Réduction des matrices

Etant donné un endomorphisme u d'un espace vectoriel E de dimension finie, il est très souvent indispensable de trouver une base de E par rapport à laquelle la matrice de u soit aussi simple que possible — le degré maximum de « simplicité » qu'on peut espérer étant fourni par les matrices diagonales. L'outil principal pour résoudre ce problème est la théorie des vecteurs propres exposée au § 34, qui suffit déjà dans beaucoup de cas. Pour des endomorphismes u tout à fait généraux, on doit utiliser les raisonnements nettement plus difficiles du § 35, que le lecteur débutant pourra négliger, mais qui sont néanmoins aussi utiles que ceux du § 34, dans les applications de la théorie (équations différentielles linéaires à coefficients constants par exemple).

Le § 36 a pour but de fournir des classes de matrices dont on peut affirmer d'avance qu'elles sont réductibles à la forme diagonale. Ici l'outil principal consiste à utiliser sur l'espace E un « produit scalaire » analogue au produit scalaire classique dans l'espace usuel, et permettant de donner un sens à la notion de vecteurs « orthogonaux ». Les considérations du § 36 sont aussi à la base de la classification des « quadriques » (surfaces définies par des équations algébriques du second degré), dont nous n'avons pas parlé dans le texte.

1. Définition des vecteurs propres et valeurs propres

Soient E un espace vectoriel sur un corps commutatif K, et u un endomorphisme de E. On appelle **vecteur propre** de u tout vecteur *non nul* $x \in E$ tel que $u(x)$ soit proportionnel à x; il est clair qu'alors le sous-espace vectoriel D de E engendré par x (i.e. l'ensemble des multiples de x) vérifie $u(D) \subset D$; réciproquement, si une droite D de E, passant par l'origine, vérifie $u(D) \subset D$, tout vecteur non nul porté par D est un vecteur propre de u.

On dit qu'un scalaire $\lambda \in K$ est une **valeur propre** de u s'il existe un vecteur *non nul* $x \in E$ tel que

$$u(x) = \lambda x; \tag{1}$$

x est alors un vecteur propre de u; on dit que x est un vecteur propre **associé** à la valeur propre λ.

On remarquera que la relation (1) signifie que x est annulé par l'endomorphisme

$$u - \lambda . 1$$

de E (où 1 désigne l'endomorphisme unité de E); donc, pour que λ soit valeur propre de u, il faut et il suffit que

$$\mathrm{Ker}(u - \lambda . 1) \neq 0.$$

Supposons E de dimension finie sur K; on peut alors appliquer à $u - \lambda . 1$ le Corollaire 2 du Théorème 8 du § 23, et on obtient donc le résultat suivant :

THÉORÈME 1. *Soit u un endomorphisme d'un espace vectoriel* E *de dimension finie sur un corps commutatif* K. *Pour qu'un scalaire $\lambda \in K$ soit une valeur propre de u, il faut et il suffit que l'on ait*

$$\det(u - \lambda . 1) = 0. \tag{2}$$

Ce résultat va nous permettre de montrer que les valeurs propres de u sont les racines d'une équation algébrique à coefficients dans K.

2. *Polynôme caractéristique d'une matrice*

Soient E un espace vectoriel de dimension finie n sur le corps K et u un endomorphisme de E; choisissons une base $(a_i)_{1\leqslant i\leqslant n}$ de E, et soit

$$U = (\alpha_{ij})_{1\leqslant i,j\leqslant n}$$

la matrice de u par rapport à cette base (§ 12, n° 3). Comme celle de l'endomorphisme unité de E est la matrice unité

$$1_n = (\delta_{ij})_{1\leqslant i,j\leqslant n} \quad \text{avec } \delta_{ij} = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j \end{cases},$$

on voit que par rapport à la base considérée l'endomorphisme $u - \lambda.1$ est représenté par la matrice

$$U - \lambda.1_n = (\alpha_{ij} - \lambda\delta_{ij}) = \begin{pmatrix} \alpha_{11}-\lambda & \alpha_{21} & \dots & \alpha_{n1} \\ \dots & \dots & \dots & \dots \\ \alpha_{1n} & \alpha_{2n} & \dots & \alpha_{nn}-\lambda \end{pmatrix}, \tag{3}$$

qu'on obtient en retranchant λ à chaque terme diagonal α_{ii} de U. D'après le Théorème 1, les valeurs propres de u s'obtiennent donc en écrivant la relation

$$\begin{vmatrix} \alpha_{11}-\lambda & \alpha_{21} & \dots & \alpha_{n1} \\ \dots & \dots & \dots & \dots \\ \alpha_{1n} & \alpha_{2n} & \dots & \alpha_{nn}-\lambda \end{vmatrix} = 0. \tag{4}$$

Considérons alors K comme plongé dans l'anneau K[X] des polynômes à une indéterminée à coefficients dans K, et formons la matrice $U - X.1_n$, à coefficients dans l'anneau commutatif K[X]; son déterminant

$$p_U(X) = \det(U - X.1_n) = \begin{vmatrix} \alpha_{11}-X & \alpha_{21} & \dots & \alpha_{n1} \\ \dots & \dots & \dots & \dots \\ \alpha_{1n} & \alpha_{2n} & \dots & \alpha_{nn}-X \end{vmatrix} \tag{5}$$

est un élément de K[X], i.e. un polynôme à une indéterminée à coefficients dans K; on l'appelle le **polynôme caractéristique de la matrice** U, et la relation (4) montre que *les valeurs propres de u sont les racines dans* K *de l'équation*

$$p_U(\lambda) = 0. \tag{6}$$

Il faut remarquer que le polynôme p_U ne change pas si l'on remplace U par la matrice U' de u par rapport à une autre base de E; en effet, on a alors (§ 15, Corollaire du Théorème 2)

$$U' = PUP^{-1}$$

pour une matrice $P \in GL(n, K)$; alors, et comme $P1_nP^{-1} = 1_n$, on a

$$U' - X.1_n = PUP^{-1} - X.P1_nP^{-1} = P(U - X.1_n)P^{-1}$$

et par suite

$$p_{U'}(X) = \det(P).p_U(X).\det(P)^{-1} = p_U(X)$$

en vertu du théorème de multiplication des déterminants; ce qui prouve notre assertion.

Il est donc naturel d'appeler **polynôme caractéristique de l'endomorphisme** u le polynôme $p_U(X)$ où U est la matrice de u par rapport à une base quelconque de E. On notera ce polynôme

$$p_u(X),$$

et on a évidemment

$$p_u(\lambda) = \det(u - \lambda.1) \quad \text{pour tout } \lambda \in K \tag{7}$$

(si K est un corps infini, cette relation suffit à caractériser p_u d'après le Théorème 1 du § 28). Le Théorème 1 s'énonce alors en disant que *les valeurs propres de u sont les racines de son polynôme caractéristique.*

D'autre part, les considérations précédentes rendent naturelles la définition suivante : on appelle **valeur propre d'une matrice carrée** $U = (\alpha_{ij})_{1\leqslant i,j\leqslant n}$ à coefficients dans K tout élément de K (ou, plus généralement, d'un sur-corps commutatif de K) qui vérifie l'équation (6).

3. *Forme du polynôme caractéristique*

Conservant les notations ci-dessus, nous allons chercher à obtenir quelques renseignements sur la forme du polynôme

$$p_U(X) = \begin{vmatrix} \alpha_{11}-X & \alpha_{21} & \dots & \alpha_{n1} \\ \alpha_{12} & \alpha_{22}-X & \dots & \alpha_{n2} \\ \dots & \dots & \dots & \dots \\ \alpha_{1n} & \alpha_{2n} & \dots & \alpha_{nn}-X \end{vmatrix}.$$

Lorsqu'on développe ce déterminant, on trouve une somme de $n!$ termes; le « terme principal » est le produit

$$(\alpha_{11}-X)(\alpha_{22}-X)\dots(\alpha_{nn}-X) \tag{8}$$

des termes diagonaux du déterminant considéré; chacun des autres termes est lui aussi un produit de n termes du déterminant considéré, mais $n-2$ au plus de ces n termes se trouvent sur la diagonale principale; par suite, $p_U(X)$ *est somme de* (8) *et d'un polynôme de degré $n-2$ au plus en* X. Il s'ensuit que les monômes de degré $> n-2$ de p_U sont les mêmes que ceux du polynôme (8), et par conséquent on a une relation de la forme

$$(-1)^n p_U(X) = X^n - (\alpha_{11} + \alpha_{22} + \dots + \alpha_{nn})X^{n-1} + \dots,$$

les termes non écrits étant de degré $n-2$ au plus.

On peut donc écrire

$$(-1)^n p_U(X) = X^n - \tau_1(U)X^{n-1} + \tau_2(U)X^{n-2} - \dots + (-1)^n\tau_n(U); \tag{9}$$

les coefficients $\tau_i(U) \in K$ sont évidemment des fonctions polynômiales des coefficients α_{ij} de la matrice U, à coefficients entiers rationnels; on a vu que

$$\tau_1(U) = \alpha_{11} + \alpha_{22} + \cdots + \alpha_{nn} \tag{9}$$

est la somme des coefficients diagonaux de la matrice U; on appelle ce scalaire la **trace** (*) de la matrice U, et on le désigne le plus souvent par la notation

$$\mathrm{Tr}(U).$$

D'autre part, en faisant $X = 0$ dans (9), et en tenant compte du fait évident *a priori* que $p_U(0) = \mathrm{dét}(U)$, on voit que

$$\tau_n(U) = \mathrm{dét}(U). \tag{10}$$

Exemple 1. Si $n = 2$ et

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

on a

$$p_U(X) = \begin{vmatrix} a - X & b \\ c & d - X \end{vmatrix} = (a-X)(d-X) - bc = X^2 - \mathrm{Tr}(U)X + \mathrm{dét}(U).$$

Si $n = 3$ et si

$$U = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}$$

il vient

$$p_U(X) = \begin{vmatrix} a - X & b & c \\ a' & b' - X & c' \\ a'' & b'' & c'' - X \end{vmatrix} = -X^3 + \mathrm{Tr}(U)X^2 - \tau_2(U)X + \mathrm{dét}(U)$$

on laisse au lecteur le soin de calculer $\tau_2(U)$; cf. *Exercice* 40.

4. *Existence de valeurs propres*

Étant donné qu'une équation algébrique à coefficients dans un corps algébriquement clos K possède toujours au moins une racine dans K (par définition même des corps algébriquement clos...), on a évidemment le résultat suivant :

Théorème 2. *Tout endomorphisme d'un espace vectoriel non nul de dimension finie sur un corps* algébriquement clos *possède au moins une valeur propre.*

Il est clair de même que toute matrice carrée à coefficients dans un corps algébriquement clos K possède au moins une valeur propre dans K.

Dans la pratique élémentaire, ces résultats s'appliquent surtout lorsque $K = \mathbf{C}$.

(*) Voir § 12, *Exercice* 8, § 16, *Exercice* 5, § 26, *Exercices* 4 et 5, § 34, *Exercices* 18 et 27.

Remarque 1. Une matrice à coefficients dans un corps K non algébriquement clos peut fort bien n'avoir aucune valeur propre dans K. Prenons par exemple $K = \mathbf{R}$ et la matrice

$$U = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

qui, en coordonnées rectangulaires, représente la rotation d'angle θ autour de l'origine. Ses valeurs propres sont les solutions de l'équation

$$\begin{vmatrix} \cos\theta - \lambda & -\sin\theta \\ \sin\theta & \cos\theta - \lambda \end{vmatrix} = (\cos\theta - \lambda)^2 + \sin^2\theta = 0;$$

pour que cette équation possède une racine réelle il faut et il suffit que θ soit multiple de π; dans le cas contraire, les racines sont les nombres complexes

$$\cos\theta \pm i.\sin\theta,$$

qui ne sont pas réels.

Soient E un espace vectoriel de dimension finie sur un corps commutatif K, et u un endomorphisme de E. On dit que u **a toutes ses valeurs propres dans** K si le polynôme p_u a toutes ses racines dans K, i.e. (§ 33, n° 1) si l'on peut écrire

$$(-1)^n p_u(X) = (X - \lambda_1)^{r_1} \ldots (X - \lambda_q)^{r_q}$$

où les λ_i sont les diverses racines de p_u dans K, et les r_i leurs ordres de multiplicité. De même on dit qu'une matrice carrée U à coefficients dans K a toutes ses valeurs propres dans K si son polynôme caractéristique a toutes ses racines dans K. C'est toujours le cas si le corps de base est algébriquement clos.

Exemple 2. — Prenons $K = \mathbf{R}$ et une matrice U d'ordre 2 ; on a

$$p_U(X) = X^2 - \mathrm{Tr}(U)X + \mathrm{dét}(U),$$

donc U a toutes ses valeurs propres réelles si et seulement si l'on a

$$\mathrm{Tr}(U)^2 - 4.\mathrm{dét}(U) \geqslant 0.$$

5. *Réduction à la forme triangulaire*

Une matrice carrée U à coefficients dans un anneau est dite **triangulaire** si elle est de la forme

$$\begin{pmatrix} \alpha_{11} & \alpha_{21} & \alpha_{31} & \ldots & \alpha_{n1} \\ 0 & \alpha_{22} & \alpha_{32} & \ldots & \alpha_{n2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \alpha_{nn} \end{pmatrix},$$

autrement dit si ceux de ses termes qui sont situés en-dessous de la diagonale sont nuls. D'autre part, un endomorphisme u d'un espace vectoriel E de dimension finie sur un corps K est dit **trigonalisable** s'il existe une base de E par rapport à laquelle

la matrice de u soit triangulaire, autrement dit s'il existe une base $x_1, \ldots, x_n$ de E telle que l'on ait des relations de la forme

$$(10)\qquad \begin{cases} u(x_1) = \alpha_{11}x_1 \\ u(x_2) = \alpha_{21}x_1 + \alpha_{22}x_2 \\ \cdots\cdots\cdots\cdots\cdots \\ u(x_n) = \alpha_{n1}x_1 + \alpha_{n2}x_2 + \cdots + \alpha_{nn}x_n ; \end{cases}$$

s'il en est ainsi il est clair que u possède au moins une valeur propre dans K, à savoir α_{11}; de plus on a alors

$$p_u(X) = \begin{vmatrix} \alpha_{11} - X & \alpha_{21} & \cdots & \alpha_{n1} \\ 0 & \alpha_{22} - X & \cdots & \alpha_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \alpha_{nn} - X \end{vmatrix}$$

et donc

$$(11)\qquad p_u(X) = (\alpha_{11} - X)(\alpha_{22} - X)\ldots(\alpha_{nn} - X)$$

en vertu du § 24, *Exemple* 2. Comme les α_{ii} sont dans K, on voit donc qu'alors u a toutes ses valeurs propres dans K. Cette condition, nécessaire pour que u soit trigonalisable (et toujours vérifiée si K est algébriquement clos), est aussi suffisante — autrement dit, on a le résultat suivant :

THÉORÈME 3. *Soient* E *un espace vectoriel de dimension finie sur un corps commutatif* K, *et* u *un endomorphisme de* E. *Pour que* u *soit trigonalisable il faut et il suffit que* u *ait toutes ses valeurs propres dans* K.

Tout revient à montrer que la condition est suffisante; pour la commodité du lecteur débutant, nous allons d'abord le faire lorsque K est *algébriquement clos*, le cas général étant un peu plus difficile à traiter.

Nous devons donc montrer que, si K est algébriquement clos, *tout* endomorphisme de E est trigonalisable. Soit u un tel endomorphisme; comme K est algébriquement clos, u possède au moins une valeur propre, autrement dit il existe un $\alpha_{11} \in K$ et un vecteur *non nul* $x_1 \in E$ tels que l'on ait

$$(12)\qquad u(x_1) = \alpha_{11}x_1.$$

Soit D le sous-espace vectoriel de dimension 1 de E engendré par x_1, de sorte que D est stable par u, et soit F un supplémentaire de D dans E, de sorte que $E = D \oplus F$ (somme directe); l'existence de F résulte du § 19, Corollaire 2 du Théorème 2. Désignons par p l'homomorphisme de E sur F obtenu en projetant chaque $x \in E$ sur F parallèlement à D (§ 17, n° 4), et construisons un endomorphisme v de F en posant

$$(13)\qquad v(x) = p(u(x)) \quad \text{pour tout } x \in F;$$

comme F est de dimension $n - 1$, on peut, en raisonnant par récurrence, supposer le Théorème déjà établi pour F et v, donc construire une base $x_2, \ldots, x_n$ de F telle

que l'on ait des relations de la forme

$$(14)\qquad \begin{cases} v(x_2) = \alpha_{22}x_2 \\ v(x_3) = \alpha_{32}x_2 + \alpha_{33}x_3 \\ \cdots\cdots\cdots\cdots\cdots \\ v(x_n) = \alpha_{n2}x_2 + \alpha_{n3}x_3 + \ldots + \alpha_{nn}x_n ; \end{cases}$$

mais la relation (13) montre que, pour tout $x \in F$, le vecteur $u(x)$ ne diffère du vecteur $v(x)$ que par un multiple scalaire de x_1, et en particulier on aura des relations de la forme

$$(15)\qquad \begin{cases} u(x_2) = \alpha_{21}x_1 + v(x_2) \\ u(x_3) = \alpha_{31}x_1 + v(x_3) \\ \cdots\cdots\cdots\cdots\cdots \\ u(x_n) = \alpha_{n1}x_1 + v(x_n) ; \end{cases}$$

cela dit, puisque $x_2, \ldots, x_n$ forment une base de F il est clair que $x_1, x_2, \ldots, x_n$ forment une base de E, et les relations (12), (14) et (15) montrent que la matrice de u par rapport à cette base est triangulaire. Le Théorème est donc établi pour un corps K algébriquement clos.

