§ 21

1. Soit V un espace vectoriel de dimension finie n sur un corps commutatif K ; quels que soient les entiers p, $q \geqslant 0$, on désigne par

$$\mathrm{T}^p_q(\mathrm{V})$$

l'espace vectoriel formé par les tenseurs p fois covariants et q fois contravariants sur V.

a) Soient $(a_i)_{1 \leqslant i \leqslant n}$ une base de V et $(a^j)_{1 \leqslant i \leqslant n}$ la base duale de V*. Montrer que les éléments

$$(*) \qquad a_{i_1} \otimes \cdots \otimes a_{i_p} \otimes a^{j_1} \otimes \cdots \otimes a^{j_q}$$

(où $i_1, \ldots, j_q$ prennent toutes les valeurs comprises entre 1 et n) forment une base de l'espace vectoriel $\mathrm{T}^p_q(\mathrm{V})$ [NB — On trouvera dans l'*Exemple* 6 du § 21 la règle pour identifier chaque $a \in \mathrm{V}$ à un tenseur d'espèce $\binom{1}{0}$; elle est essentielle pour donner un sens à l'expression (*) ci-dessus].

En déduire que $\mathrm{T}^p_q(\mathrm{V})$ est de dimension n^{p+q} sur K.

b) Soit u un *auto*morphisme de V. Étant donné un tenseur $f \in \mathrm{T}^p_q(\mathrm{V})$, on considère sur $(\mathrm{V}^*)^p \times \mathrm{V}^q$ la fonction f' donnée par

$$f'(y_1, \ldots, y_p, x_1, \ldots, x_q) = f[{}^t u(y_1), \ldots, {}^t u(y_p), u^{-1}(x_1), \ldots, u^{-1}(x_q)]$$

quels que soient les $y_i \in \mathrm{V}^*$ et les $x_i \in \mathrm{V}$. Montrer que $f' \in \mathrm{T}^p_q(\mathrm{V})$ et que l'application $f \to f'$ ainsi définie dans $\mathrm{T}^p_q(\mathrm{V})$ est linéaire. On désigne dans ce qui suit cette application par

$$\mathrm{T}^p_q(u).$$

Montrer que l'on a

$$\mathrm{T}^p_q(v \circ u) = \mathrm{T}^p_q(v) \circ \mathrm{T}^p_q(u)$$

quels que soient $u, v \in \mathrm{GL}(\mathrm{V})$. En déduire que l'application $u \to \mathrm{T}^p_q(u)$ est un homomorphisme du groupe des automorphismes de V dans le groupe des automorphismes de $\mathrm{T}^p_q(\mathrm{V})$.

On pose

$$u(a_i) = \sum_j \alpha^j_i a_j,$$

de sorte que $(\alpha^j_i)_{1 \leqslant i,j \leqslant n}$ est la matrice de u par rapport à la base (a_i) de V. Calculer la matrice de $\mathrm{T}^p_q(u)$ par rapport à la base de $\mathrm{T}^p_q(\mathrm{V})$ définie dans la question *a*).

c) Soit u un *endo*morphisme de V. Étant donné un tenseur $f \in \mathrm{T}^p_q(\mathrm{V})$, on définit une nouvelle fonction f'' sur $(\mathrm{V}^*)^p \times \mathrm{V}^q$ en posant

$$f''(y_1, \ldots, y_p, x_1, \ldots, x_q) = \sum_{1 \leqslant i \leqslant p} f[y_1, \ldots, y_{i-1}, {}^t u(y_i), y_{i+1}, \ldots, y_p, x_1, \ldots, x_q] - \sum_{1 \leqslant j \leqslant q} f[y_1, \ldots, y_p, x_1, \ldots, x_{j-1}, u(x_j), x_{j+1}, \ldots, x_q].$$

