C.C.P., MP, 2001, Mathématiques II

(7 pages)

Erreur d'énoncé: n doit être non nul (et $n \geqslant 2$ aurait été préférable pour la partie IV).

Partie I

1. Par développement par rapport à la première ligne, on obtient $\det C_P = (-1)^{n+1}(-a_0) = (-1)^n a_0 = (-1)^n P(0)$. Donc $\underline{C_P \text{ est inversible si et seulement si } P(0) \neq 0}$.

2. En développant par rapport à la dernière colonne, on obtient :

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

$$= (-X - a_{n-1}) \begin{vmatrix} -X & 0 & \cdots & 0 \\ 1 & -X & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 1 & -X \end{vmatrix} + \cdots + (-1)^{n+k+1}(-a_k) \left| \begin{array}{cccc|ccc} -X & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 1 & -X & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \cdots & 1 & -X & 0 & \cdots & 0 \\ \hline 0 & \cdots & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & & & \vdots & 0 & \ddots & \vdots \\ \vdots & & & \vdots & \vdots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \end{array} \right| \begin{matrix} \\ \\ \\ \\ \updownarrow k \\ \\ \\ \\ \updownarrow n-1-k \end{matrix}$$

$$+ \cdots + (-1)^{n+1}(-a_0) \begin{vmatrix} 1 & -X & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & -X \\ 0 & \cdots & 0 & 1 \end{vmatrix}$$

$$= (-X - a_{n-1})(-X)^{n-1} + \cdots + (-1)^{n+k+1}(-a_k)(-X)^k + \cdots + (-1)^{n+1}(-a_0)$$

$$= (-1)^n \left[X^n + a_{n-1}X^{n-1} + \cdots + a_k X^k + \cdots + a_0 \right]$$

soit $\underline{\chi_{C_P} = (-1)^n P}$.

3. Si $Q = \chi_A$ alors $\deg Q = n$ et son coefficient dominant est $(-1)^n$. Réciproquement, si $\deg Q = n$ et son coefficient dominant est $(-1)^n$, posons $P = (-1)^n Q$: on a alors $Q = \chi_{C_P}$ d'après [**4**].

$\underline{\text{Il existe } A \in \mathcal{M}_n(\mathbb{K}) \text{ telle que } Q = \chi_A \text{ si et seulement si } Q \text{ a pour terme de plus haut degré } (-1)^n X^n}$.

4. **a.** $\chi_{{}^tC_P} = \chi_{C_P}$ donne $\underline{\mathrm{Sp}({}^tC_P) = \mathrm{Sp}(C_P)}$.

b. $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathrm{Ker}\big({}^tC_P - \lambda I_n\big) \iff \begin{pmatrix} 0 & 1 & & 0 \\ \vdots & \ddots & \ddots & \\ 0 & \cdots & 0 & 1 \\ -a_0 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \lambda \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$

$$\iff \begin{cases} \lambda x_1 = x_2 \\ \lambda x_2 = x_3 \\ \vdots \\ \lambda x_{n-1} = x_n \\ \lambda x_n = -a_0 x_1 - \cdots - a_{n-2} x_{n-1} - a_{n-1} x_n \end{cases}$$

$$\iff \begin{cases} x_2 = \lambda x_1 \\ x_3 = \lambda^2 x_1 \\ \vdots \\ x_n = \lambda^{n-1} x_1 \\ 0 = P(\lambda)\, x_1 \end{cases}$$

et on a $P(\lambda) = 0$ donc $\mathrm{Ker}\big({}^tC_P - \lambda I_n\big) = \mathbb{K}. \begin{pmatrix} 1 \\ \lambda \\ \vdots \\ \lambda^{n-1} \end{pmatrix}$.

