MP* 1 (Rabat)

My Ismail Mamouni

http ://myismail.net

مُوني مولاي اسماعيل

Préparation aux Concours (CNC-CCP)

Matrices Compagnon

UTILISATIONS DES MATRICES COMPAGNON

Notations et définitions :

Dans tout le problème K désigne $\mathbb{R}$ ou $\mathbb{C}$ et n est un entier naturel.

Si u est un endomorphisme d'un K-espace vectoriel E, on note $u^0 = id_E$ et $\forall n \in \mathbb{N}, u^{n+1} = u^n \circ u$.

On note $K_n[X]$ la K-algèbre des polynômes de degré inférieur ou égal à n, $\mathcal{M}_n(K)$ la K-algèbre des matrices carrées de taille n à coefficients dans K de matrice unité I_n et $GL_n(K)$ le groupe des matrices inversibles de $\mathcal{M}_n(K)$; les éléments de $\mathcal{M}_n(K)$ sont notés $M = (m_{i,j})$.

Pour une matrice A de $\mathcal{M}_n(K)$, on note ${}^tA$ la transposée de la matrice A, $\mathrm{rg}(A)$ son rang, $\chi_A = \det(A - XI_n)$ son polynôme caractéristique et $\mathrm{Sp}\,(A)$ l'ensemble de ses valeurs propres.

Si $P = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ est un polynôme unitaire de $K_n[X]$ on lui associe

$$\text{la } \textbf{matrice compagnon } C_P = \begin{pmatrix} 0 & 0 & . & . & 0 & -a_0 \\ 1 & 0 & . & . & 0 & -a_1 \\ 0 & 1 & 0 & . & 0 & -a_2 \\ . & . & . & . & . & . \\ 0 & . & 0 & 1 & 0 & -a_{n-2} \\ 0 & . & . & 0 & 1 & -a_{n-1} \end{pmatrix} \in \mathcal{M}_n(K)$$

(c'est-à-dire la matrice $C_P = (c_{i,j})$ est définie par $c_{i,j} = 1$ pour $i - j = 1$, $c_{i,n} = -a_{i-1}$ et $c_{i,j} = 0$ dans les autres cas).

Les parties II. III. et IV. utilisent les résultats de la partie I. et sont indépendantes entre elles.

I. Propriétés générales

Dans cette partie on considère le polynôme $P = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ de $K_n[X]$ et C_P sa matrice compagnon associée.

1. Montrer que C_P est inversible si et seulement si $P(0) \neq 0$.
2. Calculer le polynôme caractéristique de la matrice C_P et déterminer une constante k telle que $\chi_{C_p} = kP$.
3. Soit Q un polynôme de $K_n[X]$, déterminer une condition nécessaire et suffisante pour qu'il existe une matrice A de $\mathcal{M}_n(K)$ telle que $\chi_A = Q$.
4. On note ${}^tC_P$ la transposée de la matrice C_P.
   (a) Justifier la proposition : $\mathrm{Sp}\,(C_P) = \mathrm{Sp}\,({}^tC_P)$.

(b) Soit λ élément de $\mathrm{Sp}\left({}^tC_P\right)$, déterminer le sous-espace propre de ${}^tC_P$ associé à λ.

(c) Montrer que ${}^tC_P$ est diagonalisable si et seulement si P est scindé sur K et a toutes ses racines simples.

(d) On suppose que P admet n racines $\lambda_1, \lambda_2, \ldots, \lambda_n$ deux à deux distinctes, montrer que ${}^tC_P$ est diagonalisable et en déduire que le déterminant de Vandermonde $\begin{vmatrix} 1 & 1 & . & . & 1 \\ \lambda_1 & \lambda_2 & . & . & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & . & . & \lambda_n^2 \\ . & . & . & . & . \\ \lambda_1^{n-1} & \lambda_2^{n-1} & . & . & \lambda_n^{n-1} \end{vmatrix}$ est non nul.

