précédente. Ainsi la seule racine éventuelle de P dans $\mathbb{N} \setminus \{0,1\}$ est 2 d'après la question précédente.
Supposons que 2 soit racine de P. Sans perte de généralité, on peut supposer $a < \min(b,c,d)$. Puisque $2^a + 2^b = 2^c + 2^d$ i.e. $1 + 2^{b-a} = 2^{c-a} + 2^{d-a}$. Comme $b-a$, $c-a$ et $d-a$ sont des entiers strictement positifs, 2 divise 2^{b-a}, 2^{c-a} et 2^{d-a}. On en déduit que 2 divise 1 ce qui est absurde.
Finalement, l'équation $n^a + n^b = n^c + n^d$ n'admet pas de solution dans $\mathbb{N} \setminus \{0,1\}$.

10 Soit λ une racine de P. Alors

$$\lambda^p + \sum_{k=0}^{p-1} a_k\lambda^k = 0$$

puis pour tout $n \in \mathbb{N}$,

$$\lambda^{n+p} + \sum_{k=0}^{p-1} a_k\lambda^{n+k} = 0$$

ce qui signifie que $n \mapsto \lambda^n$ appartient à F.

11 L'application φ est clairement linéaire. Comme une suite de F est uniquement déterminée par ses p premiers termes, φ est bijective. Autrement dit φ est un isomorphisme de F sur $\mathbb{C}^p$ et $\dim F = \dim \mathbb{C}^p = p$.

12 **12.a** Soit $i \in [\![0, p-1]\!]$. Alors

$$e_i(p) = -\sum_{k=0}^{p-1} a_k e_i(k) = -a_i$$

12.b Soit $(\lambda_0, \dots, \lambda_{p-1}) \in \mathbb{C}^p$ tel que $\sum_{k=0}^{p-1} \lambda_k e_k = 0$. En évaluant cette égalité en $i \in [\![0, n-1]\!]$, on obtient $\lambda_i = 0$. On en déduit que la famille $(e_0, \dots, e_{p-1})$ est libre. Comme $\dim F = p$, cette famille est une base de F.
Remarque. On aurait aussi pu remarquer que $(e_0, \dots, e_{p-1})$ est l'image de la base canonique de $\mathbb{C}^p$ par l'isomorphisme φ^{-1}.

12.c Posons $v = \sum_{i=0}^{p-1} u(i)e_i$. Alors $\varphi(u) = \varphi(v) = (u(0), \dots, u(p-1))$. Comme φ est injective, $u = v$.

13 f est clairement linéaire donc f est un endomorphisme de E. Soit $u \in F$. Alors

$$\forall n \in \mathbb{N},\ u(n+p) = \sum_{k=0}^{p-1} a_k u(n+k)$$

Par conséquent

$$\forall n \in \mathbb{N},\ u(n+1+p) = \sum_{k=0}^{p-1} a_k u(n+1+k)$$

ou encore

$$\forall n \in \mathbb{N},\ f(u)(n+p) = \sum_{k=0}^{p-1} a_k f(u)(n+k)$$

donc $f(u) \in F$. Ainsi F est stable par f.

14 Soit $j \in [\![0, n-1]\!]$. Alors

$$\begin{aligned}
g(e_j) &= \sum_{i=0}^{p-1} g(e_j)(i)e_i \quad \text{d'après la question } \mathbf{12.c}\\
&= \sum_{i=0}^{p-1} e_j(i+1)e_i\\
&= e_j(p)e_p + \sum_{i=1}^{p-1} \delta_{i+1,j}e_i\\
&= -a_je_p + \sum_{i=1}^{p-1} \delta_{i,j-1}e_i \qquad \text{d'après la question } \mathbf{12.a}\\
&= \begin{cases} -a_0e_p & \text{si } j = 0\\ -a_je_p + e_{j-1} & \text{sinon}\end{cases}
\end{aligned}$$

Ceci signifie que la matrice de g dans la base $(e_0, \dots, e_{p-1})$ est $\mathrm{C}_\mathrm{P}^\mathsf{T}$.

15 **15.a** Pour tout $k \in [\![0, p-1]\!]$, $u_k : n \mapsto \lambda_k^n$ est un vecteur de F d'après la question **10**. De plus, u_k est clairement un vecteur propre de g pour la valeur propre λ_k. Les vecteurs $u_0, \dots, u_{p-1}$ étant associés à des valeurs propres distinctes, la famille $(u_0, \dots, u_{p-1})$ est libre. Comme $\dim \mathrm{F} = p$, cette famille est une base de F.

15.b Il suffit de décomposer u dans la base $(u_0, \dots, u_{p-1})$.

