
MATHEMATIQUES 2

I. Propriétés générales

1. En développant $\det(C_P)$ suivant sa première ligne, on obtient :

$$\det(C_P) = (-1)^{n+1}(-a_0).1 = (-1)^n P(0),$$

et donc $C_P \in GL_n(\mathbb{K}) \Leftrightarrow \det(C_P) \neq 0 \Leftrightarrow P(0) \neq 0$.

$$C_P \in GL_n(\mathbb{K}) \Leftrightarrow P(0) \neq 0.$$

2. En développant $\det(C_P - XI_n)$ suivant sa dernière colonne, on obtient :

$$\chi_{C_P} = (-a_{n-1} - X)(-X)^{n-1} + \sum_{k=0}^{n-2} (-1)^{n+k+1}(-a_k)\Delta_k,$$

où Δ_k est le déterminant

$$\begin{vmatrix} -X & 0 & \dots & 0 & 0 & \dots & \dots & 0 \\ \times & -X & \ddots & \vdots & \vdots & & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & & \vdots \\ \times & \dots & \times & -X & 0 & \dots & \dots & 0 \\ \times & \dots & \dots & \times & 1 & \times & \dots & \times \\ \vdots & & & \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & & & \vdots & \vdots & \ddots & \ddots & \times \\ \times & \dots & \dots & \times & 0 & \dots & 0 & 1 \end{vmatrix},$$

$(-X)$ étant écrit k fois. Un calcul par blocs fournit

$\Delta_k = (-X)^k$ et donc,

$$\chi_{C_P} = (-1)^n(X^n + a_{n-1}X^{n-1} + \sum_{k=0}^{n-2} (-1)^k a_k (-1)^k X^k) = (-1)^n(X^n + \sum_{k=0}^{n-1} a_k X^k) = (-1)^n P.$$

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

3. Si Q est un tel polynôme, il est nécessaire que Q soit un polynôme de degré n et de coefficient dominant $(-1)^n$. La question 2. montre alors que cette condition est suffisante.

4. a) On sait que C_P et ${}^t C_P$ ont même polynôme caractéristique (à savoir $(-1)^n P$) et donc même spectre.

$$\text{Sp}(C_P) = \text{Sp}({}^t C_P).$$

b) Soit λ une valeur propre de tC_P . Soit $X = (x_i)_{1 \leq i \leq n} \in \mathcal{M}_{n,1}(\mathbb{K})$.

$$\begin{aligned} {}^tC_P X = \lambda X &\Leftrightarrow \forall k \in \llbracket 1, n-1 \rrbracket, x_{k+1} = \lambda x_k \text{ et } -\sum_{i=0}^{n-1} a_i x_{i+1} = \lambda x_n \\ &\Leftrightarrow \forall k \in \llbracket 2, n \rrbracket, x_k = \lambda^{k-1} x_1 \text{ et } -\sum_{i=0}^{n-1} a_i \lambda^i x_1 = \lambda^n x_1 \\ &\Leftrightarrow \forall k \in \llbracket 2, n \rrbracket, x_k = \lambda^{k-1} x_1 \text{ et } (\lambda^n + \sum_{i=0}^{n-1} a_i \lambda^i) x_1 = 0 \\ &\Leftrightarrow \forall k \in \llbracket 2, n \rrbracket, x_k = \lambda^{k-1} x_1 \text{ et } P(\lambda) x_1 = 0 \\ &\Leftrightarrow \forall k \in \llbracket 2, n \rrbracket, x_k = \lambda^{k-1} x_1 \text{ (car } P(\lambda) = 0\text{)}. \end{aligned}$$

Donc, le sous-espace propre de tC_P associé à la valeur propre λ est $\text{Vect}((1, \lambda, \lambda^2, \dots, \lambda^{n-1}))$. En particulier, tout sous-espace propre de C_P est une droite vectorielle.

$$\forall \lambda \in \text{Sp}({}^tC_P), \text{Ker}({}^tC_P - \lambda I_n) = \text{Vect}((1, \lambda, \lambda^2, \dots, \lambda^{n-1})).$$

c) tC_P est diagonalisable (dans \mathbb{K}) si et seulement si $\chi_{{}^tC_P} = \chi_{C_P} = (-1)^n P$ est scindé sur \mathbb{K} et pour toute valeur propre λ , la dimension du sous-espace propre associé est l'ordre de multiplicité de cette valeur propre.