Montrer qu'on a encore $f'' \in \mathrm{T}^p_q(\mathrm{V})$ et que l'application $f \to f''$ de $\mathrm{T}^p_q(\mathrm{V})$ dans lui-même ainsi définie est linéaire. On la note dans ce qui suit $\mathrm{D}^p_q(u)$. Montrer qu'on a

$$\mathrm{D}^p_q(u + v) = \mathrm{D}^p_q(u) + \mathrm{D}^p_q(v)$$
$$\mathrm{D}^p_q(u \circ v - v \circ u) = \mathrm{D}^p_q(u) \circ \mathrm{D}^p_q(v) - \mathrm{D}^p_q(v) \circ \mathrm{D}^p_q(u)$$

quels que soient les endomorphismes u et v de V. Connaissant la matrice de u par rapport à la base (a_i) de V, calculer celle de $\mathrm{D}^p_q(u)$ par rapport à la base (*) de la question *a*).

¶ **2.** Soient V un espace vectoriel de dimension finie sur un corps commutatif K, et T un tenseur deux fois covariant et trois fois contravariant sur V. Montrer qu'il existe un et un seul tenseur U une fois covariant et deux fois contravariant sur V dont les composantes par rapport à toute base de V sont données, en fonction de celles de T, par la relation

$$\mathrm{U}^i_{jk} = \sum_{1 \leqslant h \leqslant n} \mathrm{T}^{ih}_{jkh}.$$

Interpréter cette opération (**contraction** du tenseur T par rapport au second indice covariant et au troisième indice contravariant) en regardant U et T comme des formes multilinéaires.

¶ **3.** Soit T un tenseur deux fois covariant et deux fois contravariant. Montrer que le scalaire

$$\sum_{1 \leqslant i,j \leqslant n} \mathrm{T}^{ij}_{ji}$$

est indépendant de la base choisie pour le définir.

¶¶ **4.** Soient L et M deux modules sur un anneau commutatif K. On considère le module

$$\mathrm{N} = \mathrm{K}^{(\mathrm{L} \times \mathrm{M})}$$

admettant pour base l'ensemble $\mathrm{L} \times \mathrm{M}$ (§§ 10, 11, *Exercice* 15) ; identifiant chaque élément de $\mathrm{L} \times \mathrm{M}$ à l'élément correspondant de N, on considère dans N le sous-module N' engendré par les éléments de N qui sont de la forme

$$(\lambda' x' + \lambda'' x'', \mu' y' + \mu'' y'') - \lambda'\mu'(x', y') - \lambda'\mu''(x', y'') - \lambda''\mu'(x'', y') - \lambda''\mu''(x'', y'').$$

On appelle **produit tensoriel des modules** L et M le module quotient N/N' ; on le désigne par la notation

$$\mathrm{L} \otimes \mathrm{M}.$$

Étant donnés des éléments $x \in \mathrm{L}$ et $y \in \mathrm{M}$, on désigne par

$$x \otimes y$$

l'élément de $\mathrm{L} \otimes \mathrm{M} = \mathrm{N}/\mathrm{N}'$ représenté par l'élément (x, y) de N.

a) Montrer que l'application

$$(x, y) \to x \otimes y$$

de $L \times M$ dans $L \otimes M$ est *bilinéaire*, et que les « produits » $x \otimes y$ engendrent le module $L \otimes M$.

b) Soit f une application de $L \times M$ dans un K-module quelconque E. Montrer que, pour que f soit *bilinéaire*, il faut et il suffit qu'il existe une application *linéaire*

$$\bar{f} : L \otimes M \to E$$

telle que l'on ait

$$f(x, y) = \bar{f}(x \otimes y)$$

quels que soient $x \in L$ et $y \in M$; l'application $\bar{f}$ est alors unique. (Ce résultat est la propriété fondamentale des produits tensoriels de modules : ils servent à ramener l'étude des applications bilinéaires à celle des applications linéaires).

c) On suppose L et M libres de type fini; soient $(a_i)_{1 \leqslant i \leqslant p}$ une base de L et $(b_j)_{1 \leqslant j \leqslant q}$ une base de M; montrer que les produits

$$a_i \otimes b_j \qquad (1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q)$$

forment une base de $L \otimes M$. En déduire que

$$\dim(L \otimes M) = \dim(L) . \dim(M)$$

si K est un corps.