c. Si P est scindé à racines simples alors $\chi_{{}^tC_P}$ aussi et donc ${}^tC_P$ est diagonalisable.
Réciproquement, si ${}^tC_P$ est diagonalisable alors $\chi_{{}^tC_P}$ est scindé donc P aussi et, pour tout λ racine de P, on a $\lambda \in \mathrm{Sp}\big({}^tC_P\big)$ et la multiplicité de λ est égale à $\dim\Big(\mathrm{Ker}\big({}^tC_P - \lambda I_n\big)\Big)$. Or, on a vu au [**b**] que $\dim\Big(\mathrm{Ker}\big({}^tC_P - \lambda I_n\big)\Big) = 1$. Donc P est scindé à racines simples.
Ainsi ${}^tC_P$ est diagonalisable si et seulement si P est scindé à racines simples.

d. $\diamond$ Puisque $\deg P = n$, si P a n racines deux à deux distinctes alors P est scindé à racines simples et donc [**c**] donne ${}^tC_P$ est diagonalisable.

$\diamond$ La famille $\left(\begin{pmatrix} 1 \\ \lambda_1 \\ \vdots \\ \lambda_1^{n-1} \end{pmatrix}, \ldots, \begin{pmatrix} 1 \\ \lambda_n \\ \vdots \\ \lambda_n^{n-1} \end{pmatrix}\right)$ est formée de vecteurs propres associés à des valeurs propres distinctes. Elle est donc libre et donc on a bien : $\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ \vdots & \vdots & & \vdots \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \cdots & \lambda_n^{n-1} \end{vmatrix} \neq 0$

5. **a.** Prenons $n = 2002, \quad P = X^{2002} - X^{2001} - X^{2000} - 1999 \quad$ et $\quad A = C_P$.
On a $\chi_A = P$ et le théorème de Cayley-Hamilton donne $P(A) = O$.

REMARQUE: Comme $P(0) = 0$ et $P(t) \xrightarrow[t \to +\infty]{} +\infty$, P a au moins une racine α dans $\mathbb{R}$ donc dans $\mathbb{K}$ et, pour tout n, la matrice $A = \alpha\, I_n$ vérifie l'équation.

b. Puisque $f^{n-1} \neq 0$, on a $\mathrm{Ker}\, f^{n-1} \neq E$ et on peut fixer $e \in E \setminus \mathrm{Ker}\, f^{n-1}$ puis poser, pour $k \in [\![1, n]\!]$, $e_k = f^{k-1}(e)$. Montrons que $(e_1, \ldots, e_n)$ est une base de E : si il existe $(\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n$ et $(\lambda_1, \ldots, \lambda_n) \neq$

$(0,\dots,0)$ tel que $\sum_{k=1}^{n}\lambda_k e_k=\vec{0}$, posons $r=\text{Min}\{k\mid\lambda_k\neq 0\}$; on a alors

$$\vec{0}=f^{n-r}\left(\sum_{k=1}^{n}\lambda_k e_k\right)=f^{n-r}\left(\sum_{k=r}^{n}\lambda_k e_k\right)=\sum_{k=r}^{n}\lambda_k f^{n-r+k-1}(e)$$
$$=\lambda_r f^{n-1}(e)+f^n\left(\sum_{k=r+1}^{n}\lambda_k f^{k-r}(e)\right)=\lambda_r f^{n-1}(e)$$

donc, puisque $f^{n-1}(e)\neq\vec{0}$, $\lambda_r=0$ ce qui contredit la définition de r. Donc $(e_1,\dots,e_n)$ est une famille libre de E donc une base de E et, pour $k\in[\![1,n-1]\!]$, $f(e_k)=f^k(e)=e_{k+1}$ et $f(e_n)=f^n(e)=\vec{0}$.

Donc il existe une base $\mathcal{B}$ de E telle que $\text{Mat}\,(f,\mathcal{B})=\begin{pmatrix}0&&&0\\1&0&&0\\&\ddots&\ddots&\vdots\\&&1&0\end{pmatrix}=C_{X^n}$.

Partie II

6. On a $\lambda X=AX$ donc $\forall i\in[\![1,n]\!]$, $\lambda x_i=\sum_{k=1}^{n}a_{ik}x_k$ donc $|\lambda x_i|=\left|\sum_{k=1}^{n}a_{ik}x_k\right|\leqslant\sum_{k=1}^{n}|a_{ik}|\,|x_k|\leqslant\sum_{k=1}^{n}|a_{ik}|\,\|X\|_\infty$ donc $\forall i\in[\![1,n]\!],\quad|\lambda x_i|\leqslant r_i\,\|X\|_\infty$.