D'après b), tout sous-espace propre de tC_P est de dimension 1, et donc

$${}^tC_P \text{ est diagonalisable si et seulement si } P \text{ est scindé sur } \mathbb{K}, \text{ à racines simples.}$$

d) D'après b), pour $1 \leq k \leq n$, le sous-espace propre associé à la valeur propre λ_k est engendré par le vecteur $e_k = (\lambda_k^{i-1})_{1 \leq i \leq n}$. D'après c), tC_P est diagonalisable. On en déduit que la famille $(e_k)_{1 \leq k \leq n}$ est une base de E et donc que le déterminant de VANDERMONDE $\det(\lambda_k^{i-1})_{1 \leq i, k \leq n}$ est non nul.

5. a) D'après 2., si A est la matrice compagnon
$$\begin{pmatrix} 0 & \dots & \dots & 0 & 1999 \\ 1 & 0 & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix},$$
 de format 2002, le polynôme ca-

ractéristique de A est $P_A = X^{2002} - X^{2001} - X^{2000} - 1999$. D'après le théorème de CAYLEY-HAMILTON, la matrice A vérifie

$$A^{2002} = A^{2001} + A^{2000} + 1999I_{2002}.$$

b) Soit x_0 un vecteur de E tel que $f^{n-1}(x_0) \neq 0$. Montrons que la famille $(x_0, f(x_0), \dots, f^{n-1}(x_0))$ est libre.

Supposons par l'absurde que cette famille soit liée. Alors, il existe $(\lambda_0, \dots, \lambda_{n-1}) \neq (0, \dots, 0)$ tel que $\sum_{k=0}^{n-1} \lambda_k f^k(x_0) = 0$.

Soit $p = \text{Min}\{k \in \llbracket 0, n-1 \rrbracket / \lambda_k \neq 0\}$. Par définition, $0 \leq p \leq n-1$ et $\sum_{k=p}^{n-1} \lambda_k f^k(x_0) = 0$. En prenant l'image des deux

membres par f^{n-1-p} ($n-1-p$ est un entier positif), on obtient $\sum_{k=p}^{n-1} \lambda_k f^{k+n-p-1}(x_0) = 0$ et donc $\lambda_p f^{n-1}(x_0) = 0$ (puisque, pour $k \geq n$, $f^k(x_0) = 0$). Comme $f^{n-1}(x_0) \neq 0$, on obtient $\lambda_p = 0$ ce qui contredit la définition de p .

Donc, la famille $(x_0, f(x_0), \dots, f^{n-1}(x_0))$ est libre. Etant de cardinal $n = \dim(E)$, cette famille est une base de E .

Dans cette base, la matrice de f est la matrice compagnon $\begin{pmatrix} 0 & \dots & \dots & 0 \\ 1 & \ddots & & \vdots \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}$.

II. Localisation des racines d'un polynôme

6. Puisque $AX = \lambda X$, on a : $\forall i \in \llbracket 1, n \rrbracket$, $\lambda x_i = \sum_{j=1}^n a_{i,j} x_j$. Mais alors, pour $i \in \llbracket 1, n \rrbracket$,

$$|\lambda x_i| \leq \sum_{j=1}^n |a_{i,j}| \times |x_j| \leq \left(\sum_{j=1}^n |a_{i,j}| \right) \|X\|_\infty = r_i \|X\|_\infty.$$

$$\boxed{\forall i \in \llbracket 1, n \rrbracket, |\lambda x_i| \leq r_i \|X\|_\infty.}$$