Passons maintenant au *cas d'un corps commutatif* K *quelconque*; on va naturellement s'inpsirer de la démonstration précédente, et raisonner par récurrence sur la dimension n de E. Choisissons d'abord une valeur propre $\alpha_{11} \in K$ de u et un vecteur propre correspondant $x_1 \in E$; on a donc à nouveau la relation (12). Comme ci-dessus, notons D la droite engendrée par x_1, F un sous-espace de dimension $n - 1$ supplémentaire de D dans E, et v l'endomorphisme de F donné par (13) : tout revient évidemment à faire voir que v est trigonalisable. Or, si l'on raisonne par récurrence sur n, en sorte qu'on peut supposer le théorème déjà démontré pour $n - 1 = \dim(F)$, tout revient, pour montrer que v est trigonalisable, à prouver que v *a toutes ses valeurs propres dans* K.

Pour cela choisissons une base quelconque $y_2, \ldots, y_n$ de F et soit V la matrice de v par rapport à cette base; comme on a des relations de la forme

$$u(y_i) = \alpha_{i1}x_1 + v(y_i) \quad (2 \leqslant i \leqslant n)$$

il est clair que, par rapport à la base $x_1, y_2, \ldots, y_n$ de E, l'endomorphisme u admet pour matrice

$$U = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{n1} \\ 0 & \beta_{22} & \cdots & \beta_{n2} \\ 0 & \beta_{23} & \cdots & \beta_{n3} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \beta_{2n} & \cdots & \beta_{nn} \end{pmatrix}$$

où l'on a posé $V = (\beta_{ij})_{2 \leqslant i,j \leqslant n}$. Retranchant X aux termes diagonaux de U et calculant à l'aide du § 24, *Exemple* 2 le déterminant de la matrice ainsi obtenue on trouve

$$p_U(X) = (\alpha_{11} - X)\, p_V(X).$$

Par suite, le polynôme $p_v = p_u$ divise le polynôme $p_U = p_u$, et comme celui-ci a toutes ses racines dans K par hypothèse, il en est donc de même de p_v (§ 33, fin du n° 1); autrement dit, v a bien toutes ses valeurs propres dans K, et la démonstration est achevée.

COROLLAIRE 1. *Soit* E *un espace vectoriel de dimension finie sur un corps algébriquement clos; tout endomorphisme de* E *est trigonalisable.*

COROLLAIRE 2. *Soit* U *une matrice carrée d'ordre* $n \geqslant 1$ *à coefficients dans un corps algébriquement clos* K. *Il existe une matrice* $P \in GL(n, K)$ *telle que la matrice*

$$PUP^{-1}$$

soit triangulaire.

Il suffit pour le voir d'appliquer le Corollaire 1 à l'endomorphisme de K^n défini par U, et de tenir compte du § 15, Corollaire du Théorème 2.

COROLLAIRE 3. *Soit* U *une matrice carrée d'ordre* $n \geqslant 1$ *à coefficients dans un corps commutatif* K. *Les propriétés suivantes sont équivalentes :*

a) il existe une matrice $P \in GL(n, K)$ *telle que* PUP^{-1} *soit triangulaire ;*

b) la matrice U *a toutes ses valeurs propres dans* K.

En considérant l'endomorphisme u de K^n défini par U, la propriété *a)* signifie que u est trigonalisable; comme $p_u = p_U$, le Corollaire 3 résulte donc aussitôt du Théorème.

Une matrice $U \in M_n(K)$ qui vérifie la propriété *a)* est dite **trigonalisable sur K.** Bien entendu, il existe toujours une matrice inversible P telle que PUP^{-1} soit triangulaire, mais en général P est à coefficients non dans K, mais dans un corps algébriquement clos contenant K (par exemple, si $K = \mathbf{R}$, on est en général obligé de prendre pour P une matrice inversible complexe) — il suffit pour le voir d'appliquer le Corollaire 2. Dire que U est trigonalisable sur K signifie qu'on peut supposer P à coefficients dans K.

Comme on le verra au § suivant, on peut grandement améliorer le Théorème 3 en montrant qu'il existe une base de E par rapport à laquelle la matrice de u comporte beaucoup plus de zéros qu'une matrice triangulaire; mais la démonstration du résultat complet est nettement plus difficile que celle du Théorème 3, lequel suffit dans beaucoup d'applications.

6. *Cas où toutes les valeurs propres sont simples*

Le Théorème 3 ne repose sur aucune hypothèse concernant les multiplicités des valeurs propres de u. Il arrive fréquemment dans la pratique que non seulement le polynôme p_u ait toutes ses racines dans K mais en outre que celles-ci soient toutes simples. On a alors un résultat beaucoup plus précis que le Théorème 3.

Avant de l'établir, nous allons tout d'abord démontrer le résultat suivant :

THÉORÈME 4. *Soient* u *un endomorphisme d'un espace vectoriel* E *sur un corps commutatif et* $x_1, \ldots, x_n \in E$ *des vecteurs propres de* u *associés à des valeurs propres* deux à deux distinctes $\lambda_1, \ldots, \lambda_n$. *Alors les vecteurs* $x_1, \ldots, x_n$ *sont linéairement indépendants.*

Soit F le sous-espace vectoriel de E engendré par $x_1, \ldots, x_n$; les relations

$$u(x_i) = \lambda_i x_i \quad (1 \leqslant i \leqslant n) \tag{16}$$

montrent que, si

$$x = \sum \xi_i x_i$$

est un vecteur de F, le vecteur

$$u(x) = \sum \xi_i u(x_i) = \sum \lambda_i \xi_i x_i$$

est encore dans F. Par suite F est stable par u, et on peut considérer l'endomorphisme v de F induit par u. On a $v(x_i) = \lambda_i x_i$ et par suite les λ_i sont des valeurs propres de v; les λ_i étant supposés deux à deux distincts on voit que v possède *au moins* n valeurs propres. Mais celles-ci sont racines d'une équation de degré égal à dim (F); on a donc

$$n \leqslant \dim(F);$$

comme $x_1, \ldots, x_n$ engendrent F, on en déduit (§ 19, Théorème 10) que ces vecteurs forment en fait une base de F, et sont donc linéairement indépendants, ce qui achève la démonstration. (Voir aussi les *Exercices* 38 et 39 de ce §).

Remarque 2. L'hypothèse que les valeurs propres λ_i sont *deux à deux distinctes* est essentielle pour assurer la validité du Théorème 4. Par exemple prenons pour u l'application nulle, ou l'application identique; alors, quels que soient $x_1, \ldots, x_n$ *non nuls*, il est clair que $x_1, \ldots, x_n$ sont des vecteurs propres de u, mais il est évidemment hors de question de démontrer que n vecteurs non nuls dans un espace vectoriel quelconque sont toujours linéairement indépendants !

Nous pouvons maintenant énoncer et démontrer le résultat annoncé au début de ce n° :

THÉORÈME 5. *Soit* u *un endomorphisme d'un espace vectoriel* E *de dimension finie* $n \geqslant 1$ *sur un corps commutatif* K. *Supposons que le polynôme caractéristique* p_u *de* u *admette* n *racines simples* $\lambda_1, \ldots, \lambda_n$ *dans* K. *Alors il existe une base de* E *par rapport à laquelle la matrice de* u *est*

$$\begin{pmatrix} \lambda_1 & 0 & 0 & \ldots & 0 \\ 0 & \lambda_2 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \lambda_n \end{pmatrix}$$

Pour chaque i, choisissons dans E un vecteur propre x_i de u appartenant à la valeur propre λ_i; d'après le Théorème précédent, les n vecteurs ainsi obtenus sont linéairement indépendants, et comme ils sont en nombre $n = \dim(E)$, ils forment donc une base de E. Il est clair que la matrice de u par rapport à cette base n'est autre que celle de l'énoncé.

COROLLAIRE. *Soit* U *une matrice carrée d'ordre n à coefficients dans un corps commutatif* K. *Supposons que son polynôme caractéristique* p_U *possède n racines simples* $\lambda_1, \ldots, \lambda_n$ *dans* K. *Il existe alors une matrice* $P \in GL(n, K)$ *telle que l'on ait*

$$PUP^{-1} = \begin{pmatrix} \lambda_1 & 0 & 0 & \ldots & 0 \\ 0 & \lambda_2 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \lambda_n \end{pmatrix}.$$

Il suffit pour le voir d'appliquer le Théorème 5 à l'endomorphisme de K^n défini par U.

Exemple 3. Prenons $n = 2$ et $K = \mathbf{C}$; l'équation caractéristique de U est

$$X^2 - \mathrm{Tr}(U)X + \mathrm{dét}(U) = 0,$$

elle a donc deux racines simples (i.e. distinctes) dans K si et seulement si

$$\mathrm{Tr}(U) - 4.\mathrm{dét}(U) \neq 0;$$

s'il en est ainsi, U est donc semblable (§ 15, n° 5) à une matrice diagonale.

Il n'en est plus nécessairement de même si $\mathrm{Tr}(U)^2 - 4.\mathrm{dét}(U) = 0$, par exemple si

$$U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix};$$

pour que U soit semblable à une matrice diagonale, il faut que U admette dans K^2 deux vecteurs propres linéairement indépendants, i.e. non proportionnels; or, la matrice considérée a pour seule valeur propre 1, et les vecteurs propres correspondants sont les $x = (\xi_1, \xi_2)$ tels que l'on ait $Ux = x$, i.e.

$$\begin{aligned} \xi_1 + \xi_2 &= \xi_1 \\ \xi_2 &= \xi_2, \end{aligned}$$

autrement dit ce sont les multiples scalaires du premier vecteur de la base canonique; on ne peut donc pas trouver dans K^2 deux vecteurs propres non proportionnels de U.

Exemple 4. Prenons $K = \mathbf{R}$ et $n = 2$; alors le Corollaire s'applique si et seulement si

$$\mathrm{Tr}(U)^2 - 4.\mathrm{dét}(U) > 0.$$

Dans ce cas, il existe une matrice inversible *réelle* P telle que PUP^{-1} soit diagonale. Lorsqu'on a au contraire

$$\mathrm{Tr}(U)^2 - 4.\mathrm{dét}(U) < 0,$$

il existe une matrice inversible P *complexe* telle que PUP^{-1} soit diagonale (appliquer l'*Exemple* 3), mais on ne peut pas prendre pour P une matrice réelle.

Enfin, supposons

$$\mathrm{Tr}(U)^2 - 4.\mathrm{dét}(U) = 0,$$

et soit $\lambda \in \mathbf{C}$ l'unique valeur propre de U; celle-ci est du reste réelle, et l'on a même

$$\lambda = \frac{\mathrm{Tr}(U)}{2}$$

vu la théorie des équations du second degré à discriminant nul. S'il existe une matrice inversible P (réelle ou complexe) telle que

$$PUP^{-1} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix},$$

il est clair que p_U est aussi le polynôme caractéristique du second membre, i.e. $(X - \lambda_1)(X - \lambda_2)$; comme p_U admet par hypothèse λ pour racine double il vient donc

$$\lambda_1 = \lambda_2 = \lambda,$$

et par suite

$$PUP^{-1} = \lambda.1_2,$$

d'où résulte que

$$U = \lambda.1_2.$$

Lorsque $\mathrm{Tr}(U)^2 - 4.\mathrm{dét}(U) = 0$, il est donc impossible de « diagonaliser » U sauf dans le cas où U est déjà une matrice diagonale.

7. *Caractérisation des endomorphismes diagonalisables*

Soit u un endomorphisme d'un espace vectoriel E de dimension finie n sur un corps commutatif K. On dit que u est **diagonalisable** s'il existe une base de E formée de vecteurs propres de u, autrement dit par rapport à laquelle la matrice de u soit diagonale. Le Théorème 5 donne une condition *suffisante* pour qu'il en soit ainsi : à savoir, que le polynôme caractéristique de u ait toutes ses racines dans K, et qu'elles soient toutes simples (ou, si l'on préfère, que ce polynôme admettre n racines deux à deux distinctes dans K). Mais cette condition n'est évidemment pas nécessaire (exemple trivial : l'endomorphisme unité; sa matrice par rapport à n'importe quelle base de E est diagonale, mais son polynôme caractéristique, à savoir

$$(1 - X)^n,$$

ne possède pas de racines simples !).

On va donc énoncer une condition *nécessaire et suffisante* pour qu'un endomorphisme u de E soit diagonalisable. Pour cela, nous aurons besoin des notions suivantes. Étant donnée une valeur propre λ de u, nous appellerons **multiplicité de** λ la multiplicité de λ comme racine du polynôme p_u. D'autre part, nous appellerons **sous-espace propre de** E **associé à** λ l'ensemble (qui est évidemment un sous-espace vectoriel de E) des vecteurs propres de u associés à λ; on notera $E(\lambda)$ ce sous-espace; on a donc

$$E(\lambda) = \mathrm{Ker}(u - \lambda.1),$$

THÉORÈME 6. *Soit u un endomorphisme d'un espace vectoriel* E *de dimension finie sur un corps* K. *Pour que u soit diagonalisable, il faut et il suffit que les deux conditions suivantes soient remplies* :

a) *le polynôme caractéristique p_u a toutes ses racines dans* K;

b) *pour toute valeur propre λ, la dimension du sous-espace propre* $E(\lambda)$ *est égale à la multiplicité de λ comme racine de p_u.*

Supposons ces conditions vérifiées, et soient $\lambda_1, \ldots, \lambda_q$ les racines de p_u, et $r_1, \ldots, r_q$ leurs ordres de multiplicité. En vertu du Théorème 4, les sous-espaces vectoriels $E(\lambda_1), \ldots, E(\lambda_q)$ sont linéairement indépendants au sens du § 17, n° 3; comme on a en outre

$$\dim E(\lambda_1) + \cdots + \dim E(\lambda_q) = n = \dim E$$

en vertu des relations (*)

$$\dim E(\lambda_i) = r_i, \quad r_1 + \cdots + r_q = n,$$

on voit (§ 19, Corollaire 3 du Théorème 13) que

$$E = E(\lambda_1) \oplus \cdots \oplus E(\lambda_q) \quad \text{(somme directe)}; \tag{17}$$

on obtient alors une base de E en réunissant des bases de $E(\lambda_1), \ldots, E(\lambda_q)$; cette base est formée de vecteurs propres de u, et u est donc bien diagonalisable.

Supposons inversement que u soit diagonalisable; notons encore $\lambda_1, \ldots, \lambda_q$ ses diverses valeurs propres et posons

$$s_i = \dim E(\lambda_i).$$

Les sous-espaces $E(\lambda_i)$ sont linéairement indépendants (Théorème 4); comme E admet une base formée de vecteurs propres de u, i.e. d'éléments de ces sous-espaces, on voit que ces sous-espaces engendrent E. On a donc comme plus haut la relation (17), et on obtient une base de E en réunissant des bases de $E(\lambda_1), \ldots, E(\lambda_q)$; par rapport à cette base, la matrice de u est évidemment

$$U = \begin{pmatrix} \lambda_1 & & & & 0 \\ & \ddots & & & \\ & & \lambda_1 & & \\ & & & \ddots & \\ & & & & \lambda_q \\ 0 & & & & \ddots \\ & & & & & \lambda_q \end{pmatrix}$$

avec s_i termes diagonaux égaux à λ_i; le polynôme caractéristique de U, i.e. de u, est donc

$$p_u(X) = (\lambda_1 - X)^{s_1} \ldots (\lambda_q - X)^{s_q};$$

(*) La première exprime l'hypothèse (*b*), et la seconde l'hypothèse (*a*) de l'énoncé.

cela prouve d'une part que toutes ses racines sont dans K, d'autre part que la multiplicité de λ_i est égale à $s_i = \dim E(\lambda_i)$, et ceci achève la démonstration.

Remarque 3. La condition *a*) est toujours remplie si K est algébriquement clos, par exemple si $K = \mathbf{C}$.