5. *Exemples :*

(a) Déterminer une matrice A (dont on précisera la taille n) vérifiant :

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

(b) Soit E un K-espace vectoriel de dimension n et f un endomorphisme de E vérifiant : $f^{n-1} \neq 0$ et $f^n = 0$; montrer que l'on peut trouver une base de E dans laquelle la matrice de f est une matrice compagnon que l'on déterminera.

II. Localisation des racines d'un polynôme

Soit $A = (a_{i,j})$ une matrice de $\mathcal{M}_n(\mathbb{C})$, on pose pour tout entier $1 \leqslant i \leqslant n$:

$$r_i = \sum_{j=1}^{n} |a_{i,j}| \text{ et } D_i = \{z \in \mathbb{C}, |z| \leqslant r_i\}.$$

Pour $X = \begin{pmatrix} x_1 \\ x_2 \\ . \\ x_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{C})$, on note $\|X\|_\infty = \max\limits_{1 \leqslant i \leqslant n} |x_i|$.

6. Soit $\lambda \in \mathrm{Sp}\,(A)$ et $X = \begin{pmatrix} x_1 \\ x_2 \\ . \\ x_n \end{pmatrix}$ un vecteur propre associé à λ.

Montrer que pour tout entier $1 \leqslant i \leqslant n$: $|\lambda x_i| \leqslant r_i \|X\|_\infty$.

7. Démontrer que $\mathrm{Sp}\,(A) \subset \bigcup\limits_{i=1}^{n} D_k$.

8. Soit $P = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ un polynôme de $\mathbb{C}[X]$, établir que toutes les racines de P sont dans le disque fermé de centre 0 et de rayon $R = \max\{|a_0|, 1 + |a_1|, 1 + |a_2|, \ldots, 1 + |a_{n-1}|\}$.

9. *Application :*

Soit a, b, c et d quatre entiers naturels distincts et non nuls, montrer que l'équation d'inconnue n :

$$n^a + n^b = n^c + n^d$$

n'admet pas de solution sur $\mathbb{N} \setminus \{0, 1\}$.

III. Suites récurrentes linéaires

On note $E = \mathbb{C}^{\mathbb{N}}$ l'espace vectoriel des suites de complexes et si u est une suite de E, on écrira $u(n)$ à la place de u_n pour désigner l'image de n par u.

On considère le polynôme $P = X^p + a_{p-1}X^{p-1} + \ldots + a_0$ de $\mathbb{C}[X]$ avec $a_0 \neq 0$ et on lui associe le sous-espace vectoriel F de E formé des éléments u vérifiant la relation :

$$\forall n \in \mathbb{N} : u(n+p) = -a_{p-1}u(n+p-1) - \ldots - a_0 u(n).$$

10. Montrer que si λ est racine de P alors la suite $n \mapsto \lambda^n$ est élément de F.
11. Soit φ l'application de F vers $\mathbb{C}^p$ définie par : $u \mapsto (u(0), u(1), \ldots, u(p-1))$, montrer que φ est un isomorphisme d'espaces vectoriels. Quelle est la dimension de F ?
12. Pour tout entier $0 \leqslant i \leqslant p-1$ on définit les élements e_i de F par :
$$e_i(i) = 1 \text{ et, lorsque } 0 \leqslant j \leqslant p-1 \text{ et } j \neq i,\ e_i(j) = 0.$$
   (a) Déterminer pour $0 \leqslant i \leqslant p-1$ $e_i(p)$.
   (b) Montrer que le système de vecteurs $(e_0, e_1, \ldots, e_{p-1})$ est une base de F.
   (c) Soit u un élément de F, établir que $u = \sum\limits_{i=0}^{p-1} u(i)e_i$.
13. Si u est un élément de E, on définit l'élément $f(u)$ de E par : $f(u) : n \mapsto u(n+1)$. Montrer que l'application f ainsi définie est un endomorphisme de E et que F est stable par f.
14. Si g est l'endomorphisme de F induit par f, montrer que la matrice de g dans la base $(e_0, e_1, \ldots, e_{p-1})$ est ${}^t C_P$.
15. On suppose que P admet p racines non nulles et deux à deux distinctes : λ_0, λ_1, ..., λ_{p-1}.
   (a) Déterminer une base de F formée de vecteurs propres de g.
   (b) En déduire que, si u est élément de F, il existe des constantes complexes k_0, k_1, ..., k_{p-1} telles que : $\forall n \in \mathbb{N}, u(n) = k_0\lambda_0^n + k_1\lambda_1^n + \ldots + k_{p-1}\lambda_{p-1}^n$.
16. *Exemple :* (On revient à la notation usuelle u_n)