7. Appliquons le résultat de [**6**] à i_0 tel que $|x_{i_0}|=\|X\|_\infty$, on obtient $|\lambda|\,\|X\|_\infty\leqslant r_{i_0}\,\|X\|_\infty$ donc, puisque $X\neq\vec{0}$, $|\lambda|\leqslant r_{i_0}$ donc $\lambda\in D_{i_0}$.

Ainsi $\forall\lambda\in\text{Sp}(A),\ \exists\, i_0\in[\![1,n]\!],\quad\lambda\in D_{i_0}$ donc $\text{Sp}(A)\subset\bigcup_{k=1}^{n}D_k$.

8. On a vu au [**2**] que les racines de P sont les valeurs propres de C_P et on peut appliquer [**7**] à $A=C_p$ avec $r_1=|a_0|$ et pour $i\in[\![2,n]\!]$, $r_i=1+|a_{i-1}|$. Or, $\bigcup_{k=1}^{n}D_k$ est le disque fermé de centre 0 et de rayon $\underset{1\leqslant i\leqslant n}{\text{Max}}\,r_i$ donc toutes les racines de P appartiennent à $B_f(0,R)$ où $R=\text{Max}\Big\{|a_0|,1+|a_1|,\dots,1+|a_{n-1}|\Big\}$.

9. Pour fixer les idées, supposons que $a=\text{Max}\{a,b,c,d\}$. Si $n\in\mathbb{N}$ est solution de l'équation proposée, il est racine de $P=X^a+x^b-X^c-X^d\in\mathbb{C}_a[X]$ donc, avec les notations de [**8**], on a $|n|\leqslant R$ avec $R=2$ car $|a_0|=0$ et $1+|a_k|=\begin{cases}2&\text{si } k\in\{b,c,d\}\\1&\text{sinon}\end{cases}$. Mais, si 2 était solution, on aurait, en supposant, par exemple, $c>d$, $2^b\left(2^{a-b}+1\right)=2^d\left(2^{c-d}+1\right)$ donc, par unicité de la décomposition en produit de nombres premiers, $b=d$ ce qui est exclu. 0 et 1 étant clairement solutions, on peut conclure que : les seules solutions $n\in\mathbb{N}$ de $n^a+n^b=n^c+n^d$ sont 0 et 1 .

REMARQUE: Plus simplement, si $n\neq 0$ est solution de l'équation, en notant $m=\text{Min}\{a,b,c,d\}$, on a $n^{a-m}+n^{b-m}=n^{c-m}+n^{d-m}$ donc, modulo n, $1\equiv 0$ ce qui donne $n=1$.

Partie III

10. Si $\forall n,\ u(n)=\lambda^n$ alors $\forall n,\ u(n+p)+a_{p-1}u(n+p-1)+\cdots+a_0u(n)=\lambda^n\left(\lambda^p+a_{p-1}\lambda^{p-1}+\cdots+a_0\right)=\lambda^n P(\lambda)$. Donc la suite $n\mapsto\lambda^n$ appartient à F si et seulement si λ est racine de P .

11. $\diamond$ φ est clairement linéaire et soit $\alpha=\left(\alpha_0,\dots,\alpha_{p-1}\right)\in\mathbb{C}^p$, il existe une et une seule suite $u\in F$ telle que $\varphi(u)=\alpha$: c'est la suite définie par $u(0)=\alpha_0,\dots u(p-1)=\alpha_{p-1}$ et, pour $n\geqslant p$, $u(n)=-a_{p-1}u(n-1)-\cdots-a_0u(n-p)$. Donc φ est bijective et donc φ est un isomorphisme de F sur $\mathbb{C}^p$.
$\diamond$ On a donc $\dim F=\dim\mathbb{C}^p$ soit $\dim F=p$.