Remarque 4. La condition *b*) signifie que $E(\lambda)$ *possède la plus grande dimension possible* (ce qui est conforme au bon sens, puisqu'on désire trouver suffisamment de vecteurs propres pour pouvoir en extraire une base de E); autrement dit, quel que soit l'endomorphisme u, on a l'inégalité

$$\dim E(\lambda) \leqslant \text{multiplicité de } \lambda$$

pour toute valeur propre de u dans K.

Pour établir ce point posons $E(\lambda) = F$; il est clair que $u(F) \subset F$ et que l'endomorphisme v de F induit par u est l'homothétie de rapport λ; le polynôme caractéristique de v est donc

$$p_v(X) = (\lambda - X)^{\dim E(\lambda)};$$

pour établir le résultat cherché il suffit donc de faire voir que $p_v(X)$ divise $p_u(X)$. Autrement dit, on est ramené à établir le résultat général que voici : *soit* F *un sous-espace de* E *stable par u*, i.e. tel que $u(F) \subset F$; *soit v l'endomorphisme de* F *induit par u*, i.e. tel que $v(x) = u(x)$ pour tout $x \in F$; *alors le polynôme p_v divise le polynôme p_u.*

Pour cela, choisissons arbitrairement une base $x_1, \ldots, x_r$ de F, et complétons-la en une base de E (ce qui est toujours possible : § 19, Corollaire 2 du Théorème 2). La matrice de u par rapport à la base obtenue est évidemment de la forme

$$U = \begin{pmatrix} V & T \\ 0 & W \end{pmatrix}$$

où V est la matrice de v par rapport à la base $x_1, \ldots, x_r$, où T est une matrice à r lignes et $n - r$ colonnes, et où W est une matrice carrée d'ordre $n - r$). Par suite

$$U - X.1_n = \begin{pmatrix} V - X.1_r & T \\ 0 & W - X.1_{n-r} \end{pmatrix},$$

et le § 24, *Exemple* 2 montre que

$$\det (V - X.1_n) = \det (V - X.1_r) \det (W - X.1_{n-r}),$$

ce qui s'écrit encore

$$p_u(X) = p_v(X) p_w(X)$$

et démontre le résultat annoncé.

A la notion d'endomorphisme diagonalisable correspond celle de matrice diagonalisable. Une matrice $U \in M_n(K)$ est dite **diagonalisable** s'il existe une matrice $P \in GL(n, K)$ telle que la matrice PUP^{-1} soit diagonale; en raison du § 15, n° 5, cela veut dire que l'endomorphisme de K^n défini par U est diagonalisable. C'est

toujours le cas si le polynôme caractéristique p_U a toutes ses racines dans K, et si elles sont toutes simples.

Une notion analogue mais un peu plus subtile est celle de **matrice semi-simple.** On appelle ainsi toute matrice $U \in M_n(K)$ possédant la propriété suivante : il existe un sur-corps commutatif L de K tel que U soit diagonalisable en tant que matrice à coefficients dans L (on démontre qu'on peut alors prendre pour L n'importe quel sur-corps algébriquement clos de K). Si l'on regarde U comme la matrice d'un endomorphisme u de K^n, cela veut dire, intuitivement, que u possède « suffisamment » de vecteurs propres pourvu qu'on autorise les vecteurs propres à avoir leurs coordonnées dans un sur-corps de K.

Exemple 3. Prenons $K = \mathbf{R}$ et la matrice

$$U = \begin{pmatrix} \cos\theta, & -\sin\theta \\ \sin\theta, & \cos\theta \end{pmatrix};$$

ses valeurs propres dans $\mathbf{C}$ sont (*Remarque* 1) les nombres

$$\cos\theta \pm i.\sin\theta;$$

si θ n'est pas multiple de π, ces valeurs propres sont distinctes, en sorte que U est diagonalisable en tant que matrice à coefficients dans $\mathbf{C}$; mais elle ne l'est pas comme matrice à coefficients dans $\mathbf{R}$, puisque ses valeurs propres ne sont pas réelles — autrement dit, sur le corps $\mathbf{R}$, la matrice U est seulement semi-simple (y compris évidemment pour θ multiple de π).

§ 35. Forme canonique d'une matrice

Le but de ce § est de démontrer le Théorème de Jordan dont on trouvera l'énoncé plus loin, et qui remplace la réduction à la forme diagonale pour les matrices non diagonalisables. Quoique ce théorème joue un grand rôle dans certaines parties des Mathématiques (notamment dans la théorie des équations différentielles linéaires), sa connaissance n'est pas indispensable au lecteur débutant. Celui-ci pourra donc, soit négliger purement et simplement ce §, soit ne l'étudier qu'à titre d'exercice.

1. Le théorème de Hamilton-Cayley

Soient K un anneau commutatif et f un polynôme à une indéterminée à coefficients dans K, à savoir

$$f(X) = a_0 + a_1X + \cdots + a_rX^r.$$

Étant donnés un sur-anneau L de K tel que K soit dans le *centre* de L (i.e. tel que $au = ua$ pour $a \in K$, $u \in L$) et un élément u de L, nous poserons

$$f(u) = a_0 + a_1u + \cdots + a_ru^r;$$

lorsque L est commutatif on retrouve la définition du § 28, n° 1 (dans le cas général, on pourrait se ramener à un anneau commutatif en remplaçant L par le sous-anneau $K[u]$ formé des combinaisons linéaires, à coefficients dans K, des puissances de u).

Si en particulier on prend $L = M_n(K)$, anneau des matrices carrées d'ordre n à coefficients dans K, on voit qu'on peut définir $f(U)$ pour tout polynôme $f \in K[X]$ et toute matrice carrée U à coefficients dans K (ou même dans un sur-anneau commutatif de K).

Ceci dit :

THÉORÈME 1. *Soient* U *une matrice carrée à coefficients dans un anneau commutatif* K *et*

$$p_U(X) = \det(U - X.1)$$

son polynôme caractéristique. On a alors

$$p_U(U) = 0.$$

Posons, si U est d'ordre n,

$$(-1)^n p_U(X) = X^n - \tau_1(U)X^{n-1} + \cdots + (-1)^n \tau_n(U)$$

comme au § 34, n° 3. Les coefficients $\tau_i(U)$ sont des polynômes à coefficients entiers rationnels en les éléments de U, polynômes dont les coefficients sont évidemment indépendants de U comme de l'anneau de base K : par exemple la formule

$$\tau_1(U) = \alpha_{11} + \cdots + \alpha_{nn}$$

permettant de calculer $\tau_1(U)$ en fonction des coefficients α_{ij} de U est la même pour toutes les matrices U de degré n et tous les anneaux commutatifs. Comme

$$(-1)^n p_U(U) = U^n - \tau_1(U)U^{n-1} + \cdots + (-1)^n \tau_n(U).1_n,$$

on voit donc qu'il existe des polynômes f_{ij} ($1 \leqslant i, j \leqslant n$) à coefficients *entiers rationnels*, à n^2 indéterminées X_{ij} ($1 \leqslant i, j \leqslant n$), tels que, pour tout anneau commutatif K et toute matrice

$$U = (\alpha_{ij})_{1 \leqslant i, j \leqslant n}$$

de degré n à coefficients dans K, les coefficients de la matrice $p_U(U)$ s'obtiennent en substituant les coefficients de U aux indéterminées dans les polynômes f_{ij}. Pour montrer que $p_U(U) = 0$, il suffit donc de montrer que les polynômes f_{ij} sont nuls, i.e. que leurs coefficients sont nuls, et pour cela (§ 28, Théorème 1) que chaque f_{ij} s'annule toutes les fois qu'on y remplace les indéterminées par des *entiers rationnels* arbitraires. Mais par construction même des f_{ij} cela signifie qu'on a $p_U(U) = 0$ pour toute matrice carrée à coefficients dans l'anneau **Z**.

Ainsi, pour établir le Théorème 1 pour *tout* anneau commutatif K, il suffit de l'établir pour l'anneau **Z**. Pour cela nous allons l'établir pour un corps K *algébriquement clos* quelconque; le Théorème sera alors établi pour **C**, donc pour le sous-anneau **Z** de **C**, donc dans tous les cas !

Pour cela considérons l'endomorphisme u de K^n ayant U pour matrice par rapport à la base canonique. En vertu du § 34, Théorème 3, il existe une base $(x_i)_{1 \leqslant i \leqslant n}$ de K^n telle que l'on ait des relations

$$(1) \qquad u(x_i) = \rho_{ii}x_i + \cdots + \rho_{i1}x_1 \quad (1 \leqslant i \leqslant n);$$

comme le déterminant d'une matrice triangulaire est le produit de ses termes diagonaux on a alors

$$p_U(X) = p_u(X) = (\rho_{11} - X) \ldots (\rho_{nn} - X),$$

et tout revient par conséquent, puisque $p_U(U)$ est évidemment la matrice (par rapport à la base canonique de K^n) de l'endomorphisme

$$p_u(u) = (\rho_{11} - u) \ldots (\rho_{nn} - u),$$

à montrer que celui-ci est nul. Or posons

$$u_i = \rho_{ii} - u;$$

il résulte de (1) que

$$u_j(x_i) = (\rho_{ii} - \rho_{jj})x_i + y_{ij}$$

où y_{ij} appartient au sous-espace vectoriel F_{i-1} de K^n engendré par les vecteurs $x_1, \ldots, x_{i-1}$, et il résulte aussitôt de ces formules que l'on a

$$u_i(F_i) \subset F_{i-1}$$

pour tout i. Pour en déduire que l'endomorphisme

$$v = p_u(u) = u_1 \circ \cdots \circ u_n$$

est nul, il suffit alors de remarquer que

$$v(K^n) = v(F_n) = u_1 \circ \cdots \circ u_{n-1} \circ u_n(F_n) \subset u_1 \circ \cdots \circ u_{n-1}(F_{n-1}) \subset \cdots \subset u_1(F_1)$$

et comme on a évidemment $u_1(F_1) = \{0\}$, le Théorème est établi.

Exemple 1. Si U est une matrice carrée d'ordre 2 à coefficients dans un anneau commutatif quelconque, on a

$$U^2 - \mathrm{Tr}(U).U + \text{dét}\,(U).1_2 = 0.$$

On conseille au lecteur de vérifier ce résultat par un calcul direct.

Remarque 1. Comme $p_U(X) = \text{dét}\,(U - X.1_n)$, le lecteur débutant et ingénieux aura sans doute l'idée de démontrer le Théorème 1 en écrivant que

$$p_U(U) = \text{dét}\,(U - U.1_n) = \text{dét}\,(U - U) = \text{dét}\,(0) = 0.$$

Cette démonstration séduisante repose malheureusement sur l'erreur qui consiste à croire que, lorsqu'on remplace dans $U - X.1_n$ l'indéterminée X par la matrice U, on trouve la matrice $U - U.1_n = 0$, ce qui n'est pas le cas; en effet, $U - X.1_n$ s'obtient en retranchant X aux termes diagonaux de U, et si l'on remplace X par U dans le résultat obtenu on trouve la matrice

$$\begin{pmatrix} \alpha_{11} - U & \alpha_{21} & \cdots & \alpha_{n1} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{1n} & \alpha_{2n} & \cdots & \alpha_{nn} - U \end{pmatrix}$$

à coefficients dans le sous-anneau commutatif de $M_n(K)$ engendré par K et U; or cette matrice n'est visiblement pas nulle en général ! Le théorème de Hamilton-Cayley affirme seulement que le *déterminant* de cette matrice est nul.

Cette *Remarque* montre qu'on peut être parfois induit en erreur par les notations qu'on utilise.

2. *Décomposition en endomorphismes nilpotents*

Le premier pas dans la démonstration du Théorème de Jordan consiste à établir le résultat suivant :

THÉORÈME 2. *Soit u un endomorphisme d'un espace vectoriel* E *de dimension finie sur un corps commutatif* K, *et supposons que le polynôme p_u ait toutes ses racines dans* K. *Posons*

$$p_u(X) = (\lambda_1 - X)^{r_1} \dots (\lambda_q - X)^{r_q}$$

où $\lambda_1, \dots, \lambda_q \in K$ sont les diverses racines de p_u et $r_1, \dots, r_q$ leurs ordres de multiplicité. Enfin, posons

$$E_i = \mathrm{Ker}\,[(u - \lambda_i)^{r_i}] \quad \text{pour} \quad 1 \leqslant i \leqslant q.$$

Alors E *est somme directe des sous-espaces* E_i, *et on a*

$$\dim(E_i) = r_i \quad \text{pour} \quad 1 \leqslant i \leqslant q.$$

Pour simplifier les notations, posons

$$p(X) = p_u(X), \qquad f_i(X) = (\lambda_i - X)^{r_i}$$
$$g_i(X) = f_1(X) \dots f_{i-1}(X) f_{i+1}(X) \dots f_q(X).$$

Comme les λ_i sont deux à deux distincts, les polynômes g_i ($1 \leqslant i \leqslant q$) sont premiers entre eux, et par suite il existe des polynômes $h_i \in K[X]$ tels que l'on ait

$$\sum_{1 \leqslant i \leqslant q} h_i(X) g_i(X) = 1.$$

Posant

$$u_i = f_i(u), \qquad v_i = g_i(u), \qquad w_i = h_i(u)$$

de sorte que les $3q$ endomorphismes de E ainsi obtenus commutent deux à deux (car ce sont tous des polynômes en u), on a donc

$$w_1 \circ v_1 + \dots + w_q \circ v_q = j_E,$$

endomorphisme identique de E. Ceci montre qu'on a

$$x = w_1(v_1(x)) + \dots + w_q(v_q(x)) \quad \text{pour tout } x \in E; \tag{a}$$

mais d'après le Théorème 1 on a

$$0 = p(u) = f_i(u) g_i(u) = u_i \circ v_i$$

pour tout i, et puisque u_i et w_i commutent il vient *a fortiori* $u_i \circ w_i \circ v_i = 0$. Ceci montre que

$$w_i(v_i(x)) \in E_i$$

pour tout i et tout x, et (a) prouve donc que

$$E = E_1 + \dots + E_q.$$

Il reste à montrer que la somme est directe et que $\dim(E_i) = r_i$; comme

$$r_1 + \dots + r_q = d^0(p_u) = \dim(E),$$

le Corollaire 3 du Théorème 13 du § 19 montre d'ailleurs qu'il suffit d'établir les relations

$$\dim(E_i) \leqslant r_i. \tag{3}$$

Or comme $E_i = \mathrm{Ker}\,(u_i)$ et comme u commute à u_i, il est clair que $u(E_i) \subset E_i$; désignant par u_i' l'endomorphisme de E_i induit par u, on voit donc (§ 34, *Remarque* 4) que le polynôme p_u est divisible par le polynôme $p_{u_i'}$. Comme le polynôme p_u a toutes ses racines dans K, il en est donc de même de $p_{u_i'}$, et par suite il existe une base de E_i par rapport à laquelle la matrice de u_i' est triangulaire (§ 34, Théorème 3); mais comme on a

$$(u_i' - \lambda_i)^{r_i} = 0$$

par construction même de E_i, les coefficients diagonaux de la matrice de u_i' par rapport à la base en question sont nécessairement égaux à λ_i, en sorte que

$$p_{u_i'}(X) = (\lambda_i - X)^{\dim(E_i)}.$$

Pour que ce polynôme divise p_u il est évidemment nécessaire que la relation (3) soit vérifiée, ce qui achève la démonstration.

Les scalaires $\lambda_1, \dots, \lambda_q$ sont naturellement les diverses *valeurs propres de u*. Le Théorème 2 montre que E est somme directe de sous-espaces E_i tels que l'on ait

$$u(E_i) \subset E_i, \qquad (u - \lambda_i)^{r_i} = 0 \ \text{ dans } \ E_i.$$

Comme on obtient une base de E en réunissant des bases des divers E_i, on voit que, pour mettre la matrice de u par rapport à une base de E sous une forme aussi simple que possible il suffit de se placer dans E_i et de résoudre le même problème pour l'endomorphisme de E_i induit par u ou, ce qui revient au même, par $u - \lambda_i$, lequel est **nilpotent,** ce qui veut dire que l'une de ses puissances est nulle.

Ainsi tout revient maintenant, étant donné un endomorphisme nilpotent d'un espace vectoriel, à choisir une base de celui-ci par rapport à laquelle la matrice de l'endomorphisme donné soit aussi simple que possible. C'est ce qu'on va faire dans le n° suivant.

3. *Structure des endomorphismes nilpotents*

Voici maintenant le second pas dans la démonstration du Théorème de Jordan :

THÉORÈME 3. *Soit u un endomorphisme d'un espace vectoriel* E *de dimension finie $n \geqslant 1$ sur un corps commutatif* K. *Supposons qu'il existe un entier $p \geqslant 0$ tel que*

$$u^p = 0$$

(i.e. que u soit nilpotent). *Il existe alors une base de* E *par rapport à laquelle la matrice de* u *est de la forme*

$$\begin{pmatrix} 0 & \nu_2 & 0 & \dots & 0 & 0 \\ 0 & 0 & \nu_3 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & \nu_n \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

où chaque scalaire ν_i *est égal à* 0 *ou à* 1.