   Soit a, b et c trois réels distincts.

   Déterminer une base de l'espace vectoriel des suites définies par u_0, u_1 et u_2 et par la relation de récurrence valable pour tout $n \in \mathbb{N}$:
$$u_{n+3} = (a+b+c)u_{n+2} - (ab+ac+bc)u_{n+1} + abc.$$

IV. Matrices vérifiant : $\mathrm{rg}(U - V) = 1$

Dans cette partie, pour une matrice A, on notera C_A la matrice compagnon du polynôme $(-1)^n\chi_A$.

17. Une matrice A est-elle nécessairement semblable à la matrice compagnon C_A ?

   Pour tout couple (U, V) de matrices de $GL_n(K)$, on considère les deux propositions suivantes, que l'on identifie chacune par un symbole :

   (*) : $\mathrm{rg}(U - V) = 1$

   (**) : Il existe une matrice inversible P telle que $U = P^{-1}C_U P$ et $V = P^{-1}C_V P$.
18. Montrer qu'un couple (U, V) de matrices distinctes de $GL_n(K)$ vérifiant (**) vérifie (*).
19. Déterminer un couple (U, V) de matrices de $GL_2(K)$ $(n = 2)$ vérifiant (*) mais ne vérifiant pas (**) et déterminer le plus grand commun diviseur des polynômes χ_U et χ_V.

   Dans la suite de cette partie, (U, V) est un couple de matrices de $GL_n(K)$ vérifiant (*) et tel que χ_U et χ_V sont deux polynômes premiers entre eux.

   Soit E un K-espace vectoriel de dimension n et de base B, on désigne par u et v les automorphismes de E tels que U (respectivement V) soit la matrice de u (respectivement v) dans la base B.

   Enfin on pose $H = \mathrm{Ker}(u - v)$.
20. Montrer que H est un hyperplan vectoriel de E.

21. Soit $F \neq \{0\}$ un sous-espace vectoriel de E stable par u et par v c'est-à-dire :
$$u(F) \subset F \text{ et } v(F) \subset F.$$
On notera u_F (respectivement v_F) l'endomorphisme induit par u (respectivement v) sur F.
On rappelle que χ_{u_F} divise χ_u.
   (a) Montrer que F n'est pas inclus dans H.
   (b) On suppose que $F \neq E$, montrer que $F + H = E$ puis que l'on peut compléter une base B_F de F par des vecteurs de H pour obtenir une base B' de E. En utilisant les matrices de u et v dans la base B' montrer que l'on aboutit à une contradiction.
   (c) Quels sont les seuls sous-espaces stables à la fois par u et par v ?
22. Pour $j \in \mathbb{N}$, on note $G_j = \left\{x \in E, u^j(x) \in H\right\}$.
   (a) Montrer que les sous-espaces G_j sont des hyperplans vectoriels de E.
   (b) Montrer que $\bigcap\limits_{j=0}^{n-2} G_j \neq \{0\}$.
   (c) Soit y un vecteur non nul de $\bigcap\limits_{j=0}^{n-2} G_j$, on pose pour $0 \leqslant j \leqslant n-1$: $e_j = u^j(y)$.
   Montrer que $B'' = (e_0, e_1, \ldots, e_{n-1})$ est une base de E.
   (On pourra considérer $F = \operatorname{Vect}\left\{y, u(y), \ldots, u^{p-1}(y)\right\}$ où p est le plus grand entier naturel non nul pour lequel la famille $\left(y, u(y), \ldots, u^{p-1}(y)\right)$ est libre).
   (d) Montrer que la matrice de u (respectivement v) dans B'' est C_U (respectivement C_V).
   (e) Conclure.
23. *Application :*
Soit u et v deux automorphismes d'un K-espace vectoriel E de dimension n vérifiant :
$$\operatorname{rg}(u - v) = 1,\ \chi_u(X) = (-1)^n\,(X^n + 1) \text{ et } \chi_v(X) = (-1)^n\,(X^n - 1).$$
En utilisant une action de groupe, montrer que le groupe engendré par u et v est fini de cardinal inférieur ou égal à $(2n)!$.