d) Montrer qu'il existe un isomorphisme et un seul de $L \otimes M$ sur $M \otimes L$ qui applique $x \otimes y$ sur $y \otimes x$ quels que soient $x \in L$ et $y \in M$.

e) Soient L, M, L′ et M′ quatre modules sur K; on considère des homomorphismes

$$u : L \to L' \qquad \text{et} \qquad v : M \to M';$$

montrer qu'il existe un et un seul homomorphisme

$$f : L \otimes M \to L' \otimes M'$$

tel que l'on ait

$$f(x \otimes y) = u(x) \otimes v(y)$$

quels que soient $x \in L$ et $y \in M$ (observer que le second membre est fonction bilinéaire de x et y). On dit que f est le produit tensoriel des homomorphismes u et v, et on le note généralement $u \otimes v$. [Cette notation traditionnelle peut prêter à confusion, car elle désigne aussi un élément du module

$$\mathrm{Hom}(L, L') \otimes \mathrm{Hom}(M, M');$$

en pratique, on n'a presque jamais à considérer ce dernier produit tensoriel, et $u \otimes v$ a toujours la signification définie plus haut.]

f) On suppose L, ..., M′ libres de type fini; on choisit des bases de ces modules, donc (question *c*) ci-dessus) de $L \otimes M$ et $L' \otimes M'$; calculer la matrice de $u \otimes v$ par rapport à ces bases en fonction des matrices de u et v par rapport aux bases choisies dans L, ..., M′. [Le résultat obtenu conduit à la notion de **produit tensoriel de deux matrices**; soient

$$A = (a_{ij})_{1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q} \qquad \text{et} \qquad B = (b_{kh})_{1 \leqslant k \leqslant m,\ 1 \leqslant h \leqslant n}$$

deux matrices à coefficients dans un anneau commutatif K. On appelle produit tensoriel de A et B la matrice à pm colonnes et qn lignes définie comme suit : on numérote les colonnes du produit tensoriel à l'aide des couples (i, k) tels que $1 \leqslant i \leqslant p$, $1 \leqslant k \leqslant m$, et les lignes à l'aide

des couples (j, h) tels que $1 \leqslant j \leqslant q$, $1 \leqslant h \leqslant n$; cela dit, le terme de la matrice produit tensoriel

$$A \otimes B$$

situé à l'intersection de la colonne d'indice (i, k) et de la ligne d'indice (j, h) est par définition

$$a_{ij} b_{kh}.$$

Par exemple :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} u & v \\ u' & v' \\ u'' & v'' \end{pmatrix} = \begin{pmatrix} au & av & bu & bv \\ cu & cv & du & dv \\ au' & av' & bu' & bv' \\ cu' & cv' & du' & dv' \\ au'' & av'' & bu'' & bv'' \\ cu'' & cv'' & du'' & dv'' \end{pmatrix};$$

on utilise, pour ordonner les couples d'entiers (i, k), l'ordre lexicographique, qui consiste à convenir que (i, j) précède (k, h) si $i \leqslant k$, ou bien si $i = k$ et $j \leqslant h$.]

g) Soient L, L′, L″, M, M′ et M″ six modules sur l'anneau K; on prend des homomorphismes

$$u' : L \to L', \qquad u'' : L' \to L'', \qquad v' : M \to M', \qquad v'' : M' \to M'';$$

montrer qu'on a

$$(u'' \circ u') \otimes (v'' \circ v') = (u'' \otimes v'') \circ (u' \otimes v').$$

En déduire que si A′, A″, B′, B″ sont des matrices à coefficients dans K, la formule

$$(A''A') \otimes (B''B') = (A'' \otimes B'') . (A' \otimes B')$$

est vraie pourvu qu'elle ait un sens.

h) Soient L, M et N trois modules. Montrer qu'il existe un et un seul isomorphisme

$$(L \otimes M) \otimes N \to L \otimes (M \otimes N)$$

qui, quels que soient $x \in L$, $y \in M$ et $z \in N$, applique $(x \otimes y) \otimes z$ sur $x \otimes (y \otimes z)$. [« Associativité » du produit tensoriel; dans la pratique on ne fait aucune différence entre $(x \otimes y) \otimes z$ et $x \otimes (y \otimes z)$, qu'on écrit $x \otimes y \otimes z$].