7. Soient λ une valeur propre de A et $X = (x_i)_{1 \leq i \leq n}$ un vecteur propre associé. Soit i_0 un indice tel que $\|X\|_\infty = |x_{i_0}|$. D'après 6., on a

$$|\lambda| \times \|X\|_\infty = |\lambda x_{i_0}| \leq r_{i_0} \|X\|_\infty.$$

Mais X est un vecteur propre et donc $X \neq 0$. Par suite, $\|X\|_\infty > 0$ et l'inégalité $|\lambda| \|X\|_\infty \leq r_{i_0} \|X\|_\infty$ fournit

$$|\lambda| \leq r_{i_0}.$$

On a ainsi montré que, pour toute valeur propre λ , il existe un indice i_0 tel que $|\lambda| \leq r_{i_0}$ ou encore tel que $\lambda \in D_{i_0}$. Par suite, toute valeur propre de A appartient à $\cup_{1 \leq i \leq n} D_i$. Finalement,

$$\boxed{\text{Sp}(A) \subset \cup_{1 \leq i \leq n} D_i.}$$

8. Notons $(\lambda_1, \dots, \lambda_n)$ la famille des racines (distinctes ou confondues) de P dans \mathbb{C} . Puisque $(-1)^n P$ est le polynôme caractéristique de C_P , $(\lambda_1, \dots, \lambda_n)$ est aussi la famille des valeurs propres de C_P .

D'après 7. chaque valeur propre λ a un module inférieur ou égal à au moins l'un des r_i de la matrice C_P . Or, pour la matrice C_P , $r_1 = |a_0|$ et pour $i \geq 2$, $r_i = |1| + | - a_{i-1} | = 1 + |a_{i-1}|$. Ainsi, toute racine de P a un module inférieur ou égal au plus grand des nombres $|a_0|, 1 + |a_1|, \dots, 1 + |a_{n-1}|$ ou encore

$$\boxed{\text{toutes les racines de } P \text{ sont dans le disque fermé de centre } O \text{ et de rayon } R = \max\{|a_0|, 1 + |a_1|, \dots, 1 + |a_{n-1}|\}.$$

9. Soit P le polynôme $X^d + X^c - X^b - X^a$. D'après 8., les racines de P ont un module au plus égal à $1 + |\pm 1| = 2$. Une racine de P , qui est de plus un nombre entier supérieur ou égal à 2 ne peut donc être que 2.

Réciproquement, on n'a jamais $2^a + 2^b = 2^c + 2^d$. En effet, dans le cas contraire, on peut diviser les deux membres de cette égalité par 2^α où α est le plus petit des quatre nombres a, b, c ou d . L'un des quatre termes est alors 1 et les trois autres sont des puissances strictement positives de 2 et donc des nombres pairs. Ainsi, l'un des deux membres de l'égalité $2^{a-\alpha} + 2^{b-\alpha} = 2^{c-\alpha} + 2^{d-\alpha}$ est un nombre pair et l'autre est un nombre impair, ce qui est impossible.

$$\boxed{\text{L'équation } n^a + n^b = n^c + n^d \text{ n'a donc pas de solution dans } \mathbb{N} \setminus \{0, 1\}.$$

III. Suites récurrentes linéaires

10. Soit $\lambda \in \mathbb{C}$ tel que $P(\lambda) = 0$.

Soit $n \in \mathbb{N}$. $\lambda^{n+p} + a_{p-1} \lambda^{n+p-1} + \dots + a_1 \lambda^{n+1} + a_0 \lambda^n = \lambda^n P(\lambda) = 0$. Ainsi, la suite $(\lambda^n)_{n \in \mathbb{N}}$ est dans F .

11. • Soient $(u, v) \in F^2$ et $(\alpha, \beta) \in \mathbb{C}^2$.

$$\varphi(\lambda u + \mu v) = (\lambda u_0 + \mu v_0, \dots, \lambda u_{p-1} + \mu v_{p-1}) = \lambda(u_0, \dots, u_{p-1}) + \mu(v_0, \dots, v_{p-1}) = \lambda\varphi(u) + \mu\varphi(v).$$

Donc, φ est une application linéaire de F dans \mathbb{C}^p .