Fin de l'énoncé.

GCP 2001
COMPOSITION de MATHEMATIQUE II
(Série MP)

Partie I

1) En développant par rapport à la première ligne on trouve $\det C_P = \pm a_0$, d'où le résultat.
2) Le plus rapide est de développer par rapport à la dernière colonne, on trouve alors

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

et on reconnaît $(-1)^n(X^n + a_{n-1}X^{n-1} + \ldots + a_0) = (-1)^n P(X)$.
Donc $k = (-1)^n$.
3) Il faut et il suffit que le terme dominant de Q soit $(-1)^n X^n$.
4)a) Les valeurs propres sont les racines de χ qui se calcule par un déterminant; or le déterminant est invariant par transposition.

4)b) on a ${}^tC_P = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \dots & & 0 & 1 \\ -a_0 & -a_1 & \dots & & -a_{n-1} \end{pmatrix}$; si $X = \begin{pmatrix} x_1 \\ x_2 \\ \ddots \\ x_n \end{pmatrix}$ il vient le système

$$\begin{cases} x_2 & = \lambda x_1 \\ x_3 & = \lambda x_2 \\ \vdots & \\ x_n & = \lambda x_{n-1} \\ -a_0 x_1 & -\ldots - a_{n-1}x_n = \lambda x_n \end{cases} \iff \begin{cases} x_i = \lambda^{i-1}x_1 \ \forall i = 1\ldots n \\ (-a_0 - a_1\lambda - \ldots - a_{n-1}\lambda^{n-1})x_1 \quad = \lambda^n x_1 \end{cases}$$

Donc x_1 ne peut être nul (un vecteur propre n'est pas nul), λ est racine de P et tout vecteur propre est multiple de $X_\lambda = \begin{pmatrix} 1 \\ \lambda \\ \ddots \\ \lambda^{n-1} \end{pmatrix}$

4c) On vient de constater que les espaces propres sont tous limités à des droites; la matrice ${}^tC_P$ n'est donc diagonalisable que s'il y a assez de telles droites pour engendrer l'espace entier, c'est à dire si P a n racines distinctes (et donc simples). La réciproque est du cours (puisque $P = \pm\chi_{{}^tC_P}$).
4d)) Si P est scindé à racines simples, comme on vient de le voir une matrice de passage qui diagonalise ${}^tC_P$ est $V = \begin{pmatrix} 1 & \dots & 1 \\ \lambda_1 & \dots & \lambda_n \\ \ddots & & \\ \lambda_1^{n-1} & \dots & \lambda_n^{n-1} \end{pmatrix}$, qui est inversible puisque matrice de passage ! Bien sûr son déterminant est assez connu.
Remarque: à ce stade on pourrait diagonaliser aussi bien la matrice C_P, car de $V^{-1}{}^tC_PV = \Delta$ on déduit ${}^tVC_PV^{-1} = \Delta$.
5a) Vu le contexte, on va chercher à écrire une matrice C_P où $P(X) = X^{2002} - X^{2001} - X^{2000} - 1999I_{2002}$. En particulier $n = 2002$.
Une telle matrice conviendra par le théorème de Cayley-Hamilton, qui sert beaucoup dans ce problème.
On prend donc

$$A = \begin{pmatrix} 0 & \dots & 0 & 1999 \\ 1 & \ddots & \vdots & 0 \\ & & & \\ 0 & & 0 & 1 \\ 0 & \dots & 1 & 1 \end{pmatrix}$$