i) Soient $M_1, \ldots, M_p$ des modules sur K; on forme le module

$$M_1 \otimes M_2 \otimes \cdots \otimes M_p = M_1 \otimes (M_2 \otimes \cdots \otimes M_p)$$

(définition par récurence sur p). Soit f une application de $M_1 \times M_2 \times \cdots \times M_p$ dans un K-module N. Montrer que, pour que f soit p-linéaire, il faut et il suffit qu'il existe un *homomorphisme* de modules

$$\bar{f} : M_1 \otimes \cdots \otimes M_p \to N$$

tel que l'on ait

$$f(x_1, \ldots, x_p) = \bar{f}(x_1 \otimes \cdots \otimes x_p)$$

quels que soient les $x_i \in M_i$; l'application linéaire $\bar{f}$ est alors entièrement déterminée par f (raisonner par récurrence sur p en attribuant une valeur fixe à l'une des variables figurant dans f).

j) Soit M un K-module; on considère le module

$$M \otimes M \otimes M^*$$

où M^* est le dual de M; à l'aide de la question précédente, montrer qu'il existe un et un seul homomorphisme

$$j : M \otimes M \otimes M^* \to T_1^2(M)$$

de $M \otimes M \otimes M^*$ dans le module des tenseurs 2 fois covariants et une fois contravariants sur M qui, quels que soient $x, y \in M$ et $u \in M^*$, applique l'élément

$$x \otimes y \otimes u \in M \otimes M \otimes M^*$$

sur l'élément

$$x \otimes y \otimes u \in T_1^2(M)$$

[on rappelle, *Exemple* 7 du § 21, que cette dernière expression est la forme trilinéaire sur $M^* \times M^* \times M$ dont la valeur en $(f, g, z) \in M^* \times M^* \times M$ est l'élément

$$f(x)\, g(y)\, u(z)$$

de K]. Montrer que *j est bijectif si* M *est libre de type fini.* Généraliser ce résultat en remplaçant

$$M \otimes M \otimes M^* \quad \text{par} \quad M \otimes \cdots \otimes M \otimes M^* \otimes \cdots \otimes M^*$$

(p facteurs M et q facteurs M^*) et

$$T_1^2(M) \quad \text{par} \quad T_q^p(M),$$

défini au début de l'*Exercice* 1 ci-dessus.

k) On prend $K = \mathbf{Z}$ et $M = \mathbf{Z}/p\mathbf{Z}$; montrer que $T_0^2(M)$ est réduit à 0, mais qu'il n'en est pas ainsi de $M \otimes M$ [considérer l'application $(x, y) \to xy$ de $M \times M$ dans M, multiplication des entiers modulo p]. En conclure que dans ce cas l'homomorphisme j de la question précédente n'est pas bijectif (et est même nul...).

[La notion de produit tensoriel de deux modules définie dans cet *Exercice* est beaucoup plus utile que celle de tenseur définie au § 21, sauf lorsqu'il s'agit de modules libres de type fini. La raison en est que les tenseurs du § 21 sont adaptés à l'étude des applications multilinéaires *dans l'anneau de base* K lui-même, tandis que les produits tensoriels de l'*Exercice* 21 servent à étudier les applications multilinéaires *dans des* K-*modules quelconques*. Or il peut arriver, cf. la question (*k*) de l'*Exercice* 21, que les premières soient toutes identiquement nulles, sans qu'il en soit de même des secondes. Notons enfin que le produit tensoriel, lorsqu'il s'agit de matrices ou d'espaces vectoriels de dimension finie, remonte essentiellement à Kronecker; pour cette raison, certains auteurs l'appellent le **produit kroneckerien.**]

§ 22

Calculer les déterminants suivants.