12. **a.** $e_i(p)=-a_{p-1}e_i(p-1)-\cdots-a_ie_i(i)-\cdots-a_0e_i(0)$ donc $e_i(p)=-a_i$.

b. Notons $\left(\varepsilon_1,\dots,\varepsilon_p\right)$ la base canonique de $\mathbb{C}^p$. On a $e_i=\varphi^{-1}\left(\varepsilon_{i+1}\right)$ donc la famille $\left(e_0,\dots,e_{p-1}\right)$ est l'image par l'isomorphisme φ^{-1} de la base $\left(\varepsilon_1,\dots,\varepsilon_p\right)$. Ainsi $\left(e_0,\dots,e_{p-1}\right)$ est une base de F .

c. $\forall u\in F,\ u=\varphi^{-1}\left[\varphi(u)\right]=\varphi^{-1}\left[\sum_{i=0}^{p-1}u(i)\,\varepsilon_{i+1}\right]=\sum_{i=0}^{p-1}u(i)\,\varphi^{-1}\left(\varepsilon_{i+1}\right)$ donc $\forall u\in F,\ u=\sum_{i=0}^{p-1}u(i)\,e_i$.

13. $f\in\mathcal{L}(E)$ est évident et si $u\in F$, $\forall n,\ u(n+1+p)=-a_{p-1}u(n+1+p-1)-\cdots-a_0u(n+1)$ soit $f(u)(n+p)=-a_{p-1}f(u)(n+p-1)-\cdots-a_0f(u)(n)$ donc $f(u)\in F$ ce qui montre que F est stable par f .

14. Pour $u\in F$, $f(u)\in F$ donc [**13.c**] donne $f(u)=\sum_{k=0}^{p-1}f(u)(k)\,e_k=\sum_{k=0}^{p-1}u(k+1)\,e_k=\sum_{k=0}^{p-2}u(k+1)\,e_k+u(p)\,e_{p-1}=u(1)\,e_0+\sum_{k=1}^{p-1}u(k)\,e_{k-1}+u(p)\,e_{p-1}$. En particulier, $f(e_i)=\begin{cases}e_{i-1}-a_i\,e_{p-1} & \text{si } 1\leqslant i\leqslant p-1\\ -a_0\,e_{p-1} & \text{si } i=0\end{cases}$

donc $\operatorname{Mat}\left(f,(e_0,\dots,e_{p-1})\right)=\begin{pmatrix}0&1&\cdots&0\\0&0&\ddots&\vdots\\\vdots&\vdots&&1\\-a_0&-a_1&\cdots&-a_{p-1}\end{pmatrix}={}^tC_P$.

15. **a.** D'après [**4.d**], une base de vecteurs propres pour ${}^tC_P$ est $\left(\begin{pmatrix}1\\\lambda_1\\\vdots\\\lambda_1^{n-1}\end{pmatrix},\dots,\begin{pmatrix}1\\\lambda_n\\\vdots\\\lambda_n^{n-1}\end{pmatrix}\right)$ donc une base de vecteurs propres pour g est $(v_0,\dots,v_{p-1})$ avec $v_i=\sum_{k=0}^{p-1}\lambda_i^k\,e_k$. Mais la suite $w_i:n\mapsto\lambda_i^n$ appartient à F d'après [**10**] et s'écrit $w_i=\sum_{k=0}^{p-1}\lambda_i^k\,e_k$.
Donc une base de vecteurs propres pour g est $(v_0,\dots,v_{p-1})$ avec $\forall n,\ v_i(n)=\lambda_i^n$.

b. Donc $\forall u\in F,\ \exists\,(k_0,\dots,k_{p-1})\in\mathbb{C}^p,\ u=\sum_{i=0}^{p-1}k_i\,v_i$ soit $\exists\,(k_0,\dots,k_{p-1})\in\mathbb{C}^p,\quad\forall n\in\mathbb{N},\ u(n)=\sum_{i=0}^{p-1}k_i\,\lambda_i^n$.