On peut évidemment supposer $u \neq 0$, le Théorème étant trivial si $u = 0$. Il existe alors un entier $q \geqslant 1$ tel que

$$u^q \neq 0,\ u^{q+1} = 0;$$

pour tout entier $r \geqslant 0$, nous poserons d'autre part

$$\mathrm{E}_r = \mathrm{Ker}(u^r);$$

on a $\mathrm{E}_0 = \{0\}$ et $\mathrm{E}_{q+1} = \mathrm{E}$.

LEMME 1. *La suite de sous-espaces*

$$0 = \mathrm{E}_0 \subset \mathrm{E}_1 \subset \dots \subset \mathrm{E}_q \subset \mathrm{E}_{q+1} = \mathrm{E}$$

est strictement croissante, et on a $u(\mathrm{E}_{i+1}) \subset \mathrm{E}_i$ *pour tout* $i \geqslant 0$.

Si un vecteur x est annulé par l'endomorphisme u^{i+1}, il est clair que $u(x)$ est annulé par u^i, ce qui établit la seconde assertion de l'énoncé du Lemme 1. Il reste à établir que E_{i+1} contient strictement E_i pour $0 \leqslant i \leqslant q$. Tout d'abord, la relation

$$\mathrm{E}_{i+1} \supset \mathrm{E}_i$$

est triviale pour tout i. Supposons maintenant qu'on ait $\mathrm{E}_{i+1} = \mathrm{E}_i$ pour un indice i tel que $0 \leqslant i \leqslant q$; pour tout $x \in \mathrm{E}$, on a

$$0 = u^{q+1}(x) = u^{i+1}(u^{q-i}(x)),$$

donc $u^{q-i}(x) \in \mathrm{E}_{i+1}$; de $\mathrm{E}_{i+1} = \mathrm{E}_i$ résulterait donc que $u^{q-i}(x) \in \mathrm{E}_i$ pour tout $x \in \mathrm{E}$, donc que $u^q(x) = 0$ pour tout $x \in \mathrm{E}$, contrairement à la définition de q.

LEMME 2. *Soient* i *un entier tel que* $1 \leqslant i \leqslant q$ *et* F *un sous-espace vectoriel de* E *tel que* $\mathrm{F} \cap \mathrm{E}_i = \{0\}$; *on a alors* $u(\mathrm{F}) \cap \mathrm{E}_{i-1} = \{0\}$, *et* u *induit un isomorphisme de* F *sur* $u(\mathrm{F})$.

Considérons un vecteur $x \in u(\mathrm{F}) \cap \mathrm{E}_{i-1}$; il existe un $y \in \mathrm{F}$ tel que $x = u(y)$, et comme $u^{i-1}(x) = u^i(y)$ on voit que la relation $x \in u(\mathrm{F}) \cap \mathrm{E}_{i-1}$ implique $y \in \mathrm{F} \cap \mathrm{E}_i$, donc $y = 0$, donc $x = 0$. L'application de F dans $u(\mathrm{F})$ induite par u est évidemment linéaire et surjective; elle est injective, car si $y \in \mathrm{F}$ vérifie $u(y) = 0$, ce qui implique $u(y) \in \mathrm{E}_{i-1}$, le raisonnement précédent montre aussi que $y = 0$. Le lemme est donc établi.

LEMME 3. *Il existe des sous-espaces vectoriels* $\mathrm{F}_1, \dots, \mathrm{F}_{q+1}$ *de* E *qui possèdent les propriétés suivantes* :

a) E_i *est somme directe de* E_{i-1} *et de* F_i *pour tout* i *tel que* $1 \leqslant i \leqslant q+1$;

b) u *applique injectivement* F_i *dans* F_{i-1} *pour tout* i *tel que* $2 \leqslant i \leqslant q+1$.

On prend tout d'abord pour F_{q+1} un supplémentaire de E_q dans $\mathrm{E}_{q+1} = \mathrm{E}$; le sous-espace $u(\mathrm{F}_{q+1})$ est alors contenu dans E_q, et ne rencontre E_{q-1} qu'en 0 d'après le lemme 2; par suite, il existe un supplémentaire F_q de E_{q-1} dans E_q qui contient $u(\mathrm{F}_{q+1})$; d'après le lemme 1, le sous-espace $u(\mathrm{F}_q)$ est contenu dans E_{q-1}, et ne rencontre E_{q-2} qu'en 0 d'après le lemme 2; on peut donc construire un supplémentaire F_{q-1} de E_{q-2} dans E_{q-1} qui contienne $u(\mathrm{F}_q)$; en poursuivant la construction ainsi de suite, on forme évidemment des sous-espaces F_i vérifiant la condition *a)* et tels que $u(\mathrm{F}_i) \subset \mathrm{F}_{i-1}$; le fait que u applique *injectivement* F_i dans F_{i-1} résulte alors de la seconde assertion du Lemme 2.

Nous pouvons maintenant achever la *démonstration du Théorème* 3. Pour cela, construisons les sous-espaces F_i ($1 \leqslant i \leqslant q+1$) du Lemme 3. Désignons par

$$x_{11}, x_{12}, \dots, x_{1,r_1}$$

une base de F_{q+1}. Comme ces vecteurs sont linéairement indépendants, et que u applique *injectivement* F_{q+1} dans F_q, leurs images par u sont linéairement indépendantes, et font donc partie d'une base de F_q (§ 19, Théorème 2); autrement dit, il existe une base de F_q de la forme

$$x_{21}, x_{22}, \dots, x_{2,r_1}, x_{2,r_1+1}, \dots, x_{2,r_2}$$

avec

$$u(x_{1j}) = x_{2j} \quad \text{pour} \quad 1 \leqslant j \leqslant r_1.$$

En raisonnant de même à partir des vecteurs x_{2j}, on voit qu'il existe une base

$$x_{31}, \dots, x_{3,r_3}$$

de F_{q-1} telle que l'on ait

$$u(x_{2j}) = x_{3j} \quad \text{pour} \quad 1 \leqslant j \leqslant r_2.$$

En poursuivant ainsi de suite on parvient finalement à une base

$$x_{q+1,1}, \dots, x_{q+1,r_{q+1}}$$

de $\mathrm{F}_1 = \mathrm{E}_1$, telle que l'on ait des relations

$$u(x_{q,j}) = x_{q+1,j} \quad \text{pour } 1 \leqslant j \leqslant r_q;$$

et comme $\mathrm{E}_1 = \mathrm{Ker}\,(u)$ on a en outre

$$u(x_{q+1,j}) = 0 \quad \text{pour } 1 \leqslant j \leqslant r_{q+1}.$$

Ceci dit, et comme E est évidemment somme directe des sous-espaces $F_1, \ldots, F_{q+1}$, on voit que les $r_1 + r_2 + \cdots + r_{q+1}$ vecteurs x_{ij} ainsi construits forment une base de E. On peut écrire cette base sous la forme du tableau que voici :

$$\begin{array}{llll} x_{11} & \ldots & x_{1,r_1} & \\ u(x_{11}) & \ldots & u(x_{1,r_1}), & x_{2,r_1+1} \quad \ldots \quad x_{2,r_2} \\ \ldots & \ldots & \ldots & \ldots \\ u^q(x_{11}) & \ldots & u^q(x_{1,r_1}), & u^{q-1}(x_{2,r_1+1}) \quad \ldots \quad u^{q-1}(x_{2,r_2}) \quad \ldots \quad x_{q+1,r_{q+1}}. \end{array}$$

En écrivant ces vecteurs colonne par colonne, en commençant par le bas, on trouve donc une base $(x_i)_{1 \leqslant i \leqslant n}$ de E avec la propriété que, pour chaque i, on a

$$\text{soit} \quad u(x_i) = 0, \qquad \text{soit} \quad u(x_i) = x_{i-1};$$

la matrice de u par rapport à cette base possède alors la forme indiquée dans l'énoncé du Théorème 3.

4. *Le théorème de Jordan*

Avant d'énoncer le résultat final de ce §, introduisons la définition suivante : on appelle **matrice réduite** (ou **matrice de Jordan**) à coefficients dans un corps commutatif K toute matrice carrée à coefficients dans K qui est de la forme

$$\begin{pmatrix} \lambda & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & \lambda & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \lambda & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots & \lambda & 1 \\ 0 & 0 & 0 & 0 & \ldots & 0 & \lambda \end{pmatrix}$$

autrement dit dont tous les termes diagonaux sont égaux, qui comporte des 1 immédiatement au-dessus de la diagonale, et des 0 partout ailleurs.

Par exemple,

$$(\lambda), \qquad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}, \qquad \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}$$

sont des matrices réduites d'ordres 1, 2, 3 respectivement.

Cela dit :

THÉORÈME 4 (Jordan). *Soient* E *un espace vectoriel de dimension finie sur un corps commutatif* K *et* u *un endomorphisme de* E. *Les propriétés suivantes sont équivalentes :*

a) Toutes les valeurs propres de u *sont dans* K, i.e. le polynôme p_u a toutes ses racines dans K.

b) il existe une base de E *par rapport à laquelle la matrice de* u *est de la forme*

$$\begin{pmatrix} U_1 & 0 & 0 & \ldots & 0 \\ 0 & U_2 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & U_r \end{pmatrix}$$

où chaque U_i *est une matrice réduite à coefficients dans* K.

Supposons que toutes les valeurs propres de u soient dans K, et appliquons tout d'abord le Théorème 2 ; soit u_i la restriction de u à chaque E_i. Pour chaque i, supposons construite une base $(x_{ij})_{1 \leqslant j \leqslant n_i}$ de E_i par rapport à laquelle la matrice de u_i ait la forme indiquée dans l'énoncé du Théorème; alors, en superposant les bases des divers E_i ainsi obtenues, on trouve évidemment une base de E par rapport à laquelle la matrice de u a la forme cherchée. Tout revient donc à examiner u_i. Or on a

$$u_i = \lambda_i + v_i$$

où v_i est un endomorphisme *nilpotent* de E_i; il suffit donc de montrer qu'il existe une base de E_i par rapport à laquelle la matrice de v_i est un tableau diagonal de matrices réduites; pour cela, il suffit d'appliquer le Théorème 3 à v_i et à E_i, en formant une matrice réduite toutes les fois qu'on a une « chaîne » de coefficients v_i égaux à 1. Par exemple, la matrice

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

s'écrit

$$\begin{pmatrix} U_1 & 0 & 0 \\ 0 & U_2 & 0 \\ 0 & 0 & U_3 \end{pmatrix}$$

avec

$$U_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad U_2 = (0),$$

$$U_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Il est clair qu'on procédant ainsi on montre que *a*) implique *b*).

Pour montrer que *b*) implique *a*), on observe que, d'après le § 34, *Remarque* 4, la propriété *b*) implique

$$p_u(X) = p_{U_1}(X) \ldots p_{U_r}(X);$$

pour montrer que p_u a toutes ses racines dans K, il suffit donc de montrer qu'il en est ainsi de p_U lorsque U est une matrice réduite, ce qui est clair comme on l'a vu au § 34, n° 5. Le Théorème est donc démontré.

L'hypothèse *a*) du Théorème de Jordan, et donc aussi la propriété *b*), est toujours vérifiée lorsque le corps K est *algébriquement clos*. Dans le cas général, la condition *a*) signifie aussi (§ 34, Théorème 3) que *u* est *trigonalisable*.

Bien entendu, le Théorème de Jordan s'applique aussi aux matrices : si U est une matrice carrée d'ordre n à coefficients dans K, et si U a toutes ses valeurs propres dans K, il existe une matrice $P \in GL(n, K)$ telle que

$$PUP^{-1} = \begin{pmatrix} U_1 & 0 & 0 & \dots & 0 \\ 0 & U_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & U_r \end{pmatrix}$$

où les U_i sont des matrices de Jordan.

Exemple 2. Soit U une matrice carrée d'ordre 4 sur un corps K algébriquement clos. Alors U est semblable à une matrice ayant l'une des formes que voici :

$$\begin{pmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & \lambda_3 & 0 \\ 0 & 0 & 0 & \lambda_4 \end{pmatrix}; \quad \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda_3 & 0 \\ 0 & 0 & 0 & \lambda_4 \end{pmatrix}; \quad \begin{pmatrix} & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda_4 \end{pmatrix};$$

$$\begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \mu & 1 \\ 0 & 0 & 0 & \mu \end{pmatrix}; \quad \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}.$$

Il existe à première vue d'autres possibilités, mais elles se ramènent aux précédentes — par exemple la matrice

$$\begin{pmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix} \quad \text{est semblable à} \quad \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda_1 \end{pmatrix}$$

comme on le voit en effectuant une permutation des axes de coordonnées.

EXERCICES

Il est parfaitement utopique d'espérer apprendre des Mathématiques, si élémentaires ou si supérieures soient-elles, sans résoudre des Exercices.

Les Exercices qu'on trouvera dans ce livre sont de trois sortes. Certains sont des illustrations pratiques ou même numériques des théories exposées dans le texte; le lecteur débutant ne pourra pas acquérir la technique du calcul sans résoudre une partie appréciable des Exercices de ce genre. D'autres apportent au texte des compléments théoriques élémentaires; en les étudiant, le lecteur s'habituera à manipuler le langage et les modes de raisonnements utilisés dans le texte; ceux de ces Exercices qui ne sont pas *très* faciles sont précédés d'un signe ¶. Enfin, la dernière catégorie est constituée par des Exercices qui apportent au texte des compléments importants et difficiles; ils sont destinés uniquement aux étudiants déjà avancés qui s'intéressent vraiment aux Mathématiques; ces Exercices sont précédés de deux ou même trois signes ¶.

Nous ne saurions trop insister enfin sur le fait que résoudre un Exercice ne consiste pas seulement à se convaincre, à l'aide d'un « brouillon » fait à la hâte, du fait qu'on en a à peu près compris la solution; si cette méthode est admissible pour les Exercices de calcul numérique, il faut par contre s'efforcer de *rédiger intégralement* les Exercices plus théoriques, où l'on doit construire de véritables démonstrations. De cette façon, et uniquement de cette façon, l'étudiant parviendra à acquérir un langage clair et correct, et à utiliser les termes techniques dans leur sens propre, ce qui, en Mathématiques, est le signe le plus certain de la compréhension d'un sujet.

Pour chacune des matrices figurant dans les *Exercices* **1** à **14** ci-dessous, répondre aux questions suivantes : *a*) Calculer les valeurs propres (on prendra **C** pour corps de base). *b*) Pour chaque valeur propre, calculer les vecteurs propres correspondants dans $\mathbf{C}^n$ (on identifie chaque matrice carrée d'ordre n à coefficients complexes à un endomorphisme de $\mathbf{C}^n$). *c*) Trouver, s'il y a lieu, une base de $\mathbf{C}^n$ formée de vecteurs propres. *d*) Si la matrice considérée est diagonalisable sur **C**, déterminer le plus petit sous-corps de **C** sur lequel elle est diagonalisable. *e*) Si la matrice considérée n'est pas diagonalisable sur **C**, trouver une base de $\mathbf{C}^n$ par rapport à laquelle l'endomorphisme correspondant de $\mathbf{C}^n$ possède une matrice triangulaire.