16 Avec les notations des questions précédentes,

$$\mathrm{P} = \mathrm{X}^2 - (a+b+c)\mathrm{X}^2 + (ab+ac+bc)\mathrm{X} - abc = (\mathrm{X}-a)(\mathrm{X}-b)(\mathrm{X}-c)$$

Ainsi P admet trois racines réelles distinctes, à savoir a, b et c. D'après la question **15**, les suites (a^n), (b^n) et (c^n) forment une base de l'espace vectoriel de l'énoncé.

17 Si A est la matrice nulle, alors $\chi_\mathrm{A} = \mathrm{X}^n$ et $\mathrm{C}_\mathrm{A} = \left(\begin{array}{c|c} 0 & 0 \\ \hline \mathrm{I}_{n-1} & 0 \end{array}\right) \neq 0$. A n'est alors évidemment pas semblable à C_A (dès que $n \geq 2$).

18 Soit $(\mathrm{U}, \mathrm{V}) \in \mathrm{GL}_n(\mathbb{K})^2$ vérifiant (*) et $\mathrm{U} \neq \mathrm{V}$. Alors $\mathrm{U}-\mathrm{V} = \mathrm{P}^{-1}(\mathrm{C}_\mathrm{U} - \mathrm{C}_\mathrm{V})\mathrm{P}$. Seule la dernière colonne de $\mathrm{C}_\mathrm{U} - \mathrm{C}_\mathrm{V}$ est potentiellement non nulle donc $\mathrm{rg}(\mathrm{U}-\mathrm{V}) = \mathrm{rg}(\mathrm{C}_\mathrm{U} - \mathrm{C}_v) \leq 1$. De plus, $\mathrm{U} \neq \mathrm{V}$ donc $\mathrm{rg}(\mathrm{U}-\mathrm{V}) \geq 1$. Finalement, $\mathrm{rg}(\mathrm{U}-\mathrm{V}) = 1$.

19 Posons par exemple $\mathrm{U} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\mathrm{V} = \begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix}$. Alors $\mathrm{U} - \mathrm{V} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ de sorte que $\mathrm{rg}(\mathrm{U}-\mathrm{V}) = 1$ mais $\mathrm{C}_\mathrm{U} = \mathrm{C}_\mathrm{V} = \mathrm{C}_{(\mathrm{X}-1)^2}$ donc (**) n'est pas vérifiée. Comme $\chi_\mathrm{U} = \chi_\mathrm{V} = (\mathrm{X}-1)^2$, $\chi_\mathrm{U} \wedge \chi_\mathrm{V} = (\mathrm{X}-1)^2$.

20 Tout d'abord, $\mathrm{rg}(u-v) = \mathrm{rg}(\mathrm{U}-\mathrm{V}) = 1$. D'après le théorème du rang, $\dim \mathrm{H} + \mathrm{rg}(u-v) = \dim \mathrm{E}$ donc $\dim \mathrm{H} = n-1$ et H est bien un hyperplan vectoriel de E.

21 **21.a** Supposons que F soit inclus dans H. Alors $u_\mathrm{F} = v_\mathrm{F}$ donc $\chi_{v_\mathrm{F}} = \chi_{v_\mathrm{F}}$ divise χ_u et χ_v. Ceci contredit le fait que χ_u et χ_v sont premiers entre eux puisque $\deg \chi_{u_\mathrm{F}} = \deg \chi_{v_\mathrm{F}} = \dim \mathrm{F} \geq 1$.

21.b Comme $\mathrm{H} \subset \mathrm{F} + \mathrm{H} \subset \mathrm{E}$, $n-1 \leq \dim(\mathrm{F}+\mathrm{H}) \leq n$. Supposons $\dim(\mathrm{F}+\mathrm{H}) = n-1 = \dim \mathrm{H}$. Alors $\mathrm{H} = \mathrm{F} + \mathrm{H}$ d'après l'inclusion précédente puis $\mathrm{F} \subset \mathrm{F} + \mathrm{H} = \mathrm{H}$, ce qui est contradictoire. Finalement, $\dim(\mathrm{F}+\mathrm{H}) = n$ i.e. $\mathrm{F}+\mathrm{H} = \mathrm{E}$. Donnons-nous des bases $\mathrm{B}_\mathrm{F} = (f_1, \dots, f_p)$ de F et $(h_1, \dots, h_{n-1})$ de H. Comme $\mathrm{F}+\mathrm{H} = \mathrm{E}$, la famille $(f_1, \dots, f_p, h_1, \dots, h_{n-1})$ engendre E. Comme $(f_1, \dots, f_p)$ est une famille libre de vecteurs de E, un théorème du cours garantit qu'on peut compléter la famille B_F en une base B' de E à l'aide de certains des vecteurs h_i.

u et v coïncident sur H et F est stable par u et v donc les matrices de u et v dans la base B' sont de la forme $\left(\begin{array}{c|c} \mathrm{A} & \mathrm{C} \\ \hline 0 & \mathrm{D} \end{array}\right)$ et $\left(\begin{array}{c|c} \mathrm{B} & \mathrm{C} \\ \hline 0 & \mathrm{D} \end{array}\right)$ avec A et D des matrices carrées. On en déduit que $\chi_u = \chi_\mathrm{A}\chi_\mathrm{D}$ et $\chi_v = \chi_\mathrm{B}\chi_\mathrm{D}$. Comme $\mathrm{F} \neq \mathrm{E}$, $\deg \chi_\mathrm{D} \geq 1$, et χ_D divise χ_u et χ_v, ce qui contredit le fait que $\chi_u \wedge \chi_v = 1$.