16. Ici, $P=X^3-(a+b+c)\,X^2+(ab+ac+bc)\,X-abc=(X-a)(X-b)(X-c)$ avec a,b,c distincts (l'hypothèse "non nulles" ne sert pas) donc [**15**] donne : une base de F est $\left((a^n)_{n\in\mathbb{N}},(b^n)_{n\in\mathbb{N}},(c^n)_{n\in\mathbb{N}}\right)$.

Partie IV

17. Non (si $n \geqslant 2$) car $\operatorname{rg}(C_A) \geqslant n-1$ donc si $\operatorname{rg}(A) < n-1$ alors A ne saurait être semblable à C_A (si $n = 1$, $A = C_A$). On peut aussi, selon [**4.c**], prendre A diagonalisable mais avec une valeur propre au moins double.

18. Si on a $(**)$ alors $U - V = P^{-1}(C_U - C_V)P$. Or, les $(n-1)$ premières colonnes de $C_U - C_V$ sont nulles donc $\operatorname{rg}(C_U - C_V) \leqslant 1$ et si on avait $\operatorname{rg}(C_U - C_V) = 0$ alors $C_U - C_V = 0$ donc $U - V = 0$ ce qui est exclu (U et V distinctes) donc $\operatorname{rg}(C_U - C_V) = 1$. Donc $\operatorname{rg}(U - V) = 1$. On a donc montré que $(**) \Longrightarrow (*)$.

19. $U = I_2, \quad V = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ vérifient (*) mais pas (**) et on a $\text{PGCD}\left(\chi u, \chi v\right) = X^2 - 1$.

On a bien $\operatorname{rg}(U - V) = 1$ et, d'autre part $\chi_U = \chi_V$ donc $C_U = C_V$ et, si on avait (**), on aurait $U = V$ ce qui n'est pas.

20. $\operatorname{rg}(u-v) = \operatorname{rg}(U-V) = 1$ et le théorème du rang donne $\dim\big(\operatorname{Ker}(u-v)\big) = n-1$: H est un hyperplan de E .

21. a. Si on avait $F \subset H$ alors $\forall x \in F,\ (u-v)(x) = \vec{0}$ donc $\forall x \in F,\ u(x) = v(x)$ c'est à dire que $u_F = v_F$. On a donc $\chi_{u_F} = \chi_{v_F}$. Posons $P = \chi_{u_F} = \chi_{v_F}$, on a $\deg P = \dim F \geqslant 1$ et P divise χu et χv ce qui contredit $\text{PGCD}\left(\chi u, \chi v\right) = 1$. Donc $F \not\subset H$.

b. $\diamond$ On a donc $F \neq F \cap H$ donc $\dim F > \dim(F \cap H)$ et donc $\dim(F+H) = \dim H + \dim F - \dim(F \cap H) > \dim H = n-1$ donc $\dim(F+H) = n$ et $F + H = E$.

$\diamond$ Notons $p = \dim F$. Soit $\mathcal{B}_F = \big(u_1, \dots, u_p\big)$ une base de F, $\mathcal{B}_H = \big(v_1, \dots, v_{n-1}\big)$ une base de H. Tout élément de E s'écrit $x = \sum_{i=1}^{p} \lambda_i u_i + \sum_{j=1}^{n-1} \mu_j v_j$ donc $\big(u_1, \dots, u_p, v_1, \dots, v_{n-1}\big)$ est génératrice de E et $\big(u_1, \dots, u_p\big)$ est libre donc le théorème de la base incomplète montre qu'on peut compléter $\mathcal{B}_F$ par des vec--teurs de H en une base $\mathcal{B}'$ de E .