• Soit $u \in F$. Si $u \in \text{Ker}(\varphi)$, alors $u_0 = u_1 = \dots = u_{p-1} = 0$. Montrons alors par récurrence que $\forall n \in \mathbb{N}$, $u_n = 0$. C'est vrai pour $n \in \llbracket 0, p-1 \rrbracket$. Soit $n \geq 0$. Supposons que $\forall k \in \llbracket n, n+p-1 \rrbracket$, $u_k = 0$. Alors,

$$u_{n+p} = -a_{p-1}u_{n+p-1} - \dots - a_0u_n = 0.$$

On a montré par récurrence que $\forall n \in \mathbb{N}$, $u_n = 0$. Ainsi, si $u \in \text{Ker}(\varphi)$, alors $u = 0$. Donc, φ est injective.

• Soit $(\alpha_0, \dots, \alpha_{p-1}) \in \mathbb{C}^p$. Soit u la suite définie par :

$$\forall k \in \llbracket 0, p-1 \rrbracket, u_k = \alpha_k \text{ et } \forall n \in \mathbb{N}, u_{n+p} = -a_{p-1}u_{n+p-1} - \dots - a_0u_n.$$

Alors, u est un élément de F tel que $\varphi(u) = (\alpha_0, \dots, \alpha_{p-1})$.

On a montré que : $\forall (\alpha_0, \dots, \alpha_{p-1}) \in \mathbb{C}^p$, $\exists u \in F / \varphi(u) = (\alpha_0, \dots, \alpha_{p-1})$. φ est donc surjective.

Finalement,

$$\varphi \text{ est un isomorphisme de } F \text{ sur } \mathbb{C}^p,$$

et en particulier,

$$\dim F = \dim \mathbb{C}^p = p.$$

12. a) $e_i(p) = -\sum_{k=0}^{p-1} a_k e_i(k) = -\sum_{k=0}^{p-1} a_k \delta_{i,k} = -a_i.$

$$\forall i \in \llbracket 0, p-1 \rrbracket, e_i(p) = -a_i.$$

b) La famille $(e_i)_{0 \leq i \leq p-1}$ est l'image de la base canonique de \mathbb{C}^p par l'isomorphisme φ^{-1} et est donc une base de F .

$$\text{La famille } (e_i)_{0 \leq i \leq p-1} \text{ est une base de } F.$$

c) Soit $u \in F$.

Puisque la famille (e_0, \dots, e_{p-1}) est une base de F , il existe $(\alpha_0, \dots, \alpha_{p-1}) \in \mathbb{C}^p$ tel que $u = \sum_{i=0}^{p-1} \alpha_i e_i$. Mais alors, pour $k \in \llbracket 0, p-1 \rrbracket$,

$$u(k) = \sum_{i=0}^{p-1} \alpha_i e_i(k) = \alpha_k.$$

Ainsi,

$$\forall u \in F, u = \sum_{i=0}^{p-1} u(i) e_i.$$

13. Soient $(u, v) \in E^2$ et $(\alpha, \beta) \in \mathbb{C}^2$. Pour tout entier naturel n ,

$$f(\alpha u + \beta v)(n) = (\alpha u + \beta v)(n+1) = \alpha u(n+1) + \beta v(n+1) = (\alpha f(u) + \beta f(v))(n),$$

et donc $f(\alpha u + \beta v) = \alpha f(u) + \beta f(v)$. f est un endomorphisme de E .