1. $\begin{pmatrix} 5 & -3 & 2 \\ 6 & -4 & 4 \\ 4 & -4 & 5 \end{pmatrix}$

2. $\begin{pmatrix} 7 & -12 & 6 \\ 10 & -19 & 10 \\ 12 & -24 & 13 \end{pmatrix}$

3. $\begin{pmatrix} 4 & -5 & 7 \\ 1 & -4 & 9 \\ -4 & 0 & 5 \end{pmatrix}$

4. $\begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}$

5. $\begin{pmatrix} 9 & -6 & -2 \\ 18 & -12 & -3 \\ 18 & -9 & -6 \end{pmatrix}$

6. $\begin{pmatrix} 1 & -3 & 4 \\ 4 & -7 & 8 \\ 6 & -7 & 7 \end{pmatrix}$

7. $\begin{pmatrix} 4 & 6 & -15 \\ 3 & 4 & -12 \\ 2 & 3 & -8 \end{pmatrix}$

8. $\begin{pmatrix} 1 & -3 & 0 & 3 \\ -2 & -6 & 0 & 13 \\ 0 & -3 & 1 & 3 \\ -1 & -4 & 0 & 8 \end{pmatrix}$

9. $\begin{pmatrix} 3 & -4 & 0 & 2 \\ 4 & -5 & -2 & 4 \\ 0 & 0 & 3 & -2 \\ 0 & 0 & 2 & -1 \end{pmatrix}$

10. $\begin{pmatrix} 3 & -1 & 1 & -7 \\ 9 & -3 & -7 & -1 \\ 0 & 0 & 4 & -8 \\ 0 & 0 & 2 & -4 \end{pmatrix}$

11. $\begin{pmatrix} 0 & 0 & 2 & 3 \\ 0 & 0 & -2 & -3 \\ 2 & -2 & 0 & -1 \\ 3 & -3 & -1 & -3 \end{pmatrix}$

12. $\begin{pmatrix} 3 & 2 & 1 & -1 \\ 2 & 2 & 1 & -1 \\ 1 & 1 & 1 & 0 \\ -1 & -1 & 0 & 0 \end{pmatrix}$

13. $\begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ 1 & 2 & 0 & 0 & \dots & 0 \\ 1 & 2 & 3 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 2 & 3 & 4 & \dots & n \end{pmatrix}$

14. $\begin{pmatrix} 0 & a & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & a & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 0 & a \\ a & 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}$ (n lignes et colonnes)

15. Soient L un espace vectoriel de dimension finie sur un corps commutatif K et u un endomorphisme de L. Soient L* le dual de L et ${}^t u$ l'endomorphisme de L* transposé de u.

a) Montrer que les valeurs propres de u et de ${}^t u$ sont les mêmes.

b) Soit $\lambda \in K$ une valeur propre de u; on note $E(\lambda)$ l'ensemble des $x \in L$ tels que $u(x) = \lambda x$, et $F(\lambda)$ l'ensemble des $f \in L^*$ tels que ${}^t u(f) = \lambda f$. Montrer que

$$\dim E(\lambda) = \dim F(\lambda)$$

(utiliser le § 19, *Exercice* 12).

c) Montrer que les polynômes caractéristiques de u et de ${}^t u$ sont les mêmes.

(On peut en fait démontrer que toute matrice carrée à coefficients dans un corps commutatif K est semblable à sa transposée; cf. § 35, *Exercice* 10).

16. Soit $G = SL(2, \mathbf{R})$ le groupe des matrices

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

à coefficients *réels* et de déterminant

$$ad - bc = 1.$$

a) Si

$$|\mathrm{Tr}(X)| > 2,$$

il existe une matrice $U \in G$ telle que

$$UXU^{-1} = \begin{pmatrix} t & 0 \\ 0 & 1/t \end{pmatrix}$$

avec $t \in \mathbf{R}$, $t \neq 0, 1, -1$ (on dit alors que X est **hyperbolique**)

b) Si

$$|\mathrm{Tr}(X)| < 2,$$

il existe une matrice $U \in G$ telle que

$$UXU^{-1} = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

avec $t \in \mathbf{R}$ (on dit alors que X est **elliptique**).

c) Si $X \neq 1_2, -1_2$ et si

$$\mathrm{Tr}(X) = +2$$

il existe une matrice $U \in G$ telle que UXU^{-1} soit égale à l'une des matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix};$$

on dit alors que X est **parabolique**.

d) On désigne par K le sous-groupe de G formé des matrices de la forme

$$\begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

(t réel), et par T le sous-groupe de G formé des matrices de la forme

$$\begin{pmatrix} u & v \\ 0 & 1/u \end{pmatrix}$$

avec u, v réels et $u > 0$. Montrer que tout élément de G s'écrit, d'une façon et d'une seule, sous la forme XY avec $X \in K$ et $Y \in T$.

En déduire que l'on peut supposer $U \in K$ dans la question *a*), et $U \in T$ dans la question *b*).

17. Soit $G = SL(2, \mathbf{C})$ le groupe des matrices

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

à coefficients *complexes* et de déterminant

$$ad - bc = 1.$$

a) Montrer que, si

$$\mathrm{Tr}(X) \neq 2, -2$$

il existe une matrice $U \in G$ telle que

$$UXU^{-1} = \begin{pmatrix} t & 0 \\ 0 & 1/t \end{pmatrix}$$

avec $t \in \mathbf{C}$, $t \neq 0, 1, -1$.

b) Montrer que, si $X \neq 1_2$, resp. -1_2 et si

$$\mathrm{Tr}(X) = 2 \quad \text{resp} \quad -2$$

il existe une matrice $U \in G$ telle que

$$UXU^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{resp.} \quad \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}.$$

c) On désigne par K l'ensemble des matrices de la forme

$$\begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix}$$

où u et v sont des nombres complexes tels que

$$|u|^2 + |v|^2 = 1,$$

et par T l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de G telles que $c = 0$, et que a et d soient réels strictement positifs. Montrer que K et T sont des sous-groupes de G, et que tout élément de G se met, d'une façon et d'une seule, sous la forme XY avec $X \in K$ et $Y \in T$.

¶ **18.** Soit K un anneau commutatif. Étant donné un polynôme

$$f(X) = a_0 + a_1 X + \cdots + a_r X^r$$

à coefficients dans K, on définit

$$f(\Lambda) = a_0 . 1_n + a_1 \Lambda + \cdots + a_r \Lambda^r$$

pour toute matrice $\Lambda \in M_n(K)$.

a) Soient f, g deux polynômes à coefficients dans K; on pose

$$f + g = p, \qquad fg = q, \qquad f(g(X)) = r(X)$$

montrer que

$$p(A) = f(A) + g(A), \qquad q(A) = f(A)\,g(A) = g(A)\,f(A), \qquad r(A) = f(g(A)).$$

(On s'efforcera d'éviter *tout* calcul en utilisant de façon appropriée les résultats du § 28).

b) Montrer que

$$f(UAU^{-1}) = U.f(A).U^{-1}$$

si $A \in M_n(K)$ et $U \in GL(n, K)$.

c) On suppose A triangulaire et on désigne par $t_1, \ldots, t_n$ ses termes diagonaux. Montrer que $f(A)$ est triangulaire, et que ses termes diagonaux sont $f(t_1), \ldots, f(t_n)$.

d) On suppose que K est un corps. Soient $t_1, \ldots, t_n$ les valeurs propres de $A \in M_n(K)$ (prises dans une extension algébriquement close de K, et chaque valeur propre étant répétée autant de fois que sa multiplicité dans l'équation caractéristique de A; le lecteur pourra supposer $K = \mathbf{C}$ s'il ne s'intéresse pas au cas général).
Montrer que les valeurs propres de $f(A)$ sont $f(t_1), \ldots, f(t_n)$, et que

$$\det(f(A)) = f(t_1)\ldots f(t_n), \qquad \mathrm{Tr}(f(A)) = f(t_1) + \cdots + f(t_n).$$

¶ **19.** Soit

$$f(X) = a_1 + a_2X + \cdots + a_nX^{n-1}$$

un polynôme à coefficients complexes. Montrer que

$$\begin{vmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ a_n & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \ldots & a_{n-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_2 & a_3 & a_4 & \ldots & a_1 \end{vmatrix} = f(z_1)\ldots f(z_n)$$

où $z_1, \ldots, z_n$ sont les racines n^{es} de l'unité (**déterminants circulants**; utiliser l'*Exercice* précédent).
Appliquer ce résultat au calcul des déterminants

$$\begin{vmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{vmatrix}, \qquad \begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{vmatrix}.$$

20. Soit s une permutation des entiers $1, 2, \ldots, n$. On considère l'endomorphisme u_s de $\mathbf{C}^n$ donné par

$$u_s(e_i) = e_{s(i)} \quad (1 \leqslant i \leqslant n)$$

où $(e_i)_{1 \leqslant i \leqslant n}$ est la base canonique de $\mathbf{C}^n$. Utiliser la décomposition de s en cycles (§ 7, *Exercice* 24) pour calculer les valeurs propres de u_s, et montrer que u_s est diagonalisable.
On remplace dans ce qui précède $\mathbf{C}$ par un corps commutatif K algébriquement clos et de caractéristique $p \neq 0$; on prend $n = p$ et pour s une permutation circulaire. Montrer que u_s n'est pas diagonalisable.

21. Soient V un espace vectoriel de dimension finie sur un corps commutatif K et F un ensemble d'endomorphismes de V; on dit que F est **trigonalisable** (ou encore que la **réduction simultanée à la forme triangulaire** est possible pour F) s'il existe une base de V par rapport à laquelle la matrice de *tout* $u \in F$ soit triangulaire.

Soit V′ un sous-espace vectoriel de V **stable** par F, i.e. tel que l'on ait

$$u(V') \subset V' \quad \text{pour tout } u \in F$$

(au lieu de stable on dit aussi **invariant**); tout $u \in F$ induit donc un endomorphisme u' de V′ et un endomorphisme $\bar{u}$ de l'espace vectoriel quotient V/V′ (§ 12, *Exercice*). Soient F′ l'ensemble des u' et $\bar{F}$ l'ensemble des $\bar{u}$.
On suppose F′ trigonalisable dans V′, et $\bar{F}$ trigonalisable dans V/V′. Montrer que F est trigonalisable dans V (on construira une base dans V en imitant la démonstration du Théorème 1 du § 18).
Déduire de là une variante de la démonstration du Théorème 3 du § 34.

¶ **22.** Soient V un espace vectoriel de dimension finie sur un corps commutatif K algébriquement clos (on peut supposer $K = \mathbf{C}$, la démonstration est la même...) et F un ensemble d'endomorphismes de V *commutant deux à deux*. On se propose de démontrer que F est trigonalisable (*Exercice* précédent).

a) Pour tout $u \in F$ et toute valeur propre $\lambda \in K$ de u, soit $V_u(\lambda)$ le sous-espace des $x \in V$ tels que $u(x) = \lambda x$. Montrer que $V_u(\lambda)$ est stable par F.

b) Déduire de là que les $u \in F$ ont un vecteur propre commun dans V [utiliser la question *a*) pour raisonner par récurence sur dim (V)].

c) Terminer la démonstration en utilisant l'*Exercice* précédent.

d) On suppose en outre chaque $u \in F$ diagonalisable. Montrer qu'il existe une base de V par rapport à laquelle la matrice de *tout* $u \in F$ est diagonale (« réduction simultanée à la forme diagonale » pour des endomorphismes diagonalisables qui commutent deux à deux).

e) Montrer qu'au lieu de supposer K algébriquement clos il suffit de supposer que tout $u \in F$ est trigonalisable [ou, pour la question *d*), diagonalisable].

¶ **23.** Soient V un espace vectoriel de dimension finie sur un corps K et F un ensemble d'endomorphismes de V. On dit que F est **irréductible** si les seuls sous-espaces vectoriels de V stables par F sont $\{0\}$ et V.

a) Montrer que, si un endomorphisme f de V commute à tout $u \in F$, les sous-espaces vectoriels $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$, ainsi que les sous-espaces propres de f, sont stables par F.

b) On suppose F irréductible et K algébriquement clos. Démontrer que les seuls endomorphismes de V qui commutent à tout $u \in F$ sont les homothéties (lemme de Schur).

c) On suppose toujours F irréductible mais on ne fait plus d'hypothèse sur K. Montrer que les endomorphismes de V qui commutent à tout $u \in F$ forment un sous-corps (éventuellement non commutatif) de l'anneau des endomorphismes de V.

d) On prend $K = \mathbf{R}$ et $V = \mathbf{R}^4$. Choisir F de telle sorte que le sous-corps de la question précédente soit le corps des quaternions du § 15, *Exercice* 11.

¶ **24.** Soient V un espace vectoriel de dimension finie n sur un corps commutatif K de caractéristique zéro, et G un groupe *fini* d'automorphismes de V; on note r l'ordre de G.

a) Soit f un endomorphisme de V; montrer que l'endomorphisme

$$f^{\natural} = \frac{1}{r} \sum_{s \in G} s \circ f \circ s^{-1}$$

commute à tout $s \in G$, et qu'on a $f^{\natural} = f$ si et seulement si f commute aux éléments de G.
Montrer qu'on a

$$(f \circ g)^{\natural} = f^{\natural} \circ g$$

si g commute aux éléments de G.

b) Soit W un sous-espace vectoriel de V invariant par G. i.e. (*Exercice* 21) tel que $s(W) \subset W$ pour tout $s \in G$ (on montrera en passant qu'on a du reste $s(W) = W$ pour tout $s \in G$). On choisit (§ 17, Corollaire du Théorème 2 combiné avec le fait que W admet un supplémentaire dans V) un endomorphisme p de V tel que

$$p^2 = p, \qquad p(V) = W.$$

Montrer que

$$\mathrm{Im}(p^q) = W.$$

c) En considérant, dans la question *b*), le noyau de p^q, démontrer le théorème suivant : tout sous-espace de V *invariant par* G admet dans V un supplémentaire *invariant par* G.

d) Soient V un espace vectoriel de dimension finie sur un corps algébriquement clos de caractéristique 0 (par exemple $\mathbf{C}$) et G un groupe commutatif fini d'automorphismes de V. Montrer qu'il existe une base de V par rapport à laquelle la matrice de *tout* $s \in G$ est diagonale; si de plus G est d'ordre n, les coefficients diagonaux de ces matrices sont des racines n^{e} de l'unité. [On utilisera la question *b*) de l'*Exercice* 22].

e) Soit X une matrice carrée à coefficients dans un corps algébriquement clos de caractéristique 0; si

$$X^n = 1$$

pour un entier $n \geqslant 1$, alors X est diagonalisable. Montrer à l'aide d'un exemple que ce résultat ne s'étend pas aux corps de caractéristique $p \neq 0$.

f) Montrer que le résultat de la question *c*) est encore valable en caractéristique $p \neq 0$ pourvu que l'ordre r du groupe G ne soit pas multiple de p. Même résultat pour la question *d*).

¶ **25.** Soit V un espace vectoriel de dimension finie $n + 1$ sur un corps commutatif K algébriquement clos et de caractéristique 0. On considère trois endomorphismes u, v et h de V satisfaisant aux formules de commutation suivantes :

$$[h, u] = 2u, \qquad [h, v] = -2v, \qquad [u, v] = h$$

où l'on pose d'une façon générale $[f, g] = f \circ g - g \circ f$. On suppose enfin l'ensemble $\{u, v, h\}$ *irréductible*, i.e. que les seuls sous-espaces vectoriels de V stables à la fois par u, v et h sont $\{0\}$ et V.

a) Soient $x \in V$ et $\lambda \in K$ tels que $h(x) = \lambda x$. Montrer que le vecteur $y = u(x)$ vérifie $h(y) = (\lambda + 2)y$, et que le vecteur $z = v(x)$ vérifie $h(z) = (\lambda - 2)z$.

b) Montrer qu'il existe un vecteur $x \neq 0$ et un scalaire $\lambda \in K$ tels que l'on ait

$$h(x) = \lambda x, \qquad u(x) = 0.$$

c) Le vecteur x satisfaisant à la question *b*), on pose

$$x_k = v^k(x)/k\,! \quad (k \geqslant 0).$$

Démontrer les relations

$$\begin{aligned} h(x_k) &= (\lambda - 2k)x_k, \\ u(x_k) &= (\lambda - k + 1)x_{k-1}, \\ v(x_k) &= (k+1)x_{k+1}. \end{aligned}$$

d) En tenant compte de l'hypothèse d'irréductibilité faite au début, déduire de là que $\lambda = n$ et que les $n + 1$ vecteurs $x_0, x_1, \ldots, x_n$ forment une base de V. Quelles sont les matrices de u, v et h par rapport à cette base? Réciproque? Cas $n = 2$ ou 3?

e) On prend pour V l'espace vectoriel formé des polynômes de degré n au plus, à une indéterminée et à coefficients dans K. Montrer que la situation décrite dans les questions précédentes est effectivement réalisée si l'on définit u, v et h comme suit : u transforme chaque polynôme $f(X)$ en le polynôme $nXf(X) - X^2f'(X)$, v transforme chaque polynôme $f(X)$ en le polynôme $f'(X)$, et h transforme $f(X)$ en $-nf(X) + 2Xf'(X)$; on désigne naturellement par f' le polynôme dérivé de f.

¶ **26.** Soient V un espace vectoriel de dimension finie sur un corps K algébriquement clos de caractéristique 0 (par exemple $K = \mathbf{C}$), et u, v, w trois endomorphismes de V. On suppose

$$[u, w] = [v, w] = 0, \qquad [u, v] = w.$$

Montrer qu'il existe une base de V par rapport à laquelle les matrices de u, v et w sont triangulaires. Déterminer toutes les solutions u, v, w du problème lorsque V est de dimension 3.

¶¶ **27.** Soit V un espace vectoriel de dimension finie sur un corps commutatif K. Un ensemble F d'endomorphismes de V est appelé une **algèbre de Lie** (d'endomorphismes de V) si F est un espace vectoriel (i.e. si l'on a $\alpha u + \beta v \in F$ quels que soient $u, v \in F$ et $\alpha, \beta \in K$), et si de plus on a

$$u \circ v - v \circ u \in F \quad \text{quels que soient } u, v \in F.$$

(Exemple : prendre les combinaisons linéaires de u, v, h dans l'*Exercice* 25, ou de u, v et w dans l'*Exercice* 26).