5b) Attention au piège: bien sûr que C_{X^n} conviendrait, mais ce n'est pas ce que l'on demande !
On commence par utiliser l'hypothèse: on prend un vecteur e_1 tel que $f^{n-1}(e_1)$ soit non nul, et on applique f: $f(e_1) = e_2, \dots, f^k(e_1) = e_{k+1}$.
Je dis que la famille ainsi construite $(e_1, \dots, e_n)$ **est une base.**
Pour le prouver, on vérifie qu'elle est libre (et son cardinal est n):
supposant que $\alpha_1e_1 + \dots\alpha_ne_n = 0$, on a en appliquant f^{n-1} et par linéarité $\alpha_1f^{n-1}(e_1) + 0 + \dots + 0 = 0$, d'où $\alpha_1 = 0$.
On recommence de proche en proche, en appliquant cette fois f^{n-2} pour annuler α_2, etc.
Finalement la combinaison linéaire est triviale et la famille est libre.
Dans cette base, on a bien

$$\mathrm{Mat}(f) = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & & \vdots & \vdots \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & & & & \\ 0 & \dots & & 1 & 0 \end{pmatrix}$$

Partie II

6) Par hypothèse, on a pour tout $i = 1 \dots n$

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

Par l'inégalité triangulaire,

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

7) Soit i un indice tel que $|x_i| = \|X\|_\infty$, dans les conditions de la question précédente.
On a alors $|\lambda| \leq r_i$, c'est à dire $\lambda \in D_i$.
Ceci est vrai pour n'importe quelle valeur propre, qui appartiendra donc à l'un des disques D_i. Au total,

$$\mathrm{Sp}(A) \subset \bigcup_{k=1}^{n} D_k$$

(qui d'ailleurs n'est autre que le plus grand des n disques).
8) On va se servir de la première partie ! En effet, les racines de P sont les valeurs propres de sa matrice compagne C_P. Or

$$r_1 = |a_0| \quad r_2 = 1 + |a_1| \quad \ldots \quad r_n = 1 + |a_n|$$

comme on le lit sur la matrice C_P. En appliquant la question précédente, on en déduit que toutes les racines de P sont dans le disque $D_R = \bigcup_{k=1}^{n} D_k$ où $R = \max r_k$.
9) Une application amusante !
Supposons pour fixer les idées que a soit le plus grand des quatre entiers a, b, c, d (on a forcément alors c ou $d > b$, mais peu importe). Posons

$$P(X) = X^a + X^b - X^c - X^d$$

La matrice C_P ne contient que des $0, \pm 1$ et on a avec les notations de la question précédente $R = 2$.
Les seules racines entières possibles sont donc $0, 1, 2$.
Reste à exclure le dernier cas: or si 2 est racine, on a (avec par exemple $c > d$)

$$2^b(1 + 2^{a-b}) = 2^d(1 + 2^{c-d})$$

ce qui ne serait possible qu'avec $b = d$ contrairement à l'hypothèse, par unicité de la décomposition en facteurs premiers puisque les contenus des parenthèses sont impairs (ou par le théorème de Gauss si vous y tenez).
Donc les seules racines dans $\mathbb{N}$ de $n^a + n^b = n^c + n^d$ sont 0 et 1.