Soit $u \in F$. Montrons que $f(u) \in F$. Pour $n \in \mathbb{N}$,

$$\begin{aligned} f(u)(n+p) &= u(n+p+1) = -a_{p-1}u(n+p) - \dots - a_1u(n+2) - a_0u(n+1) \\ &= -a_{p-1}f(u)(n+p-1) - \dots - a_1f(u)(n+1) - a_0f(u)(n). \end{aligned}$$

Ceci montre que $f(u) \in F$. On a montré que F est stable par f .

$$f \in \mathcal{L}(E) \text{ et } f(F) \subset F.$$

14. Soit $i \in \llbracket 1, p-1 \rrbracket$. D'après 12.c),

$$g(e_i) = \sum_{k=0}^{p-1} g(e_i)(k)e_k = \sum_{k=0}^{p-1} e_i(k+1)e_k = \sum_{k=0}^{p-2} \delta_{i,k+1}e_k + e_i(p)e_{p-1} = e_{i-1} - a_i e_{p-1} \text{ (d'après 12.a)}.$$

D'autre part,

$$g(e_0) = \sum_{k=0}^{p-2} \delta_{0,k+1}e_k + e_0(p)e_{p-1} = -a_0 e_{p-1}.$$

La matrice de g dans la base (e_0, \dots, e_{p-1}) est donc

$$\begin{pmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ & & & & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 & \\ -a_0 & \dots & \dots & -a_{p-2} & -a_{p-1} & \end{pmatrix} \text{ qui est } {}^t C_p.$$

15. a) Pour $i \in \llbracket 0, p-1 \rrbracket$, posons $v_i = (\lambda_i^n)_{n \in \mathbb{N}}$. Tout d'abord, d'après 10., chaque v_i est élément de F . Ensuite, d'après 12.c), la matrice de la famille (v_0, \dots, v_{p-1}) est la matrice de VANDERMONDE $(\lambda_i^j)_{0 \leq i, j \leq p-1}$. Puisque les λ_i sont deux à deux distincts, le déterminant de cette matrice est non nul d'après 4.d). On en déduit que la famille (v_0, \dots, v_{p-1}) est une base de F . Enfin, pour $n \in \mathbb{N}$,

$$g(v_i) = (\lambda_i^{n+1})_{n \in \mathbb{N}} = \lambda_i (\lambda_i^n)_{n \in \mathbb{N}} = \lambda_i v_i,$$

ce qui montre que v_i est un vecteur propre de g associé à la valeur propre λ_i . Finalement, la famille (v_0, \dots, v_{p-1}) est une base de F formée de vecteurs propres de g .

b) Par suite, pour chaque $u \in F$, il existe des constantes complexes k_0, \dots, k_{p-1} telles que $u = k_0 v_0 + \dots + k_{p-1} v_{p-1}$ ou encore telles que $\forall n \in \mathbb{N}, u_n = k_0 \lambda_0^n + \dots + k_{p-1} \lambda_{p-1}^n$.

16. Ici, le polynôme P est le polynôme

$$P = X^3 - (a + b + c)X^2 + (ab + ac + bc)X - abc = (X - a)(X - b)(X - c).$$

Il est de degré 3 et a trois racines simples à savoir a, b et c . D'après ce qui précède, les éléments de F sont les suites de la forme

$$k_0(a^n)_{n \in \mathbb{N}} + k_1(b^n)_{n \in \mathbb{N}} + k_2(c^n)_{n \in \mathbb{N}}, (k_0, k_1, k_2) \in \mathbb{C}^3.$$

IV. Matrices vérifiant $rg(U - V) = 1$

17. Une matrice compagnon est nécessairement non nulle. La matrice compagnon de la matrice nulle n'est donc pas semblable à la matrice nulle (car il existe une et une seule matrice semblable à la matrice nulle, à savoir la matrice nulle elle-même).

Une matrice A n'est pas nécessairement semblable à la matrice compagnon C_A .

18. Si U et V vérifient (**), alors $U - V = P^{-1}(C_U - C_V)P$. La matrice $U - V$ est donc semblable à la matrice $C_U - C_V$ et a en particulier même rang que cette dernière matrice. Maintenant, la matrice $C_U - C_V$ a $n - 1$ colonnes nulles et le rang de $C_U - C_V$, et donc le rang de $U - V$, vaut au plus 1. Comme $U - V$ n'est pas la matrice nulle, $U - V$ est de rang exactement 1.