1. $\begin{vmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{vmatrix}$

2. $\begin{vmatrix} 2\sin t\cos t & 2\sin^2 t - 1 \\ 2\cos^2 t - 1 & 2\sin t\cos t \end{vmatrix}$

3. $\begin{vmatrix} 4 & -3 & 5 \\ 3 & -2 & 8 \\ 1 & -7 & -5 \end{vmatrix}$

4. $\begin{vmatrix} 3 & 4 & -5 \\ 8 & 7 & -2 \\ 2 & -1 & 8 \end{vmatrix}$

5. $\begin{vmatrix} x^2+1 & xy & xz \\ xy & y^2+1 & yz \\ xz & yz & z^2+1 \end{vmatrix}$

6. $\begin{vmatrix} \cos a & \sin a\cos b & \sin a\sin b \\ -\sin a & \cos a\cos b & \cos a\sin b \\ 0 & -\sin b & \cos b \end{vmatrix}$

7. $\begin{vmatrix} 1 & 0 & 1+i \\ 0 & 1 & i \\ 1-i & -i & 1 \end{vmatrix}$

8. $\begin{vmatrix} 1 & 1 & 1 \\ 1 & z & z^2 \\ 1 & z^2 & z \end{vmatrix}$ où $z = \cos(4\pi/3) + i\sin(4\pi/3)$

9. $\begin{vmatrix} \sin^2 a & \cos 2a & \cos^2 a \\ \sin^2 b & \cos 2b & \cos^2 b \\ \sin^2 c & \cos 2c & \cos^2 c \end{vmatrix}$

10. $\begin{vmatrix} 1 & a & a^4 \\ 1 & b & b^4 \\ 1 & c & c^4 \end{vmatrix}$

11. $\begin{vmatrix} 1 & x & x^2 \\ 1 & y & y^2 \\ 1 & z & z^2 \end{vmatrix}$

12. $\begin{vmatrix} x+a & b & c \\ a & x+b & c \\ a & b & x+c \end{vmatrix}$

13. $\begin{vmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{vmatrix}$

14. $\begin{vmatrix} a & b & c \\ a & x & c \\ a & b & x \end{vmatrix}$

15. $\begin{vmatrix} ab & ab' & ab'' \\ a'b & a'b' & a'b'' \\ a''b & a''b' & a''b'' \end{vmatrix}$

16. $\begin{vmatrix} 1 & x & x^3 \\ a & 1 & x \\ b & c & 1 \end{vmatrix}$

¶ **17.** Soient V un espace vectoriel de dimension n sur un corps commutatif K, et f une forme bilinéaire *alternée* sur V. On suppose que le seul vecteur $a \in V$ tel que

$$f(a, x) = 0 \quad \text{pour tout } x \in V$$

est $a = 0$ (on dit alors que f est **non dégénérée**).

a) Soit A la matrice formée par les coefficients $a_{ij} = f(a_i, a_j)$ de f par rapport à une base (a_i) de V. Montrer que, pour que f soit non dégénérée, il faut et il suffit que A soit inversible (utiliser le Théorème 2 du § 20).

b) Soient $a, b \in V$ tels que $f(a, b) \neq 0$. On pose $f_a(x) = f(a, x)$ et $f_b(x) = f(b, x)$; montrer que f_a et f_b sont des formes linéaires non proportionnelles sur V, et que les $x \in V$ tels que

$$(*) \qquad f(a, x) = f(b, x) = 0$$

forment un sous-espace vectoriel de dimension $n - 2$ de V.

c) Les hypothèses restant celles de *b*), montrer que V est somme directe du plan engendré par a et b et du sous-espace V′ des solutions de (*). Montrer que la restriction de f à V′ est non dégénérée.

d) En raisonnant par récurrence sur n, montrer *i*) que s'il existe sur V une forme bilinéaire alternée non dégénérée alors la dimension de V est paire *ii*) que si f est une forme bilinéaire alternée non dégénérée sur un espace vectoriel V de dimension $2p$, il existe une base de V par rapport à laquelle la matrice de f est

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

où 0_p désigne la matrice nulle à p lignes et p colonnes.