On dit qu'une algèbre de Lie F d'endomorphismes de V est **résoluble** s'il existe une suite croissante

$$(*) \qquad \{0\} = F_0 \subset F_1 \subset \ldots \subset F_n = F$$

de sous-espaces vectoriels de F tels que l'on ait

$$(**) \qquad u \circ v - v \circ u \in F_{i-1} \quad \text{quels que soient } u, v \in F_i$$

pour tout i tel que $1 \leqslant i \leqslant n$. On se propose de démontrer que *si* K *est algébriquement clos et de caractéristique* 0 (par exemple si $K = \mathbf{C}$), *et si* F *est résoluble, il existe une base de* V *par rapport à laquelle la matrice de tout* $u \in F$ *est triangulaire* [Théorème de Lie, qui généralise le résultat *c*) de l'*Exercice* 22 ainsi que l'*Exercice* 26 comme on le voit facilement].

a) Démontrer le théorème dans le cas où $n = 1$ dans la suite (*).

b) Montrer que le terme F_{n-1} de (*) est une algèbre de Lie résoluble.

c) On suppose trouvé un vecteur $x \neq 0$ dans V tel que l'on ait une relation de la forme

$$(***) \qquad u(x) = \lambda(u).x \quad \text{pour tout } u \in F_{n-1}$$

(autrement dit, x est un vecteur propre commun aux $u \in F_{n-1}$). On prend un $v \in F_n$, et on pose $y = v(x)$. Montrer qu'on a

$$u(y) = \mu(u).y \quad \text{pour tout } u \in F_{n-1},$$

où $\mu(u)$ est un scalaire qu'on calculera. En remplaçant v par ξv dans le résultat obtenu (où ξ est un élément arbitraire de K), en conclure que

$$\mu(u) = \lambda(u) \quad \text{pour tout } u \in F_{n-1}.$$

d) On note $V(\lambda)$ le sous-espace de V formé des $x \in V$ vérifiant (***). Montrer qu'il est stable par tout $v \in F_n$, et que les restrictions à $V(\lambda)$ de deux éléments quelconques de F_n commutent

(utiliser l'*Exercice* 8 des §§ 12, 13, 14). En déduire que les $u \in F$ ont au moins un vecteur propre commun dans $V(\lambda)$.

e) Terminer la démonstration en raisonnant par récurrence sur la dimension de V (utiliser l'*Exercice* 21).

f) Où intervient l'hypothèse que le corps K est de caractéristique 0 ?

g) Montrer (avec les hypothèses indiquées sur K) que le théorème de Lie *caractérise* les algèbres de Lie *résolubles*.

¶ **28.** Pour qu'une matrice carrée X à coefficients dans un corps K algébriquement clos soit nilpotente, il faut et il suffit que toutes ses valeurs propres dans K soient nulles.
Montrer que, si K est de caractéristique 0 (par exemple si $K = C$) on peut remplacer cette condition par les relations

$$\mathrm{Tr}(X) = \mathrm{Tr}(X^2) = \cdots = \mathrm{Tr}(X^n) = 0,$$

où n est l'ordre de X.
Pour qu'une matrice U, à coefficients dans K, soit unipotente (i.e. pour que $1 - U$ soit nilpotente), il faut et il suffit que la seule valeur propre de U soit 1. Quel est le polynôme caractéristique de U ?
Montrer que, si K est de caractéristique $p \neq 0$, on peut remplacer cette condition par la suivante : il existe un entier $n \geqslant 0$ tel que

$$U^{p^n} = 1.$$

29. Soit A une matrice carrée inversible à coefficients dans un corps algébriquement clos. Montrer que les valeurs propres de l'inverse de A sont les inverses des valeurs propres de A, avec les mêmes multiplicités.

¶ **30.** Soit A une matrice carrée d'ordre n à coefficients dans un corps commutatif K. Soit f une fraction rationnelle à une indéterminée à coefficients dans K; on dit que A est **substituable** dans f s'il existe des polynômes p et q tels que l'on ait

$$f = p/q \qquad \text{et} \qquad \det(q(A)) \neq 0.$$

Montrer qu'alors la matrice

$$f(A) = p(A) \cdot q(A)^{-1}$$

est indépendante du choix de p et q (pourvu que p et q satisfassent aux conditions énoncées). On suppose K algébriquement clos, et on note $\lambda_1, \ldots, \lambda_n$ les valeurs propres de A (comptées avec leurs ordres de multiplicité). Montrer que, pour que A soit substituable dans f, il faut et il suffit que f soit définie en chaque λ_i; les valeurs propres de $f(A)$ sont alors $f(\lambda_1), \ldots, f(\lambda_n)$. (Utiliser l'*Exercice* 18).

31. Soient V un espace vectoriel de dimension finie sur un corps commutatif K, u un endomorphisme de V, et W un sous-espace vectoriel de V stable par u. Montrer que si u est diagonalisable (resp. trigonalisable) il en est de même de la restriction de u à W.

¶ **32.** Soient u et v deux endomorphismes d'un espace vectoriel V de dimension finie sur un corps commutatif. On suppose que u et v sont diagonalisables et commutent. Montrer que $v \circ u$ est diagonalisable.

¶¶ **33.** Soit K un corps commutatif. Étant donnée une matrice $U \in M_n(K)$, on considère l'application $f_U : M_n(K) \to M_n(K)$ donnée par

$$f_U(X) = UX - XU = [U, X] \qquad \text{pour tout } X \in M_n(K),$$

et on considère f_U comme un endomorphisme de l'espace vectoriel $M_n(K)$. Montrer que, pour que f_U soit diagonalisable, il faut et il suffit que U le soit.

34. Soient K un corps commutatif et n un entier. Montrer que, comme espace vectoriel sur K, l'anneau $M_n(K)$ admet une base formée de matrices X possédant la propriété suivante : pour toute matrice *diagonale* $H \in M_n(K)$, on a $[H, X] = \alpha(H).X$ où $\alpha(H)$ est un scalaire dépendant de H, et que l'on calculera.

¶ **35.** Soit V un espace vectoriel de dimension finie sur un corps commutatif K; on désigne par $T^p_q(V)$ l'espace vectoriel des tenseurs p fois covariants et q fois contravariants sur V (§ 21, *Exemple* 6). Soit u un *auto*morphisme de V; on considère l'automorphisme $T^p_q(u)$ de $T^p_q(V)$ défini au § 21, *Exercice* 1. Montrer que si u est diagonalisable, il en est de même de $T^p_q(u)$. Montrer de même que, si un endomorphisme u de V est diagonalisable, l'endomorphisme $D^p_q(u)$ de $T^p_q(u)$ défini au § 21, *Exercice* 1, est diagonalisable. Calculer, dans chacun de ces deux cas, les valeurs propres de l'endomorphisme considéré dans $T^p_q(V)$ en fonction de celles de u.

¶ **36.** Les notations restant celles de l'*Exercice* précédent, on choisit une base (a_i) de V et on désigne par G le groupe des automorphismes de V dont la matrice par rapport à la base choisie est triangulaire (resp. diagonale). Construire une base de l'espace $T^p_q(V)$ par rapport à laquelle la matrice de $T^p_q(u)$ est triangulaire (resp. diagonale) pour tout $u \in G$.

¶ **37.** Soient V un espace vectoriel de dimension finie sur un corps commutatif K, et $S_r(V)$ l'espace vectoriel formé par les fonctions polynomiales homogènes et de degré r sur V (§§ 27, 28, *Exercice* 17); on associe à chaque automorphisme u de V l'automorphisme u_r de $S_r(V)$ donné par $u_r(f) = f_0 u$.
Montrer que si u est diagonalisable (resp. trigonalisable) il en est de même de u_r; calculer les valeurs propres de u_r en fonction de celles de u.
En supposant u diagonalisable, calculer $\mathrm{Tr}(u_3)$ en fonction des coefficients du polynôme caractéristique de u. Le résultat obtenu s'étend-il à tout automorphisme u de V? Existe-t-il des formules analogues pour calculer $\mathrm{Tr}(u_r)$ quel que soit r?

38. Démontrer le Théorème 4 du § 34 sans utiliser le fait que les valeurs propres sont les racines d'une équation algébrique (écrire une relation linéaire non triviale entre $x_1, \ldots, x_n$, lui appliquer u, et en déduire une relation linéaire non triviale entre $n - 1$ des vecteurs $x_1, \ldots, x_n$).

39. Démontrer le Théorème 4 du § 34 en utilisant un déterminant de Vandermonde (§ 24, *Exercice* 15) (écrire une relation linéaire non triviale entre $x_1, \ldots, x_n$ et lui appliquer successivement $u, u^2, \ldots, u^{n-1}$).

¶ **40.** Soit $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$ une matrice carrée d'ordre n à coefficients dans un anneau K. Étant données deux parties H et K de l'ensemble $\{1, 2, \ldots, n\}$ on désigne par $A_{H,K}$ la matrice formée avec les termes a_{ij} de A pour lesquels on a $i \in H$ et $j \in K$.
Soit

$$(-1)^n p_A(X) = X^n - \tau_1(A)X^{n-1} + \tau_2(A)X^{n-2} - \ldots$$

(§ 34, n° 3, formule (9)). Démontrer que les coefficients $\tau_p(A)$ de ce polynôme sont donnés par la formule

$$\tau_p(A) = \Sigma \det(A_{H,H})$$

où la somme est étendue à toutes les parties H de $\{1, 2, \ldots, n\}$ telles que $\mathrm{Card}(H) = p$.

¶¶ **41.** Soient L un anneau commutatif et A un sous-anneau de L; un $x \in L$ est dit **entier sur** A s'il vérifie une équation de la forme

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

avec $a_{n-1}, \ldots, a_0 \in A$ (la condition que le coefficient de x^n est égal à 1 est essentielle si A n'est pas un corps). Un nombre complexe est appelé un **entier algébrique** s'il est entier sur le sous-anneau **Z** de **C**.

a) Dans ce qui précède on suppose que L est de type fini comme A-module. Soit $(m_i)_{1 \leqslant i \leqslant r}$ un système fini de générateurs du A-module L. Montrer que pour tout $x \in L$ il existe des $a_{ij} \in A$ tels que

$$xm_i = \sum_{j=1}^{j=r} a_{ij}m_j \quad (1 \leqslant i \leqslant r).$$

On pose

$$\begin{vmatrix} a_{11} - x & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} - x & \cdots & a_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r1} & a_{r2} & \cdots & a_{rr} - x \end{vmatrix} = d;$$

montrer que $dm_i = 0$ pour $1 \leqslant i \leqslant r$; en déduire que $d = 0$, puis que tout $x \in L$ est entier sur A.

b) L'anneau L n'étant plus supposé de type fini sur A, soient $x_1, \ldots, x_q$ des éléments de L entiers sur A. Montrer que le sous-anneau $A[x_1, \ldots, x_q]$ est un A-module de type fini.

c) Montrer que *l'ensemble* B *des* $x \in L$ *entiers sur* A *est un sous-anneau de* L. (On l'appelle la **clôture intégrale** de A dans L). Exemple : les entiers algébriques forment un sous-anneau de **C**, résultat dû à Dedekind (ainsi que le raisonnement ci-dessus).

d) Soient C un anneau commutatif, B un sous-anneau de C, et A un sous-anneau de B. On suppose tout $x \in C$ entier sur B, et tout $x \in B$ entier sur A. Montrer que tout $x \in C$ est entier sur A.

¶ **42.** Les valeurs propres d'une matrice carrée à coefficients entiers rationnels sont des entiers algébriques. Réciproquement, tout entier algébrique est valeur propre d'une matrice carrée à coefficients dans **Z**.

43. Tout nombre rationnel qui est un entier algébrique est un entier rationnel.

¶ **44.** On considère une extension quadratique

$$L = \mathbf{Q}[\sqrt{d}]$$

du corps des nombres rationnels; on suppose que d est un entier rationnel qui n'est divisible par le carré d'aucun nombre premier (on montrera en passant qu'on peut toujours ramener une extension quadratique de **Q** à être de ce type).

a) Pour qu'un élément $z = x + y\sqrt{d}$ de L soit entier sur **Z**, il faut et il suffit que

$$2x \in \mathbf{Z} \qquad \text{et} \qquad x^2 - y^2 d \in \mathbf{Z}$$

(observer que si z est un entier algébrique il en est de même de $\bar{z} = x - y\sqrt{d}$).

b) Soit B l'anneau des $z \in L$ entiers sur **Z**. Montrer que, comme groupe additif, L admet une base formée des deux éléments

$$1, \sqrt{d} \quad \text{si } d \equiv 2 \text{ ou } 3 \pmod 4$$
$$1, \frac{1+\sqrt{d}}{2} \quad \text{si } d \equiv 1 \pmod 4.$$

45. Montrer que tout nombre algébrique est le quotient d'un entier algébrique par un entier rationnel non nul.

¶¶ **46.** On dit qu'un anneau d'intégrité commutatif A est **intégralement clos** si tout élément du corps des fractions K de A qui est entier sur A appartient à A; exemple : l'anneau **Z** (*Exercice* 43).

a) On suppose que A est un anneau de valuation (i.e. qu'on a $x \in A$ ou $x^{-1} \in A$ pour tout $x \in K$, cf. § 8, *Exercice* 6). Montrer que A est intégralement clos.

b) Si A est intersection d'anneaux de valuation de son corps des fractions K, alors A est intégralement clos [NB — On peut démontrer la réciproque].

c) Tout anneau factoriel (§ 31, *Exercice* 21) est intégralement clos, de même que tout anneau de Dedekind (§§ 10, 11, *Exercice* 14 et § 18, *Exercice* 7).

d) Si A est intégralement clos et si $\mathfrak{p}$ est un idéal premier de A, l'anneau local $A_{\mathfrak{p}}$ [§ 29, *Exercice* 9, *e*) : $A_{\mathfrak{p}}$ est l'ensemble des $x \in K$ qui peuvent s'écrire sous la forme u/v avec $u, v \in A$ et $v \notin \mathfrak{p}$] est intégralement clos.

e) Soient A un anneau d'intégrité commutatif, K son corps des fractions et L une extension de K; alors la clôture intégrale de A dans L est un anneau intégralement clos.

¶¶ **47.** Soient A un anneau intégralement clos et K son corps des fractions.

a) Soient E une extension algébriquement close de K et x un élément de E entier sur A (donc algébrique sur K). Soit f le polynôme minimal (§ 32, *Exercices* 9 et 10) de x sur K. Montrer que toutes les racines de f dans E sont des entiers sur A. En conclure que les coefficients de f appartiennent à A. (Pour vérifier qu'un élément x algébrique sur K est entier sur A, il suffit donc d'examiner son équation minimale sur K).

b) Soit L une extension de degré fini de K. Montrer qu'on a

$$\mathrm{Tr}_{L/K}(x) \in A, \qquad \mathrm{N}_{L/K}(x) \in A$$

pour tout $x \in L$ entier sur A (*Exercices* 4 et 5 du § 26).

c) On suppose, dans la question *b*), que L est extension *séparable* de K (§ 26, *Exercice* 4; on rappelle que cette condition est toujours vérifiée en caractéristique nulle). Soient $(u_i)_{1 \leqslant i \leqslant n}$ une base de L formée d'éléments entiers sur A (on montrera qu'il existe de telles bases) et $(v_i)_{1 \leqslant i \leqslant n}$ la base complémentaire (§ 26, *Exercice* 4); soit B la clôture intégrale de A dans L. Montrer que les composantes par rapport à la base (v_i) de tout $x \in B$ sont dans A. En déduire que *le* A-*module* B *est de type fini si* A *est noethérien, et isomorphe à* A^n *si* A *est principal.*

¶¶ **48.** Soient L un corps de nombres algébriques (§ 26, *Exercice* 4) et B l'anneau des $x \in L$ entiers sur **Z** (on dit habituellement que B est l'**anneau des entiers de** L).

a) Montrer que le groupe additif B admet une base à n éléments, où $n = [L : \mathbf{Q}]$ (autrement dit, qu'il existe une base de **L** sur **Q** qui est en même temps une base du **Z**-module B).

b) Montrer que, pour tout idéal I de B, la relation $I \neq \{0\}$ implique $I \cap \mathbf{Z} \neq \{0\}$ (prendre un $x \in I$ et examiner le premier coefficient non nul de son équation minimale sur **Q**). En déduire que l'anneau quotient B/I est fini pour tout idéal non nul I de B.

c) Montrer que tout idéal premier $\mathfrak{p}$ non nul de B est maximal, que B/$\mathfrak{p}$ est un corps fini, et que $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$ où p est la caractéristique de B/$\mathfrak{p}$.