21.c Ce qui précède montre que les seuls sous-espaces vectoriels de E stables à la fois par u et v sont $\{0\}$ et E.

22 **22.a** Soit $j \in \mathbb{N}$. Comme u est un automorphisme de E, on peut écrire $\mathrm{G}_j = u^{-j}(\mathrm{H})$. Comme u^{-j} est également un automorphisme, $\dim \mathrm{G}_j = \dim \mathrm{H}$ donc G_j est un hyperplan de E.

22.b $\bigcap_{j=0}^{n-2} G_j$ est l'intersection de $n-1$ hyperplans de E donc, d'après le cours, $\dim\left(\bigcap_{j=0}^{n-2} G_j\right) \geq n-(n-1) = 1$. Notamment, $\bigcap_{j=0}^{n-2} G_j \neq \{0\}$.

22.c On procède comme indiqué dans l'énoncé. Par définition de p, $(y, u(y), \dots, u^{p-1}(y))$ est libre mais $(y, u(y), \dots, u^p(y))$ ne l'est pas. Ceci signifie que $u^p(y) \in \text{vect}(y, u(y), \dots, u^{p-1}(y)) = F$. On en déduit alors que F est stable par u.
Supposons $p \leq n-1$. Alors $p-1 \geq\leq n-2$ de sorte que pour tout $j \in [\![0, p-1]\!]$, $y \in G_j$ i.e. $u^j(y) \in H$. Ainsi $F \subset H$. Comme u et v coïncident sur H, ils coïncident également sur F. Comme F est stable par u, il l'est également par v. Ainsi F est un sous-espace stable par u et v. On en déduit que $F = \{0\}$ ou $F = E$ d'après la question **21.c**. Mais y est un vecteur non nul de F donc $F = E$. Puis $p = \dim F = \dim E = n$, ce qui contredit notre supposition. Ainsi $p \geq n$. Mais comme $(y, u(y) \dots, u^{p-1}(y))$ est une famille libre de vecteurs de E, $p \leq \dim E = n$. Ainsi $p = n$. La famille $(y, u(y), \dots, u^{n-1}(y))$ est donc une famille libre de n vecteurs de E : c'est une base de E.

22.d Puisque $u(e_j) = e_{j+1}$ pour tout $j \in [\![0, n-2]\!]$, la matrice de u dans la base $\mathcal{B}''$ est une matrice compagon C_P pour un certain polynôme P. Mais alors $\chi_U = \chi_u = \chi_{C_P} = P$ donc $C_P = C_U$.
Pour tout $j \in [\![0, n-2]\!]$, $e_j \in H$ par définition de y. Comme u et v coïncident sur H, on a $v(e_j) = u(e_j) = e_{j+1}$ et le même raisonnement que précédemment montre que la matrice de v dans la base $\mathcal{B}''$ est C_V.

22.e C_U et C_V sont les matrices des endomorphismes u et v dans la *même* base $\mathcal{B}''$. En notant P la matrice de passage de la base $\mathcal{B}''$ vars la base $\mathcal{B}$. On a donc $U = P^{-1}C_UP$ et $V = P^{-1}C_VP$. Ainsi U et V vérifient (**).

$\boxed{23}$ **23.a** Puisque $\frac{1}{2}(X^n+1) - \frac{1}{2}(X^n-1) = 1$, $(X^n+1) \wedge (X^n-1) = 1$. D'après ce qui précède, il existe une base $(e_1, \dots, e_n)$ de E telle que les matrices de u et v dans cette base sont respectivement C_{X^n+1} et C_{X^n-1}. Ceci implique que $u(e_i) = v(e_i) = e_{i+1}$ pour tout $i \in [\![1, n-1]\!]$ et $v(e_n) = -u(e_n) = 1$.

23.b Remarquons que $u(X) = X$ et $v(X) = X$. On en déduit que $w(X) = X$ pour tout $w \in G$. Comme w est un automorphisme, w induit une bijection σ_w de X i.e. une permutation de X. Notons S_X l'ensemble des permutations de X. L'application $\left\{\begin{array}{ccc} G & \longrightarrow & S_X \\ w & \longmapsto & \sigma_w \end{array}\right.$ est injective, car si deux endomorphismes de E coïncident sur X, ils coïncident à fortiori sur la base $(e_1, \dots, e_n)$ de E et sont égaux. On en déduit que $\operatorname{card} G \leq \operatorname{card} S_X = (2n)!$.