e) Une matrice carrée $A = (\alpha_{ij})_{1 \leq i, j \leq n}$ à coefficients dans K est dite **alternée** ou **antisymétrique** si elle vérifie les relations

$$\alpha_{ii} = 0, \qquad \alpha_{ij} + \alpha_{ji} = 0.$$

Montrer qu'une telle matrice ne peut être inversible si n est impair. Si A est inversible et si $n = 2p$, il existe une matrice $U \in GL(n, K)$ telle que

$$UA{}^tU = \begin{pmatrix} 0_p & 1_p \\ -1_p & 0_p \end{pmatrix}.$$

f) Montrer que

$$\begin{vmatrix} 0 & x & z \\ -x & 0 & y \\ -z & -y & 0 \end{vmatrix} = 0$$

quels que soient $x, y, z \in K$.

18. Soient f, g, h trois formes linéaires sur un espace vectoriel V sur un corps commutatif K. Montrer que, pour que f, g, h soient linéairement indépendantes, il faut et il suffit que

$$f \wedge g \wedge h \neq 0.$$

19. Soient V un espace vectoriel de dimension n sur un corps commutatif K, $(a_i)_{1 \leq i \leq n}$ une base de V, et f, g, h trois formes linéaires sur V. Montrer que les coefficients de $f \wedge g \wedge h$ par rapport à la base (a_i) sont les scalaires

$$\alpha_{ijk} = \begin{vmatrix} f(a_i) & f(a_j) & f(a_k) \\ g(a_i) & g(a_j) & g(a_k) \\ h(a_i) & h(a_j) & h(a_k) \end{vmatrix}$$

20. Soient V un espace vectoriel de dimension finie sur un corps commutatif, (a_i) une base de V, f une forme bilinéaire alternée sur V, et g une forme linéaire sur V. Montrer que les coefficients par rapport à la base (a_i) de la forme trilinéaire alternée $f \wedge g$ sont les scalaires

$$\alpha_{ijk} = f(a_i, a_j)g(a_k) + f(a_j, a_k)g(a_i) + f(a_k, a_i)g(a_j).$$

21. Soit V un espace vectoriel de dimension 3 sur un corps commutatif, et soient x, y, z trois éléments de V.

a) Si x, y, z sont linéairement dépendants, on a $f(x, y, z) = 0$ pour toute forme trilinéaire alternée f sur V (exprimer l'un des vecteurs à l'aide des deux autres).

b) Si x, y, z sont linéairement indépendants, on a $f(x, y, z) \neq 0$ pour toute forme trilinéaire alternée $f \neq 0$ sur V (observer que x, y, z forment une base de V).

c) Soit a, b, c une base de V; pour que x, y, z soient linéairement indépendants, il faut et il suffit que le déterminant de leurs coordonnées par rapport à la base a, b, c soit non nul (utiliser les questions *a*) et *b*) et l'*Exemple* 7 du § 22).

(Les résultats de cet *Exercice* seront généralisés au § suivant, mais on conseille au lecteur d'examiner tout d'abord en détail le cas des espaces à trois dimensions, du reste fort important dans la pratique).

22. Les vecteurs

$$(2, -3, 1), \qquad (3, -1, 5), \qquad (1, -4, 3)$$

sont-ils linéairement indépendants dans $\mathbf{R}^3$? Même question pour les vecteurs

$$(5, 4, 3), \qquad (3, 3, 2), \qquad (8, 1, 3).$$

§ 23

1. Soit K un anneau commutatif. Montrer que les matrices $U \in M_n(K)$ telles que

$$\text{dét}(U) = 1$$

forment un sous-groupe de $GL(n, K)$ — on le désigne généralement par la notation $SL(n, K)$ et on l'appelle le **groupe spécial linéaire à n variables** sur l'anneau K.

2. Le déterminant d'une matrice nilpotente à coefficients dans un corps commutatif est nul.

3. Soit U une matrice carrée à coefficients entiers, de déterminant non nul. Montrer que les seuls nombres premiers p qui figurent dans les dénominateurs des coefficients (rationnels) de U^{-1} sont ceux qui divisent le déterminant de U.