19. On prend $U = I_2$. On a $U \in GL_2(\mathbb{K})$ et $C_u \neq I_2$. Donc U n'est pas semblable à C_u .
 On prend ensuite $V = \text{diag}(1, -1) \in GL_2(\mathbb{K})$. On a $\text{rg}(U - V) = \text{rg}(\text{diag}(0, 2)) = 1$. U et V sont donc deux éléments de $GL_2(\mathbb{K})$ vérifiant (*) et pas (**).

On a dans ce cas

$$\chi_U \wedge \chi_V = (X - 1)^2 \wedge (X - 1)(X + 1) = X - 1.$$

20. $U - V$ est de rang 1 et donc $u - v$ est de rang 1. D'après le théorème du rang, $H = \text{Ker}(u - v)$ est de dimension $n - 1$ et donc un hyperplan vectoriel de E .

21. a) (H est constitué des x de E tels que $u(x) = v(x)$ et donc u et v coïncident sur H) Puisque $F \neq \{0\}$, χ_{u_F} est de degré au moins 1. Il en est de même de χ_{v_F} . Si $F \subset H$, alors u et v coïncident sur F et en particulier $\chi_{u_F} = \chi_{v_F}$. Mais alors, $\chi_{u_F} = \chi_{v_F}$ est un polynôme de degré au moins 1 divisant à la fois χ_U et χ_V . Ceci contredit le fait que χ_U et χ_V sont premiers entre eux. Donc,

F n'est pas inclus dans H .

b) D'après a), F n'est pas inclus dans H . Donc, $F \cap H \subsetneq F$ et en particulier, $\dim(F \cap H) \leq \dim F - 1$.

$$\dim(F + H) = \dim(F) + \dim(H) - \dim(F \cap H) \geq \dim(F) + n - 1 - (\dim F - 1) = n.$$

Ainsi, $\dim(F + H) \geq n$ et donc

$F + H = E$.

Soit G un supplémetaire de $F \cap H$ dans H . On a d'une part,

$$E = F + H = F + (F \cap H + G) = (F + F \cap H) + G = F + G.$$

D'autre part, $F \cap G \subset G$ et $F \cap G \subset F \cap H$, et donc $F \cap G \subset G \cap (F \cap H) = \{0\}$. Finalement,

$$E = F \oplus G.$$

Soit alors B une base de E adaptée à la décomposition $E = F \oplus G$. B est une base de E obtenue en complétant une base B_F de F par des vecteurs de H .

c) D'après ce qui précède, les seuls sous-espaces stables à la fois par u et par v sont $\{0\}$ et E .

22. a) Pour tout j de \mathbb{N} , G_j est l'image de H par l'automorphisme u^{-j} . On en déduit que G_j a même dimension que H et donc que G_j est un hyperplan vectoriel.

b) Montrons par récurrence que $\forall k \in \llbracket 0, n - 2 \rrbracket$, $\dim \left(\bigcap_{j=0}^k G_j \right) \geq n - k - 1$.

• C'est clair pour $k = 0$.

• Soit $k \in \llbracket 0, n - 3 \rrbracket$. Supposons que $\dim \left(\bigcap_{j=0}^k G_j \right) \geq n - k - 1$ et posons $G = \bigcap_{j=0}^k G_j$. Alors,

$$\dim(G \cap G_{k+1}) = \dim(G) + \dim(G_{k+1}) - \dim(G + G_{k+1}).$$

Comme $\dim(G + G_{k+1})$ vaut $n - 1$ ou n (puisque G_{k+1} est un hyperplan), on a donc

$$\dim(G \cap G_{k+1}) \geq \dim(G) + \dim(G_{k+1}) - n = \dim(G) - 1 \geq n - (k + 1) - 1.$$

Le résultat est démontré par récurrence. En particulier, $\dim \left(\bigcap_{j=0}^{n-2} G_j \right) \geq n - (n - 2) - 1 = 1$ et donc

$\bigcap_{j=0}^{n-2} G_j \neq \{0\}$.

c) Soit $A = \{k \in \mathbb{N}^* / (y, u(y), \dots, u^{k-1}(y)) \text{ est libre}\}$. A est une partie non vide de \mathbb{N} (car $1 \in A$ puisque $y \neq 0$) et majorée (par $n = \dim(E)$). Donc, A admet un plus grand élément noté p .