[Ces résultats classiques sont dus à Dedekind, et ceux de l'*Exercice* 47 en sont des généralisations faciles. Le fait que les corps B/$\mathfrak{p}$ soient finis explique en partie l'importance d'une étude générale des corps finis, d'autant plus que *tout* corps fini peut s'obtenir de cette façon. L'un des résultats fondamentaux de Dedekind, que Gauss et Kummer avaient cherché à obtenir avant lui, est que l'anneau des entiers d'un corps de nombres algébriques est un anneau de Dedekind (d'où la terminologie...), autrement dit que *tout idéal de l'anneau* B *s'écrit, d'une façon unique à des permutations près, comme produit d'idéaux premiers*. Les *Exercices* 49 et 50 ont pour but de donner une démonstration de ce fait. On utilisera uniquement le fait que B est un anneau *noethérien* [évident d'après la question *a*) de l'*Exercice* 48], *intégralement clos* [évident d'après la question *e*) de l'*Exercice* 46], *dont tout idéal premier non nul est maximal*.]

¶¶ **49.** Soient A un anneau d'intégrité commutatif et K son corps des fractions. On utilise dans ce qui suit la notion d'idéal fractionnaire de A définie au § 10, *Exercice* 14.

a) On dit qu'un idéal fractionnaire I de A est **divisoriel** s'il est l'intersection des idéaux fractionnaires principaux (i.e. de la forme Ax, avec $x \in K$, $x \neq 0$) qui le contiennent. Montrer que si I et J sont divisoriels il en est de même de $(I : J)$.

Montrer que tout $x \in (I : I)$ est entier sur A si A est noethérien, et en déduire que

$$(I : I) = A \quad \text{si A est noethérien et intégralement clos.}$$

b) On suppose A noethérien. Montrer qu'il existe au moins un idéal premier non nul de A qui est divisoriel (considérer l'ensemble des idéaux divisoriels I tels que $I \subset A$, $I \neq A$, et en prendre un élément maximal).

c) On suppose dorénavant que A est un anneau *local* (*), *noethérien, intégralement clos, et que le seul idéal premier non nul de* A *est l'unique idéal maximal* $\mathfrak{p}$ *de* A; un anneau de valuation discrète (§ 8, *Exercice* 6) vérifie ces conditions; on se propose d'établir la réciproque.

Montrer que $\mathfrak{p}$ est divisoriel, et en déduire que

$$(A : \mathfrak{p}) \neq A.$$

Montrer que, pour tout $x \in (A : \mathfrak{p})$, on a

$$x\mathfrak{p} = \mathfrak{p} \quad \text{ou} \quad x\mathfrak{p} = A;$$

en déduire que

$$(A : \mathfrak{p}).\mathfrak{p} = A$$

et par suite que l'idéal $\mathfrak{p}$ est *inversible*.

d) Montrer qu'on a $\mathfrak{p} \neq \mathfrak{p}^2$ et $\mathfrak{p} = Ax$ pour tout $x \in \mathfrak{p}$ n'appartenant pas à $\mathfrak{p}^2$.

e) Montrer que pour tout idéal $\mathfrak{a}$ de l'anneau A il existe un entier n tel que $\mathfrak{a}$ soit contenu dans $\mathfrak{p}^n$ mais non dans $\mathfrak{p}^{n+1}$. En utilisant le fait que $\mathfrak{p}$ est inversible, montrer que $\mathfrak{a} = \mathfrak{p}^n$ et en déduire que l'anneau A est principal.

f) Démontrer que A est l'anneau d'une valuation discrète.

¶ **50.** Soit A un anneau d'intégrité commutatif, de corps des fractions K. On suppose A noethérien et intégralement clos, et que tout idéal premier non nul de A est maximal; on se propose de montrer que A est un anneau de Dedekind, i.e. que tout idéal fractionnaire de A est inversible.

(*) On appelle *anneau local* tout anneau commutatif A tel que l'ensemble des éléments non inversibles de A soit un idéal $\mathfrak{p}$ de A. Cet idéal est alors l'unique idéal maximal de A, et si A est intègre le sous-anneau $A_{\mathfrak{p}}$ du corps des fractions de A est égal à A lui-même. Inversement, si A est un anneau d'intégrité, et si $\mathfrak{p}$ est un idéal premier de A, l'anneau $A_{\mathfrak{p}}$ est un anneau local. Les anneaux locaux servent principalement à étudier les propriétés d'une variété algébrique « au voisinage » d'un point donné, ce qui explique la terminologie adoptée pour les désigner.

a) Soit $\mathfrak{p}$ un idéal premier non nul de A; montrer, à l'aide de l'*Exercice* précédent, que l'anneau local $A_{\mathfrak{p}}$ est l'anneau d'une valuation discrète de K. Soit $v_{\mathfrak{p}}$ cette valuation, choisie de telle sorte que

$$v_{\mathfrak{p}}(K^*) = \mathbf{Z}.$$

Montrer que les éléments de A sont caractérisés par le fait qu'on a

$$v_{\mathfrak{p}}(x) \geqslant 0$$

pour tout idéal premier non nul $\mathfrak{p}$ de A.

b) Montrer que, pour tout $x \in K$ non nul, les $\mathfrak{p}$ tels que $v_{\mathfrak{p}}(x) \neq 0$ sont en nombre fini (se ramener au cas où $x \in A$ et appliquer l'*Exercice* 6 du § 18 à l'idéal Ax de A). Montrer qu'étant donnés des idéaux premiers $\mathfrak{p}$, $\mathfrak{p}_1$, ..., $\mathfrak{p}_r$ de A, deux à deux distincts et en nombre fini, et des entiers n_1, ..., n_r, il existe un $x \in A$ vérifiant les relations

$$v_{\mathfrak{p}}(x) = 0, \qquad v_{\mathfrak{p}_i}(x) \geqslant n_i \quad \text{pour} \quad 1 \leqslant i \leqslant r.$$

c) Montrer que, pour tout idéal premier non nul $\mathfrak{p}$ de A, il existe un $x \in K$ tel que

$$v_{\mathfrak{p}}(x) = -1, \qquad v_{\mathfrak{q}}(x) \geqslant 0 \quad \text{pour tout} \quad \mathfrak{q} \neq \mathfrak{p}$$

(choisir un x_0 vérifiant $v_{\mathfrak{p}}(x_0) = -1$, poser $x = x_0 y$, et déterminer y à l'aide de la question précédente).

d) Montrer que tout idéal premier non nul de A est inversible, puis que A est un anneau de Dedekind (cf. § 18, *Exercice* 7).

e) Soient A un anneau de Dedekind, L une extension séparable de degré fini du corps des fractions de A, et B la clôture intégrale de A dans L. Montrer que B est un anneau de Dedekind.

[Ce procédé, appliqué à $A = k[K]$ où k est un corps commutatif, conduit à des exemples d'anneaux de Dedekind tout à fait différents de ceux de la théorie des entiers algébriques].

f) Montrer que l'anneau $\mathbf{Z}[\sqrt{-5}]$ est un anneau de Dedekind, et que l'idéal engendré dans cet anneau par 3 et $1 + 2\sqrt{-5}$ est premier et non principal.

g) Soit k un corps commutatif algébriquement clos. On pose $A = k[X]$ (où X est une indéterminée sur k), $K = k(X)$, et

$$L = K[\sqrt{X^3 + pX + q}]$$

où p et q sont des éléments donnés de k (de sorte que L est une extension quadratique de K, correspondant à la « courbe du troisième degré » d'équation

$$y^2 = x^3 + px + q).$$

Trouver la clôture intégrale B de A dans L. Étant donné un $c \in k$, soit $\mathfrak{p}$ l'idéal premier (et maximal) de A formé des $f \in A$ tels que $f(c) = 0$; dans quel cas l'idéal $\mathfrak{p}B$ engendré par $\mathfrak{p}$ dans B est-il premier? S'il n'est pas premier, comment se décompose-t-il en produit de facteurs premiers?

¶¶¶ **51.** (Autre démonstration du Nullstellensatz de Hilbert, qui utilise l'*Exercice* 41).

Soit K un corps commutatif infini et soit

$$L = K[x_1, \ldots, x_n]$$

un anneau d'intégrité commutatif, contenant K et engendré par K et un nombre fini d'éléments $x_1, \ldots, x_n$.

a) On suppose qu'il existe une relation algébrique

$$f(x_1, \ldots, x_n) = 0$$

entre les x_i, où f est un polynôme non nul à n indéterminées et à coefficients dans K, de degré total r. Soit f_r la partie homogène de degré total r de f. Étant donnés des indéterminées $Z_1, \ldots, Z_{n-1}$, Y sur K et des éléments $c_1, \ldots, c_{n-1}$ de K, on pose

$$f(Z_1 + c_1Y, \ldots, Z_{n-1} + c_{n-1}Y, Y) = \sum_{0 \leqslant k \leqslant r} p_k(Z_1, \ldots, Z_{n-1})\, Y^k;$$

montrer que le polynôme p_r est donné par

$$p_r(Z_1, \ldots, Z_{n-1}) = f_r(c_1, \ldots, c_{n-1}, 1)$$

et est donc constant. Montrer qu'il existe $c_1, \ldots, c_{n-1} \in K$ tels que

$$f_r(c_1 \ldots, c_{n-1}, 1) \neq 0$$

(utiliser l'homogénéité de f_r et le Théorème 1 du § 28). Les $c_i \in K$ étant ainsi choisis, on pose

$$z_i = x_i + c_i x_n \quad (1 \leqslant i \leqslant n-1);$$

montrer que $L = K[z_1, \ldots, z_{n-1}, x_n]$ et que x_n est entier sur le sous-anneau $K[z_1, \ldots, z_{n-1}]$ de L.

b) Déduire de là le résultat suivant (« lemme de normalisation » d'Emmy Noether; il est encore valable si K est fini, mais la démonstration est alors notablement plus difficile) : si $L = K[x_1, \ldots, x_n]$ est un anneau d'intégrité à engendrement fini sur le corps K, et si les $x \in L$ ne sont pas tous algébriques sur K, il existe $d \leqslant n$ éléments $z_1, \ldots, z_d$ de L possédant les propriétés suivantes : (*i*) les z_j sont des combinaisons linéaires des x_i à coefficients dans K (*ii*) $z_1, \ldots, z_d$ sont algébriquement indépendants sur K (*iii*) chaque élément de L est *entier* sur le sous-anneau $K[z_1, \ldots, z_d]$ de L.

c) Montrer que, si les $x \in L$ ne sont pas tous algébriques sur K, l'anneau L ne peut pas être un corps (écrire que l'inverse de z_d dans L est entier sur le sous-anneau $K[z_1, \ldots, z_d]$ et en déduire une contradiction). Autrement dit : si un anneau L à engendrement fini sur un corps commutatif K est un corps, alors L est extension algébrique (de degré fini nécessairement) de K, et en particulier $L = K$ si K est algébriquement clos (d'où le Nullstellensatz : § 33, *Exercice* 33, (*e*).

§ 35

Mettre sous la forme de Jordan les matrices suivantes (on calculera dans chaque cas le changement de base permettant de se ramener à la forme de Jordan) :

1. $\begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}$ **2.** $\begin{pmatrix} 12 & -6 & -2 \\ 18 & -9 & -3 \\ 18 & -9 & -3 \end{pmatrix}$ **3.** $\begin{pmatrix} 1 & -3 & 3 \\ -2 & -6 & 13 \\ -1 & -4 & 8 \end{pmatrix}$

4. $\begin{pmatrix} 1 & -3 & 0 & 3 \\ -2 & -6 & 0 & 13 \\ 0 & -3 & 1 & 3 \\ -1 & -4 & 0 & 8 \end{pmatrix}$ **5.** $\begin{pmatrix} 3 & -1 & 1 & -7 \\ 9 & -3 & -7 & -1 \\ 0 & 0 & 4 & -8 \\ 0 & 0 & 2 & -4 \end{pmatrix}$ **6.** $\begin{pmatrix} 0 & 0 & 0 & \ldots & n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & n & n-1 & \ldots & 2 \\ n & n-1 & n-2 & \ldots & 1 \end{pmatrix}$

¶ **7.** Montrer que si

$$A = \begin{pmatrix} a & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & a & 1 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots & a & 1 \\ 0 & 0 & 0 & 0 & \ldots & 0 & a \end{pmatrix}$$

est une matrice de Jordan d'ordre n et si $f(X)$ est un polynôme à une variable, alors

$$f(A) = \begin{pmatrix} f(a) & f_1(a) & f_2(a) & \ldots & f_{n-1}(a) \\ 0 & f(a) & f_1(a) & \ldots & f_{n-2}(a) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & f(a) \end{pmatrix}$$

où l'on pose

$$f_k(a) = f^{(k)}(a)/k\,!$$

(ceci suppose le corps de base de caractéristique 0; que se passe-t-il en caractéristique p non nulle?)

¶ **8.** Soit A une matrice carrée à coefficients dans un corps commutatif K. Montrer, sans utiliser le théorème de Hamilton-Cayley, qu'il existe des polynômes non constants $f \in K[X]$ tels que $f(A) = 0$. Montrer que ce sont les multiples de celui d'entre eux qui possède le plus petit degré possible, et que celui-ci est unique si on impose à son coefficient dominant d'être égal à 1. On dit alors que c'est le **polynôme minimal de A sur K**; il divise le polynôme caractéristique de A, et est donc de degré au plus égal à l'ordre de A.

Montrer que si A est la matrice de Jordan de l'*Exercice* précédent, le polynôme minimal de A est

$$(X - a)^n.$$

Montrer que si

$$A = \begin{pmatrix} A' & 0 \\ 0 & A'' \end{pmatrix},$$

le polynôme minimal de A est le ppcm des polynômes minimaux de A′ et A″.
Montrer que deux matrices semblables A et PAP^{-1} ont le même polynôme minimal.
En supposant K algébriquement clos et en utilisant le théorème de Jordan, déduire des résultats précédents le calcul du polynôme minimal d'une matrice carrée quelconque.
Appliquer la méthode aux matrices des *Exercices* 1 à 6 ci-dessus.

9. Soient L un corps commutatif, K un sous-corps de L, et A une matrice carrée à coefficients dans K. Le polynôme minimal de A sur K est-il égal au polynôme minimal de A sur L?

¶¶ **10.** Soient k un corps commutatif, V un espace vectoriel de dimension finie sur k, et u un endomorphisme de V. On considère l'anneau de polynôme $K = k[X]$, le K-module V[X] défini dans l'*Exercice* 19 des §§ 27, 28, et enfin le K-module V_u de l'*Exercice* 20 des §§ 27, 28; étant donnés un $x \in V$ et un $f \in K$ on notera

$$f.x = f(u)(x)$$

le produit de x par f dans le module V_u; on note d'autre part $\tilde{u}$ l'endomorphisme du K-module V[X] donné par

$$\tilde{u}(m_0 + m_1X + \cdots) = u(m_0) + u(m_1)X + \cdots$$

quels que soient les $m_i \in V$ presque tous nuls.

a) On considère l'application

$$\theta : V[X] \to V_u$$

donnée par

$$\theta(m_0 + m_1X + m_2X^2 + \cdots) = m_0 + u(m_1) + u^2(m_2) + \cdots ;$$

montrer que c'est un homomorphisme de K-modules, et que θ est surjective.

b) Montrer que le noyau de θ est égal à l'image de l'endomorphisme

$$\tilde{u} - X.j$$

de V[X] (où j désigne l'application identique de V[X] dans lui-même; $X.j$ est donc l'homothétie de rapport X dans ce $k[X]$-module).

c) Soit $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$ la matrice de u par rapport à une base de V sur k; on considère la matrice

$$A - X.1_n = \begin{pmatrix} a_{11} - X & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} - X & \cdots & a_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} - X \end{pmatrix}$$

à coefficients dans l'anneau K; montrer, à l'aide de l'*Exercice* 15 du § 32, qu'il existe des matrices $P, Q \in GL_n(K)$ telles que

$$P(A - X.1_n)Q = \begin{pmatrix} d_1(X) & 0 & \cdots & 0 \\ 0 & d_2(X) & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d_n(X) \end{pmatrix}$$

où $d_1, \ldots, d_n$ sont des polynômes non nuls tels que chacun divise le suivant (on fera attention au fait qu'en général les coefficients de P et Q dépendent effectivement de X). Montrer que pour tout i, le polynôme $d_1 \ldots d_i$ est un pgcd des mineurs d'ordre i de $A - X.1_n$. Dans ce qui suit on suppose le coefficient dominant de chaque d_i égal à 1.

d) A l'aide de la question *b*) et de l'*Exercice* 15 du § 32, montrer que le K-module V_u est isomorphe au produit direct des modules quotients K/d_iK. On suppose

$$d_1 = \cdots = d_s = 1$$

et d_{s+1} non constant; on pose

$$d_i(X) = X^{n_i} - a_{i,n_i-1}X^{n_i-1} - \cdots - a_{i,0}$$

pour $s + 1 \leqslant i \leqslant n$; enfin on considère les matrices

$$A_i = \begin{pmatrix} 0 & 0 & 0 & \cdots & a_{i,0} \\ 1 & 0 & 0 & \cdots & a_{i,1} \\ 0 & 1 & 0 & \cdots & a_{i,2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & a_{i,n_i-1} \end{pmatrix};$$

montrer qu'il existe une base de V sur k telle que la matrice de u par rapport à cette base soit

$$\begin{pmatrix} A_{s+1} & 0 & \cdots & 0 \\ 0 & A_{s+2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & A_n \end{pmatrix}.$$

Montrer que d_n est le polynôme minimal de u.

e) On dit que $d_1(X), \ldots, d_n(X)$ sont les **invariants de similitude** de u (ou de la matrice A de u par rapport à une base quelconque de V sur k). Montrer que, pour que deux endomorphismes u et v de V soient semblables (i.e. pour qu'il existe un automorphisme w de V tel que $v = w \circ u \circ w^{-1}$) il faut et il suffit qu'ils aient les mêmes invariants de similitude. [Noter que si u et v sont semblables, et si A et B sont leurs matrices par rapport à une base quelconque de V, alors les matrices $A - X.1_n$ et $B - X.1_n$ sont équivalentes sur l'anneau $K = k[X]$, et appliquer le § 32, *Exercice* 15, *e*), ou bien utiliser la fin de la question *c*) ci-dessus].
Ou encore : soient A et B deux matrices carrées d'ordre n à coefficients dans un corps commutatif arbitraire k; pour qu'il existe une matrice $U \in GL(n, k)$ telle que

$$B = UAU^{-1},$$

il faut et il suffit que, pour $1 \leqslant i \leqslant n$, le pgcd des mineurs d'ordre i de la matrice $A - X.1_n$ soit égal au pgcd des mineurs d'ordre i de la matrice $B - X.1_n$.
(Corollaire immédiat : *toute matrice* $A \in M_n(k)$ *est semblable à sa transposée* ${}^tA$).