Partie III

10) Remplaçons $u(n)$ par λ^n: on a bien $\lambda^{n+p} + a_{p-1}\lambda^{n+p-1} + \ldots + a_0\lambda^n = 0$ dès que $P(\lambda) = 0$. Cqfd (la réciproque est fausse, par exemple quand $a_0 = \lambda = 0$).
11) Tout d'abord, φ est linéaire (ses composantes sont des formes linéaires).
Ensuite, c'est une bijection, car chacune des suites élément de F est uniquement et entièrement déterminée par des p premières valeurs, compte tenu de la relation de récurrence.
Donc F, isomorphe à $\mathbb{C}^p$, est de dimension p.
12a) $e_i(p) = -a_{p-1}e_i(p-1) - \ldots - a_0 e_i(0) = -a_i$.

12b) Les e_i sont l'image de la base canonique de $\mathbb{C}^p$ par l'isomorphisme φ^{-1}.

12c) La suite u et la suite $\sum_{i=0}^{p-1} u(i)e_i$ sont deux éléments de F qui commencent par les p mêmes termes, à savoir $\varphi(u) = (u(0), u(1), \ldots, u(p-1))$.
Elles sont donc identiques: les termes ultérieurs suivent par récurrence.
Remarque : l'application φ évoque le cours sur les bases duales …

13) $f(u + \lambda v)$ est par définition la suite de terme général

$$(u + \lambda v)(n + 1) = u(n + 1) + \lambda v(n + 1)$$

C'est donc $f(u) + \lambda f(v)$ ce qui prouve la linéarité de f: ainsi $f \in \mathcal{L}(E)$.
Enfin, la relation de récurrence qui définit F devant être vraie pour tout n sera vraie pour tout $n + 1$! (la réciproque n'est PAS vraie …) ce qui signifie que $f(F) \subset F$, *ie* que F est stable par F.

14) Cela résulte de **12a)**: en effet, $e_i(p) = -a_i$ et donc

$$f(e_i) = (0, 0, 0, \ldots, 0, 1, 0, \ldots, -a_i, \ldots) \quad \text{et} \quad \varphi(f(e_i)) = (0, 0, 0, \ldots, 0, 1, 0, \ldots, -a_i)$$

En écrivant ceci en colonnes pour $i = 0 \ldots p-1$, on obtient la matrice de f dans la base (e_i) et on reconnaît ${}^tC_P$.

15a) D'après **4c)**, ${}^tC_P$ est diagonalisable et une base de vecteurs propres est donnée par les colonnes de $V = \begin{pmatrix} 1 & \ldots & 1 \\ \lambda_0 & \ldots & \lambda_{p-1} \\ \ddots & & \\ \lambda_1^{p-1} & \ldots & \lambda_{p-1}^{p-1} \end{pmatrix}$.

15b) Tout élément de F s'écrit dans cette base qui est constituée de suites géométriques (cf. **10**) autrement dit cela ne s'arrête pas à l'exposant $p-1$, mais pour tout $n \in \mathbb{N}$ on a

$$u(n) = k_0\lambda_0^n + \ldots + k_{p-1}\lambda_{p-1}^{p-1}$$

où les k_i sont tout simplement les coordonnées de u dans la base (e_i).

16) Les racines de $P(X) = X^3 - (a+b+c)X^2 + (ab+bc+ca)X - abc$ sont a, b et c.
Ces réels étant supposés distincts, tout est fini: une base de l'espace F est constituée par les trois suites géométriques $(a^n), (b^n), (c^n)$ et tout élément de F s'écrit

$$u_n = \alpha a^n + \beta b^n + \gamma c^n$$

où α, β, γ sont fonction des valeurs initiales u_0, u_1, u_2 (la matrice de passage entre ces paramètres étant de la forme V, cf. supra).

Partie IV

Notons que par la première partie, $\chi_A = \chi_{C_A} = (-1)^n P$.

17 Hé non: on peut s'inspirer du **5b)**, la matrice $C_A = \begin{pmatrix} 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & & \vdots & \vdots \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & & & & \\ 0 & \ldots & & 1 & 0 \end{pmatrix}$
convient avec $A = 0$, matrice nulle ! Alors que C_A est de rang $n - 1$.