Soit $F = \text{Vect}(y, u(y), \dots, u^{p-1}(y))$. Tout d'abord $F \neq \{0\}$ (car $y \neq 0$ et $y \in F$).

Ensuite, pour $0 \leq k \leq p-2$, $u(u^k(y)) = u^{k+1}(y) \in F$. D'autre part, par définition de p , la famille $(y, u(y), \dots, u^{p-1}(y))$ est libre et la famille $(y, u(y), \dots, u^{p-1}(y), u^p(y))$ est liée.

On en déduit que $u(u^{p-1}(y)) = u^p(y)$ est dans $\text{Vect}(y, u(y), \dots, u^{p-1}(y)) = F$. Finalement, l'image par u d'une famille génératrice de F est dans F , et donc $u(F) \subset F$. Ainsi, F est un sous-espace non nul de E stable par u . D'après 21.c), $F = E$ ou encore B'' est une base de E .

d) La matrice de u dans B'' est une matrice compagnon. Les coefficients de la dernière colonne de cette matrice sont alors, d'après I.2), les opposés des coefficients du polynôme caractéristique de u . Cette matrice est C_U . De même, la matrice de v dans B'' est C_V .

e) Si P est la matrice de passage de la base B'' à la base B alors $U = P^{-1}C_U P$ et $V = P^{-1}C_V P$. Par suite, si U et V sont deux matrices inversibles telles que $\text{rg}(U - V) = 1$ et telles que χ_U et χ_V soient premiers entre eux, alors il existe une matrice inversible P telle que $U = P^{-1}C_U P$ et $V = P^{-1}C_V P$.

23. • 0 n'est racine ni de χ_u , ni de χ_v et donc u et v sont des automorphismes de E . Le groupe G engendré par u et v est l'ensemble des produits finis de facteurs à choisir parmi u, u^{-1}, v, v^{-1} .

• Soit ω une racine de χ_v dans \mathbb{C} . Alors, $\chi_u(\omega) = (-1)^n(\omega^n + 1) = 2(-1)^n \neq 0$. Ainsi, χ_u et χ_v sont sans racine commune dans \mathbb{C} et sont donc premiers entre eux.

• On peut donc appliquer ce qui précède. Il existe une base $\mathcal{B} = (e_1, \dots, e_n)$ de E telle que

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

• L'image par u ou par v d'un vecteur e_i de \mathcal{B} est un vecteur de la forme $\pm e_j$, $1 \leq j \leq n$. Il en est de même de toute puissance (élément de \mathbb{Z}) de u , toute puissance de v et plus généralement tout produit de puissances de u et de puissances de v c'est-à-dire de tout élément de G . Ainsi, l'image de la base \mathcal{B} par un élément quelconque w de G est de la forme $(\varepsilon_1 e_{\sigma(1)}, \dots, \varepsilon_n e_{\sigma(n)})$ où σ est une permutation quelconque de $\llbracket 1, n \rrbracket$ (l'image de \mathcal{B} par l'automorphisme w est une base de E) et les ε_i sont éléments de $\{-1, 1\}$. On en déduit que $w(\mathcal{B})$ ne peut prendre que $2^n n!$ valeurs possibles et puisqu'un endomorphisme est entièrement déterminé par les images des vecteurs d'une base,

$$\text{card}(G) \leq 2^n n!,$$

ce qui améliore le résultat de l'énoncé puisque

$$(2n)! = (2n) \times (2n-1) \times (2n-2) \times \dots \times 3 \times 2 \geq (2n) \times (2n-2) \times \dots \times 2 = 2^n n!.$$