$\diamond$ On a donc $\mathcal{B}' = \big(u_1, \dots, u_p, u_{p+1}, \dots, u_n\big)$ avec $u_k \in H$ pour $k \geqslant p+1$. Or, si $x \in H$, $u(x) = v(x)$ et F est stable par u et par v donc on a

$$\operatorname{Mat}\left(u, \mathcal{B}'\right) = \left(\begin{array}{c|c} A_1 & B \\ \hline O & C \end{array}\right) \qquad \operatorname{Mat}\left(v, \mathcal{B}'\right) = \left(\begin{array}{c|c} A_2 & B \\ \hline O & C \end{array}\right) \qquad \text{avec } A_i \in \mathcal{M}_p(\mathbb{K}) \ .$$

Donc $\chi_C \mid \chi_U$, $\chi_C \mid \chi_V$ et $\deg(\chi_C) = n - p \geqslant 1$ puisque $F \neq E$, ce qui contredit $\text{PGCD}\left(\chi u, \chi v\right) = 1$. Donc $F = E$.

c. $\{\vec{0}\}$ et E sont stables par u et par v et on vient de montrer que si F est stable par u et par v et $F \neq \{\vec{0}\}$ alors $F = E$. Donc les seuls sous-espaces stables par u et par v sont E et $\{\vec{0}\}$.

22. a. Pae définition, $G_j = (u^j)^{-1}(H)$ et $U \in \mathrm{GL}_n(\mathbb{K})$ donc $u \in \mathrm{GL}(E)$ et donc $u^j \in \mathrm{GL}(E)$ donc $\dim G_j = \dim H$. Ainsi, pour tout $j \in \mathbb{N}$, G_j est un hyperplan de E .

b. On a donc $G_j = \operatorname{Ker} \varphi_j$ où φ_j est une forme linéaire non nulle sur E. On a alors $\dim\left[\bigcap_{j=0}^{n-2} G_j\right] = \dim\left[\bigcap_{j=0}^{n-2} \operatorname{Ker} \varphi_j\right] = n - \operatorname{rg}\big(\varphi_0, \dots, \varphi_{n-2}\big) \geqslant n - 2n - (n-1) = 1$. Donc $\bigcap_{j=0}^{n-2} G_j \neq \{\vec{0}\}$.

c. Suppposons le résultat faux et considérons comme le suggére l'énoncé, $F = \operatorname{Vect}\big\{y, u(y), \dots, u^{p-1}(y)\big\}$ où p est le plus grand entier naturel non nul pour lequel la famille $\big(y, u(y), \dots, u^{p-1}(y)\big)$ est libre qui est bien défini car $\big\{k \geqslant 1 \mid \big(y, u(y), \dots, u^{k-1}(y)\big)\big\}$ est non vide car (y) est libre et majoré par $n-1$. Par définition

de p, $\big(y, u(y), \dots, u^{p-1}(y)\big)$ est libre et $\big(y, u(y), \dots, u^{p-1}(y), u^p(y)\big)$ est liée donc $\exists\, \big(\alpha_0, \dots, \alpha_{p-1}\big) \in \mathbb{K}^p$ tel que $u^p(y) = \sum_{k=0}^{p-1} \alpha_k u^k(y)$. Ceci montre que $u^p(y) \in F$ et donc $u(F) = \text{Vect}\,\big\{u(y), u^2(y), \dots, u^p(y)\big\} \subset F$.
D'autre part, $\forall k \in [\![0, n-2]\!]$, $y \in G_i$ donc $u^k(y) \in H$ et et donc $v\big(u^k(y)\big) = u\big(u^k(y)\big)$ donc, puisque $p - 1 \leqslant n - 2$, $v(F) = \text{Vect}\,\big\{u(y), u^2(y), \dots, u^p(y)\big\} = u(F) \subset F$. On a donc F stable par u et par v avec $1 \leqslant \dim F \leqslant n-1$ ce qui impossible d'après [**21**]. Donc $\underline{\mathcal{B}'' \text{ est une base de } E}$.

d. On a $u(e_k) = e_{k+1}$ pour $k \in [\![0, n-2]\!]$ donc $\text{Mat}\,\big(u, \mathcal{B}''\big) = C_P$ où $P = X^n - \sum_{k=0}^{n-1} e_k^*\big(u(e_{n-1})\big)\, X^k$. Mais alors, d'après [**2**], $P = (-1)^n\, \chi_u$ donc $C_P = C_U$. D'autre part, comme vu au [**c**], $\forall k \in [\![0, n-2]\!]$, $v(e_k) = u(e_k) = e_{k+1}$ donc $\text{Mat}\,\big(v, \mathcal{B}''\big)$ est aussi une matrice compagnon et, de même que ci-dessus, c'est C_V.
On a donc $\underline{\text{Mat}\,\big(u, \mathcal{B}''\big) = C_U \quad \text{et} \quad \text{Mat}\,\big(v, \mathcal{B}''\big) = C_V}$.