18) Supposons $(**)$, c'est à dire que (U, C_U) et (V, C_V) sont simultanément semblables: comme le rang est invariant par changement de base, on a

$$\mathrm{rg}(U-V) = \mathrm{rg}(C_U - C_V) = \mathrm{rg}\begin{pmatrix} 0 & \dots & \bullet \\ \vdots & & \vdots \\ 0 & \dots & \bullet \end{pmatrix}$$

Cette matrice ne peut être nulle: on aurait $\mathrm{rg}(U-V) = 0$ et donc $U = V$ ce qui est exclu. Donc elle est de rang 1, ce qui prouve $(*)$.

19) Prenons $U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, V = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On a $C_U = C_V = \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}$ car $\chi_U = \chi_V = (X-1)^2$. Néanmoins $U = I_2$ n'est clairement pas semblable à C_U, alors que V est semblable à C_V.
Comme les polynômes caractéristiques ont été choisis égaux, leur pgcd est leur valeur commune $(X-1)^2$.

20) Par le théorème du rang, H est un hyperplan.

21a) Si $F \subset H$ on aurait $u_F = v_F$ et donc $\chi_{u_F} = \chi_{v_F}$. Mais $\chi_{u_F} | \chi_u$ et $\chi_{v_F} | \chi_v$, on aurait donc un diviseur commun non trivial contrairement à l'hypothèse que ces deux polynômes sont premiers entre eux.
Donc $F \not\subset H$.

21b) Soit $x \in F \setminus H$: alors H et x engendrent E puisque H est un hyperplan et $x \notin H$. Cela signifie que $F + H = E$ (mais pas $F \oplus H = E$!).
Il n'y a pas de théorème du cours qui permette de conclure immédiatement, même si cela paraît clair. On peut par exemple

- Utiliser deux fois le théorème de la base incomplète en partant d'une base de $F \cap H$ que l'on complètera dans F, puis dans H.
- Considérer les familles libres maximales de la forme $(B_F, h_1, \dots, h_k)$ où B_F est une base donnée de F et les h_i appartiennent à H. On vérifie qu'une telle famille engendre F et H (par maximalité), et donc c'est une base de E.
- Il y a d'autres façons de faire !

On a donc par blocs

$$\mathrm{Mat}(u) = \begin{pmatrix} \bullet & \bullet \\ 0 & \widetilde{U} \end{pmatrix} \qquad \mathrm{Mat}(v) = \begin{pmatrix} \bullet & \bullet \\ 0 & \widetilde{V} \end{pmatrix}$$

où les sous-matrices $\widetilde{U}$ et $\widetilde{V}$ coïncident, puisque u et v agissent de la même façon sur H ! (en fait, même les sous-matrices *au dessus* de celles-ci sont égales).
Donc $\chi_{\tilde{U}} = \chi_{\tilde{V}}$ est un diviseur commun de χ_U et χ_V, contrairement à l'hypothèse qu'ils sont premiers entre eux.

21c) Finalement les seuls sous-espaces stables à la fois par u et v sont E entier et $\{0\}$.

22a) u^j est, comme u, un automorphisme, qui conserve la dimension: donc $G_j = u^{-j}(H)$ est, comme H, un hyperplan.

22b) On a $\dim G_0 = \dim H = n-1, \dim G_0 \cap G_1 \geq n-2, \dots \dim G_0 \cap \dots \cap G_{n-2} \geq n-1$ en vertu du

Lemme. Si H' est un hyperplan et F un sev, on a $\dim(F \cap H') \geq \dim F - 1$.

Démonstration du lemme: soit Δ une droite supplémentaire de H'. Alors $F = F \cap H' \oplus F \cap \Delta$, et $F \cap \Delta$ est au plus une droite, cqfd.

22c) Un tel y existe d'après la question précédente.

La famille $\mathcal{F} = \{y, u(y), \ldots, u^{p-1}(y)\}$ ne peut être libre pour toute valeur de p (au maximum elle peut avoir n éléments !), soit donc p maximal tel que la famille $\mathcal{F}$ soit libre, cette famille est une base de l'espace F qu'elle engendre.