¶¶ **11.** Montrer que les matrices

$$\begin{pmatrix} 3 & 2 & -5 \\ 2 & 6 & -10 \\ 1 & 2 & -3 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 6 & 20 & -34 \\ 6 & 32 & -51 \\ 4 & 20 & -32 \end{pmatrix}$$

sont semblables en calculant leurs invariants de similitude. Même question pour

$$\begin{pmatrix} 4 & 10 & -19 & 4 \\ 1 & 6 & -8 & 3 \\ 1 & 4 & -6 & 2 \\ 0 & -1 & 1 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 41 & -4 & -26 & -7 \\ 14 & -13 & -91 & -18 \\ 40 & -4 & -25 & -8 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

¶¶ **12.** Soient L un corps commutatif, K un sous-corps de L, et A, B deux matrices carrées d'ordre n à coefficients dans K. On suppose A et B semblables comme matrices à coefficients dans L; montrer que A et B sont aussi semblables comme matrices à coefficients dans K (utiliser l'*Exercice* 10). Rapport avec l'*Exercice* 22 du § 27?

¶¶ **13.** Soit A une matrice carrée d'ordre n à coefficients dans un corps commutatif K; on suppose que le polynôme caractéristique de A a toutes ses racines dans K (i.e. que A est trigonalisable sur K). Montrer qu'il existe un tableau diagonal de matrices de Jordan sur K dont les invariants de similitude sont égaux à ceux de A. Déduire de là et de la question *e*) de l'*Exercice* 10 une nouvelle démonstration du théorème de Jordan.

¶ **14.** Soit A une matrice carrée *inversible* d'ordre n à coefficients dans un corps algébriquement clos K. Montrer qu'il existe dans $\mathrm{GL}(n, \mathrm{K})$ une matrice *diagonalisable* D et une matrice *unipotente* U telles que l'on ait

$$\mathrm{A} = \mathrm{DU} = \mathrm{UD},$$

et que de plus D et U sont uniques (se ramener à une matrice de Jordan). On dit que D et U sont les **composantes semi-simple et unipotente** de A [on peut démontrer que, si K est par exemple de caractéristique 0, ou fini, mais non nécessairement algébriquement clos, alors D et U, calculées dans une extension algébriquement close de K, sont encore à coefficients dans K; si par exemple $\mathrm{K} = \mathbf{R}$, il est clair que si $\mathrm{D}, \mathrm{U} \in \mathrm{M}_n(\mathbf{C})$ conviennent il en est encore même des matrices imaginaires conjuguées, et vu l'unicité de D et U on voit bien qu'on a en fait $\mathrm{D}, \mathrm{U} \in \mathrm{M}_n(\mathbf{R})$ dans ce cas. Naturellement, si K n'est pas algébriquement clos, D est semi-simple mais non nécessairement diagonalisable sur K.]

¶ **15.** Soit $\mathrm{X} \in \mathrm{M}_n(\mathrm{K})$ où K est algébriquement clos. Montrer qu'il existe une matrice diagonalisable D et une matrice nilpotente N telles que

$$\mathrm{X} = \mathrm{D} + \mathrm{N}, \qquad \mathrm{D}.\mathrm{N} = \mathrm{N}.\mathrm{D},$$

et que ces matrices sont entièrement déterminées par ces conditions. On prend $\mathrm{K} = \mathbf{C}$ et X à coefficients réels; montrer qu'il en est de même de D et N. (En fait, comme dans le cas précédent, on peut montrer que si X est à coefficients dans un sous-corps de caractéristique 0, ou fini, il en est de même de D et N.)

¶ **16.** On désigne par E l'ensemble de toutes les applications (*)

$$f : \mathbf{N} \to \mathbf{C}$$

qui vérifient la relation

$$(*) \qquad f(n+p) = a_{p-1} f(n+p-1) + \cdots + a_0 f(n) \quad \text{pour tout } n \in \mathbf{N},$$

où $a_0, \ldots, a_{p-1}$ sont des nombres complexes donnés.

a) Montrer qu'il existe une et une seule $f \in \mathrm{E}$ pour laquelle les nombres $f(0), \ldots, f(p-1)$ ont des valeurs données (on ne demande pas de calculer f explicitement). En déduire que E est un sous-espace vectoriel de dimension p de l'espace de toutes les applications de N dans C.

b) Pour $0 \leqslant i \leqslant p-1$, on désigne par e_i l'unique élément de E tel que l'on ait

$$e_i(j) = \begin{cases} 0 & \text{si } j \neq i \\ 1 & \text{si } j = i \end{cases} \quad \text{pour } 0 \leqslant j \leqslant p-1.$$

(*) Ces « applications » ne sont autres que les « suites » de nombres complexes, mais il est plus commode ici de les regarder comme des fonctions.

Montrer que $e_0, \ldots, e_{p-1}$ forment une base de E.

c) Montrer qu'il existe un et un seul endomorphisme u de E tel que, pour toute $f \in \mathrm{E}$, la fonction $g = u(f)$ soit donnée par

$$g(n) = f(n+1).$$

Calculer la matrice de u par rapport à la base $e_0, \ldots, e_{p-1}$ de E, et montrer que le polynôme caractéristique de u est, au signe près,

$$\mathrm{X}^p - a_{p-1}\mathrm{X}^{p-1} - \cdots - a_0.$$

d) Montrer que pour tout entier $r \geqslant 0$ et tout $\lambda \in \mathbf{C}$, le sous-espace

$$\mathrm{Ker}[(u-\lambda)^r]$$

de E est formé des $f \in \mathrm{E}$ qui sont de la forme

$$f(n) = \lambda^n g(n)$$

où la fonction g est polynomiale de degré $r-1$ au plus.

e) Soient $\lambda_1, \ldots, \lambda_h$ les diverses racines de l'équation

$$\lambda^p - a_{p-1}\lambda^{p-1} - \cdots - a_0 = 0,$$

et $r_1, \ldots, r_h$ leurs ordres de multiplicité. Montrer que, pour qu'une application f de N dans C soit dans E, i.e. vérifie la relation de récurence (*), il faut et il suffit qu'il existe des polynômes

$$g_1, \ldots, g_h \in \mathbf{C}[\mathrm{X}],$$

vérifiant

$$d^\circ(g_1) < r_1, \ \ldots, \ d^\circ(g_h) < r_h,$$

et tels que l'on ait

$$f(n) = g_1(n)\lambda_1^n + \cdots + g_h(n)\lambda_h^n \quad \text{pour tout } n \in \mathbf{N};$$

s'il en est ainsi, les polynômes $g_1, \ldots, g_h$ sont entièrement déterminés par f.

f) Trouver toutes les suites $(u_n)_{n \geqslant 0}$ de nombres complexes telles que l'on ait

$$u_{n+5} = u_{n+4} + 5u_{n+3} - u_{n+2} - 8u_{n+1} - 4u_n$$

pour tout $n \geqslant 0$.

¶ **17.** Soit $\mathrm{A} = (a_{ij})_{1 \leqslant i,\, j \leqslant p}$ une matrice carrée d'ordre p à coefficients complexes. Trouver toutes les applications

$$f = (f_1, \ldots, f_p) : \mathbf{N} \to \mathbf{C}^p$$

qui vérifient

$$f_i(n+1) = \sum_{j=1}^{j=p} a_{ij} f_j(n)$$

pour $1 \leqslant i \leqslant p$ et tout $n \in \mathbf{N}$ (Mettre A sous la forme de Jordan).

Utiliser les résultats obtenus pour retrouver ceux de l'*Exercice* précédent, en associant à toute solution de la relation (*) la fonction

$$(f(n), f(n+1), \ldots, f(n+p-1))$$

à valeurs dans $\mathbf{C}^p$.

¶ **18.** Trouver toutes les applications (f_1, f_2, f_3, f_4) de $\mathbf{N}$ dans $\mathbf{C}^4$ vérifiant les relations suivantes :

$$\begin{aligned} f_1(n+1) &= -5f_1(n) - 3f_2(n) - 2f_3(n) + 4f_4(n) \\ f_2(n+1) &= 2f_1(n) + f_3(n) - f_4(n) \\ f_3(n+1) &= 10f_1(n) + 7f_2(n) + 4f_3(n) - 9f_4(n) \\ f_4(n+1) &= 2f_1(n) + f_3(n) \end{aligned}$$

(utiliser l'*Exercice* précédent).

¶ **19.** Soit K un corps algébriquement clos et de caractéristique 0; dans cet *Exercice* (*), on considère des séries formelles à une indéterminée à coefficients dans K (§§ 27, 28, *Exercice* 11).

a) Étant donnée une série formelle

$$x = \sum_{n\in\mathbf{N}} f(n)\mathrm{T}^n/n!$$

en une indéterminée T, à coefficients dans K (de sorte que f est une application de l'ensemble $\mathbf{N}$ des entiers naturels dans K), on appelle **dérivée** de x la série formelle

$$x' = \sum_{n\in\mathbf{N}} f(n+1)\mathrm{T}^n/n!.$$

Montrer que l'application $x \to x'$ est une dérivation de l'anneau K[[T]]. Dans ce qui suit, on notera

$$x'' = (x')', \quad x''' = (x'')', \quad \ldots, \quad x^{(r)} = (x^{(r-1)})', \quad \ldots$$

les dérivées successives de x.

b) Étant données des constantes $a_0, \ldots, a_{p-1} \in \mathrm{K}$, montrer que la recherche des séries formelles

$$x = \sum_{n\in\mathbf{N}} f(n)\mathrm{T}^n/n!$$

vérifiant l'équation différentielle linéaire et homogène à coefficients constants

$$(**) \qquad x^{(p)} = a_{p-1}x^{(p-1)} + \cdots + a_0 x$$

revient à la résolution de l'équation (*) de l'*Exercice* 16.

c) Pour tout $\lambda \in \mathrm{K}$, on considère la série formelle

$$\exp(\lambda\mathrm{T}) = \sum_{n\in\mathbf{N}} \lambda^n \mathrm{T}^n/n!$$

(*) Le but de l'*Exercice* 19 et des suivants est de montrer au lecteur la liaison existant entre la théorie de la réduction des matrices et celle des systèmes d'équations différentielles. Il va de soi que, vu son importance, le sujet mériterait de beaucoup plus amples développements — mais ceux-ci appartiennent plus à un cours d'Analyse qu'à un cours d'Algèbre. L'intervention de séries formelles dans la théorie est conforme aux meilleures traditions, puisque la méthode de Cauchy-Kowalewska pour établir l'existence de solutions pour des systèmes d'équations différentielles à coefficients analytiques consiste d'abord à construire des séries entières qui vérifient « formellement » les équations données (autrement dit, à se placer, comme nous le faisons ici, dans le cadre des séries formelles, convergentes ou non), puis à démontrer, à l'aide de majorations de leurs coefficients, que ces séries formelles convergent. Dans le cas des systèmes étudiés ici, les démonstrations de convergence (lorsque $\mathrm{K} = \mathbf{C}$ bien entendu) sont triviales vu la forme particulièrement simple des séries obtenues.

(dont la définition est évidemment inspirée du développement en série entière de la fonction exponentielle classique). Étant donnée une série formelle

$$x = \Sigma f(n)\mathrm{T}^n/n!,$$

montrer que les propriétés suivantes sont équivalentes : (*i*) on a $f(n) = g(n)\lambda^n$ où g est une fonction polynomiale sur $\mathbf{N}$, à coefficients dans K, et de degré r; (*ii*) la série formelle x est produit de la série $\exp(\lambda\mathrm{T})$ par un polynôme de degré r en T, à coefficients dans K. (Il pourra être utile d'utiliser l'*Exercice* 8 des §§ 27, 28).

d) Soient $\lambda_1, \ldots, \lambda_h$ les racines dans K de l'équation

$$\lambda^p = a_{p-1}\lambda^{p-1} + \cdots + a_0$$

et $r_1, \ldots, r_h$ leurs ordres de multiplicité. Montrer que la solution générale de l'équation différentielle (**) est

$$x = g_1(\mathrm{T})\exp(\lambda_1\mathrm{T}) + \cdots + g_h(\mathrm{T})\exp(\lambda_h\mathrm{T})$$

où chaque g_i est un polynôme de degré $r_i - 1$ au plus à coefficients dans K.

e) On suppose $\mathrm{K} = \mathbf{C}$. Que resterait-il à faire pour déduire des résultats précédents la théorie classique des équations différentielles linéaires et homogènes à coefficients constants?

f) On cherche maintenant p séries formelles

$$x_i = \Sigma f_i(n)\mathrm{T}^n/n!$$

vérifiant le système

$$x_i' = \sum_{j=1}^{j=p} a_{ij}x_j$$

où les a_{ij} sont des éléments donnés de K. Montrer que la résolution de ce problème revient à celle de l'*Exercice* 17, et interpréter les résultats de l'*Exercice* 17 dans le langage de la théorie des systèmes d'équations différentielles.

Dans les *Exercices* suivants, on demande, en utilisant l'*Exercice* 19, *f*), de résoudre les systèmes différentiels donnés :

20.
$$\begin{aligned} x' &= 5x - 3y + 2z \\ y' &= 6x - 4y + 4z \\ z' &= 4x - 4y + 5z \end{aligned}$$

21.
$$\begin{aligned} x' &= 7x - 12y + 6z \\ y' &= 10x - 19y + 10z \\ z' &= 12x - 24y + 13z \end{aligned}$$

22.
$$\begin{aligned} x' &= x - 3y + 3z \\ y' &= -2x - 6y + 13z \\ z' &= -x - 4y + 8z \end{aligned}$$

23.
$$\begin{aligned} x' &= 3x - y \\ y' &= x + y \\ z' &= 3x + 5z - 3u \\ u' &= 4x - y + 3z - u \end{aligned}$$

24. Intégrer l'équation différentielle

$$x^{(5)} - x^{(4)} - 5x^{(3)} + x'' + 8x' + 4x = 0.$$

25. Utiliser l'*Exercice* 16 pour établir l'identité

$$\sum_{p=1}^{p=n} p^2 a^p = \frac{a(a+1)}{(1-a)^3} + \frac{(a-7)\,n - (2a^2 - 5a + 1)\,n^2}{2(1-a)^3}\,a^{n+1}$$

(on suppose $a \neq 1$).

26. Soient K un corps commutatif et n un entier positif. On désigne par V l'espace vectoriel (sur K) formé des polynômes à une indéterminée, à coefficients dans K, de degré au plus égal à n. Quelle est la dimension de V sur K? On désigne par D l'application de V dans V qui transforme chaque polynôme en le polynôme dérivé. Montrer que D est un endomorphisme nilpotent de V, et trouver une base de V sur K par rapport à laquelle la matrice de D ait la forme de Jordan.