4. Soit U une matrice carrée orthogonale (i.e. telle que ${}^tU.U = 1$) à coefficients dans un corps commutatif. Montrer que $\text{dét}(U) = +1$ ou -1.

5. Trouver le nombre d'inversions de la permutation

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

6. De toutes les permutations des entiers $1, 2, \dots, n$, quelle est celle dont le nombre d'inversions est maximum?

7. Montrer que pour tout entier k tel que $0 \leqslant k \leqslant \binom{n}{2}$ il existe une permutation des entiers $1, 2, \dots, n$ dont le nombre d'inversions est k.

8. On considère un déterminant d'ordre 6, dont on désigne les termes par a_{ij} $(1 \leqslant i, j \leqslant 6)$. Quel est le signe dont on doit faire précéder le produit

$$a_{61}a_{23}a_{45}a_{36}a_{12}a_{54}$$

dans le développement de ce déterminant?

¶ **9.** Dans le groupe $\mathfrak{S}_n$ des permutations de l'ensemble $\{1, 2, \dots, n\}$ on désigne par $\mathfrak{A}_n$ l'ensemble des permutations paires.

a) Montrer que $\mathfrak{A}_n$ est un sous-groupe invariant de $\mathfrak{S}_n$ (**groupe alterné** de n objets) et que le groupe quotient $\mathfrak{S}_n/\mathfrak{A}_n$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.

b) Pour $3 \leqslant i \leqslant n$ (on suppose $n \geqslant 3$) on désigne par s_i la permutation

$$\begin{pmatrix} 1 & 2 & 3 & \dots & i-1 & i & i+1 & \dots & n \\ i & 1 & 3 & \dots & i-1 & 2 & i+1 & \dots & n \end{pmatrix};$$

montrer que les s_i engendrent $\mathfrak{A}_n$.

c) Montrer que, pour $n \geqslant 5$, les seuls sous-groupes invariants de $\mathfrak{A}_n$ sont $\mathfrak{A}_n$ lui-même et le sous-groupe réduit à l'identité (ce qu'on exprime en disant que $\mathfrak{A}_n$ est un groupe **simple** pour $n \geqslant 5$). Quels sont les sous-groupes invariants de $\mathfrak{A}_n$ pour $n = 2$, 3 ou 4?

d) Montrer que, pour $n \neq 4$, le seul sous-groupe invariant non trivial de $\mathfrak{S}_n$ est $\mathfrak{A}_n$.

¶ **10.** Soit $A = (a_{ij})$ une matrice carrée inversible d'ordre n à coefficients dans un corps commutatif K. On cherche des matrices X et Y (carrées d'ordre n) à coefficients dans K, vérifiant la relation

$$A = X.Y,$$

et de la forme

$$X = \begin{pmatrix} * & 0 & 0 & \dots & 0 \\ * & * & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ * & * & * & \dots & * \end{pmatrix}, \qquad Y = \begin{pmatrix} * & * & * & \dots & * \\ 0 & * & * & \dots & * \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & * \end{pmatrix}$$

(où les signes $*$ désignent des éléments arbitraires de K). Montrer que, pour que X et Y existent, il faut et il suffit qu'on ait

$$\begin{vmatrix} a_{11} & \dots & a_{1p} \\ \dots & \dots & \dots \\ a_{p1} & \dots & a_{pp} \end{vmatrix} \neq 0 \qquad \text{pour} \qquad 1 \leqslant p \leqslant n-1.$$

Dans ce cas, on peut imposer aux coefficients diagonaux de X (ou de Y) d'être tous égaux à 1, et cette condition détermine entièrement X et Y.