Nous voulons montrer que $F = E$ c'est à dre que $p = n$.

- D'abord notons que $e_0, e_1, \ldots, e_{n-2} \in H$ par définition même de y. Raisonnons dorénavant par l'absurde: si $p < n$, on a donc $F \subset H$.
- De plus F est stable par u car l'image par u de la base $\mathcal{F}$ est encore dans F: en particulier, $u(e_{p-1})$ est combinaison linéaire de $\mathcal{F}$ par maximalité de p.
- Enfin et triomphalement, pour tout $x \in F$ on a $v(x) = u(x) \in F$ puisque $F \subset H$ et $v_F = u_F$. Donc F est stable par v lui aussi.

Nous sommes arrivés à une impossibilité d'après **21c)**. Donc $F = E, p = n$ et $B'' = \mathcal{F}$ est une base de E.

22d) Utilisons Cayley-Hamilton: $\chi_u(u)(y) = 0 = (-1)^n(u^n(y)+a_{n-1}u^{n-1}(y)+ \ldots + a_0 y)$ et donc

- $u(e_k) = u^k(y)$ pour $k < n-1$
- $u(e_{n-1}) = u(u^{n-1}(y)) = u^n(y) = -a_0 y - \ldots - a_{n-1}u^{n-1}(y) = -a_0 e_0 - \ldots - a_{n-1}e_{n-1}$.

Ce qui signifie que la matrice de u est bien C_u dans la base $B'' = \mathcal{F}$. De même pour v pour les $n-1$ premières colonnes, la dernière est alors obligatoirement constituée des coefficients de χ_v par **2**.

22e) Récapitulons: on a montré que le changement de base vers $\mathcal{F}$ change U (resp. V) en C_U (resp. C_V). Nous avons donc montré $(**)$.

23) Une application amusante encore !

D'abord notons que χ_U et χ_V sont effectivement premiers entre eux (leur différence est une constante – non nulle). Donc ce qui précède s'applique. Dans une base B'' bien choisie, on a les matrices de ces endomorphismes qui sont

$$U = \begin{pmatrix} 0 & 0 & \ldots & 0 & -1 \\ 1 & 0 & & \vdots & \vdots \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & & & & \\ 0 & \ldots & & 1 & 0 \end{pmatrix} \qquad V = \begin{pmatrix} 0 & 0 & \ldots & 0 & +1 \\ 1 & 0 & & \vdots & \vdots \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & & & & \\ 0 & \ldots & & 1 & 0 \end{pmatrix}$$

Considérons l'ensemble réunion de B'' et de son opposée:

$$X = (e_0, \ldots, e_{n-1}, -e_0, \ldots, -e_{n-1})$$

$*$ Cet ensemble a $2n$ éléments, u et v agissent sur X. Par exemple, u envoie $-e_{n-1}$ sur e_1.

$*$ Tout composé de u et v agit donc sur X, et le groupe G engendré par u et v agit sur X.

$*$ Réciproquement, tout élément de G est déterminé par son action sur X: en effet X contient une base, et tout endomorphisme est déterminé par l'image d'une base.
$*$ Le morphisme de G dans $\mathfrak{S}_X$, ensemble des permutations de X, qui définit l'action de G sur X est donc injectif, ce qui suffit à prouver que le cardinal de G est inférieur ou égal à celui de $\mathfrak{S}_X$, soit $(2n)!$, cqfd.
Remarque: il est facile de constater que l'action de u et v ne peut que permuter les vecteurs de X en changeant éventuellement leurs signes. On tombe donc dans un groupe plus petit, défini par des couples constitués d'une permutation des n indices et de n choix de signes, ce qui fait $2^n n!$ choix possibles seulement. Matriciellement il s'agit des matrices qui possèdent par ligne et par colonne un seul terme non nul, qui vaut 1 ou -1.