e. En notant P la matrice de passage de $\mathcal{B}''$ à $\mathcal{B}$, on a donc $U = P^{-1}\, C_U\, P$ et $V = P^{-1}\, C_V\, P$. On peut donc conclure que : $\underline{\forall (U, V) \in \big(\text{GL}_n(\mathbb{K})\big)^2, \quad \Big((*) \text{ et } \text{PGCD}\,\big(\chi_U, \chi_V\big) = 1\Big) \Longrightarrow (**)}$.

23. On a bien : $(u, v) \in \big(\text{GL}\,(E)\big)^2$ (car $\chi_u(0) \neq 0$ et $\chi_v(0) \neq 0$), $\text{PGCD}\,\big(\chi_u, \chi_v\big) = 1$ (car si $P \mid \chi_u$ et $P \mid \chi_v$ alors $P \mid \chi_u - \chi_v = 2(-1)^n$) et $\text{rg}(u - v) = 1$.
On peut donc appliquer le résultat de [**22**] à (u, v) : il existe une base $\mathcal{B} = \big(e_1, \dots, e_n\big)$ de E telle que

$$\text{Mat}\,\big(u, \mathcal{B}\big) = C_U = \begin{pmatrix} 0 & \cdots & 0 & -1 \\ 1 & \ddots & & 0 \\ & \ddots & \ddots & \vdots \\ 0 & & 1 & 0 \end{pmatrix} \quad \text{et} \quad \text{Mat}\,\big(v, \mathcal{B}''\big) = C_V = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \ddots & & 0 \\ & \ddots & \ddots & \vdots \\ 0 & & 1 & 0 \end{pmatrix} .$$

Le sous-groupe G de $\text{GL}\,(E)$ engendré par u et v est $G = \Big\{ w_p \circ \cdots \circ w_1 \;\Big|\; p \in \mathbb{N}^*,\ w_i \in \big\{u, v, u^{-1}, v^{-1}\big\} \Big\}$.
Mais le théorème de Cayley-Hamilton donne $v^n = \text{Id}_E$ et $u^n = -\text{Id}_E$ donc $u^{2n} = \text{Id}_E$ donc $v^{-1} = v^{n-1}$ et $u - 1 = u^{2n-1}$ donc $G = \Big\{ w_p \circ \cdots \circ w_1 \;\Big|\; p \in \mathbb{N},\ w_i \in \big\{u, v\big\} \Big\}$.
Posons $X = \big\{e_1, \dots, e_n, -e_1, \dots, -e_n\big\}$ de cardinal $2n$ (car $e_i = \varepsilon e_j$ n'est possible que pour $i = j$ et $\varepsilon = 1$ par liberté de $\mathcal{B}$) et montrons que $\forall (g, x) \in G \times X$, $g(x) \in X$ par récurrence sur p si $g = w_p \circ \cdots \circ w_1$ avec $w_i \in \big\{u, v\big\}$. Pour $p = 0$, $g = \text{Id}_E$ et le résultat est vrai et si il est vrai pour $g = w_p \circ \cdots \circ w_1$ alors, pour $h = w_{p+1} \circ w_p \circ \cdots \circ w_1 = w_{p+1} \circ g$, on a $h(x) = w_{p+1}\big(g(x)\big)$ avec $w_{p+1} \in \big\{u, v\big\}$ et $g(x) \in X$ et, comme $u(e_i) = v(e_i) = e_{i+1}$ pour $1 \leqslant i \leqslant n-1$ et $u(e_n) = -v(e_n) = -e_1$, on a bien $x \in X \Rightarrow h(x) \in X$.
Ainsi, on peut définir $* : \begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g * x = g(x) \end{array}$.
On a clairement $\forall x \in X$, $\text{Id}_E * x = x$ et $\forall (g, h) \in G^2$, $\forall x \in X$, $g * (h * x) = (g \circ h) * x$ donc $*$ est une opération de G sur X (d'aillleurs $*$ n'est rien d'autre qu'une restriction de l'action canonique de $\text{GL}\,(E)$ sur E). On sait qu'alors il existe un morphisme $\varphi : G \to \mathfrak{S}\,(X)$ de noyau $\text{Ker}\,\varphi = \big\{g \in G \mid \forall x \in X,\ g(x) = x\big\}$. Mais, ici, si $g \in \text{Ker}\,\varphi$, on a, en particulier, $\forall i \in [\![1, n]\!]$, $g(e_i) = e_i$ donc $g = \text{Id}_E$ ce qui prouve que φ est injective donc G est en bijection avec $\varphi(G) \subset \mathfrak{S}\,(X)$ et comme $\text{card}\,\big(\mathfrak{S}\,(X)\big) = (2n)!$, $\underline{G \text{ est fini et } \text{card}\,\big(G\big) \leqslant (2n)!}$.

REMARQUE: Une application linéaire étant caractérisée par l'image d'une base, G est en bijection avec $G' = \Big\{ \big(g(e_1), \dots, g(e_n)\big) \;\Big|\; g \in G \Big\}$. Posons σ la permutation circulaire $(1, 2, \dots, n)$ et montrons que $G' = G''$ où $G'' = \Big\{ \big(\varepsilon_1 e_{\sigma^k(1)}, \dots, \varepsilon_n e_{\sigma^k(n)}\big) \;\Big|\; k \in [\![0, n-1]\!],\ \varepsilon_i \in \{-1, 1\} \Big\}$.
L'inclusion $G' \subset G''$ se montre par récurrence comme ci-dessus car $\big(w(\varepsilon_1 e_{\sigma^k(1)}), \dots, w(\varepsilon_n e_{\sigma^k(n)})\big) = \big(\pm\varepsilon_1 e_{\sigma^{k+1}(1)}, \dots, \pm\varepsilon_n e_{\sigma^{k+1}(n)}\big)$ pour $w = u$ ou $w = v$ et que σ est d'ordre n.
Réciproquement, on a par récurrence facile sur k, $\forall k \in [\![0, n]\!]$, $\big(v^k(e_1), \dots, v^k(e_n)\big) = \big(e_{\sigma^k(1)}, \dots, e_{\sigma^k(n)}\big)$ et $\big(u^k(e_1), \dots, u^k(e_n)\big) = \big(e_{\sigma^k(1)}, \dots, e_{\sigma^k(n-k)}, -e_{\sigma^k(n-k+1)}, \dots, -e_{\sigma^k(n)}\big)$. Posons $g_k = v^k \circ u^{n-k}$ ($g_0 = -\text{Id}_E$, $g_n = \text{Id}_E$) , on a donc $\big(g_k(e_1), \dots, g_k(e_n)\big) = \big(e_1, \dots, e_k, -e_{k+1}, \dots, -e_n\big)$ et donc, en posant,

pour $k \in [\![1,n]\!]$, $h_k = g_{k-1} \circ g_k$, $\big(h_k(e_1),\dots,h_k(e_n)\big) = \big(e_1,\dots,e_{k-1},-e_k,e_{k+1},\dots,e_n\big)$. On obtient ainsi $\big(\varepsilon_1 e_{\sigma^k(1)},\dots,\varepsilon_n e_{\sigma^k(n)}\big) = \big(g(e_1),\dots,g(e_n)\big)$ en prenant $\alpha_i = \begin{cases} 0 & \text{si } \varepsilon_i = 1 \\ 1 & \text{si } \varepsilon_i = -1 \end{cases}$ et $g = v^k \circ h_1^{\alpha_1} \circ \cdots \circ h_n^{\alpha_n}$ et on a $g \in G$. Donc $G'' \subset G'$ et, finalement, $\text{card}\,\big(G\big) = \text{card}\,\big(G''\big)$ soit $\underline{\text{card}\,\big(G\big) = n\,2^n}$.