11. Soit K un anneau commutatif. On appelle dérivation de K toute application D de K dans K telle que l'on ait

$$D(x+y) = D(x) + D(y), \qquad D(xy) = D(x).y + x.D(y)$$

quels que soient $x, y \in K$ (cf. § 30, n° 1).
Soient D une dérivation de K et $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$ une matrice carrée d'ordre n à coefficients dans K. Pour chaque entier i tel que $1 \leqslant i \leqslant n$, on note A_i la matrice obtenue en appliquant D aux termes situés sur la i^e colonne de A. Montrer que

$$D(\text{dét}(A)) = \text{dét}(A_1) + \dots + \text{dét}(A_n)$$

(formule de dérivation des déterminants).

¶¶ **12.** Soient M un module sur un anneau commutatif, f une forme p-linéaire alternée sur M, et g une forme q-linéaire alternée sur M. On définit une application

$$h : M^{p+q} \to K$$

(où K est l'anneau de base) en posant

$$(*) \qquad h(x_1, \ldots, x_{p+q}) = \sum_{\substack{s \in \mathfrak{S}_{p+q} \\ s(1) < \cdots < s(p) \\ s(p+1) < \cdots < s(p+q)}} \varepsilon(s) \cdot f(x_{s(1)}, \ldots, x_{s(p)}) \cdot g(x_{s(p+1)}, \ldots, x_{s(p+q)})$$

où la sommation est étendue à toutes les permutations s des entiers $1, \ldots, p+q$ qui respectent l'ordre des p premiers, ainsi que des q derniers, de ces entiers.

a) Montrer que h est une forme $(p+q)$-linéaire alternée sur M. On l'appelle le **produit extérieur** des formes f et g, et on la désigne par la notation

$$h = f \wedge g.$$

b) Montrer que

$$g \wedge f = (-1)^{pq} f \wedge g.$$

c) Montrer que, si f, g, h sont trois formes multilinéaires alternées sur M, on a

$$f \wedge (g \wedge h) = (f \wedge g) \wedge h$$

(« associativité » du produit extérieur).

d) Soient $u_1, \ldots, u_p, v_1, \ldots, v_q$ des formes linéaires sur M. Dans la formule $(*)$ on prend

$$f = u_1 \wedge \cdots \wedge u_p, \qquad g = v_1 \wedge \cdots \wedge v_q$$

(cf. § 23, n° 3, *Exemple* 2). Montrer qu'alors

$$h = u_1 \wedge \cdots \wedge u_p \wedge v_1 \wedge \cdots \wedge v_q.$$

¶¶ **13.** (Généralisation du théorème de multiplication des déterminants.) Soit

$$A = (a_{ij})_{1 \leqslant i \leqslant p,\, 1 \leqslant j \leqslant q}$$

une matrice rectangulaire à coefficients dans un anneau commutatif K; on choisit un entier r tel que $1 \leqslant r \leqslant p$ et $1 \leqslant r \leqslant q$.
Étant données une partie I à r éléments de l'ensemble $\{1, \ldots, p\}$ et une partie J à r éléments de l'ensemble $\{1, \ldots, q\}$, on désigne par a_{IJ} la matrice carrée d'ordre r formée avec les a_{ij} tels que $i \in$ I et $j \in$ J; enfin, on désigne par

$$\Lambda^r(A)$$

la matrice

$$(\text{dét}\,(a_{IJ}))_{I \subset \{1, \ldots, p\},\, J \subset \{1, \ldots, q\},\, \text{Card}(I) = \text{Card}(J) = r};$$

on peut par exemple ordonner lexicographiquement les parties I à r éléments de $\{1, \ldots, p\}$ en convenant qu'une partie

$$\{i_1, \ldots, i_r\} \qquad \text{avec} \qquad i_1 < \cdots < i_r$$

précède une partie

$$\{j_1, \ldots, j_r\} \qquad \text{avec} \qquad j_1 < \cdots < j_r$$

s'il existe un entier h $(1 \leqslant h \leqslant r)$ tel que l'on ait

$$i_1 = j_1, \ldots, i_{h-1} = j_{h-1}, \; i_h < j_h$$

(cf. la méthode de numérotation des mots figurant dans un dictionnaire...) Les scalaires $\text{dét}\,(a_{IJ})$ s'appellent les **mineurs d'ordre** r de la matrice A.
Cela dit, montrer que si A et B sont deux matrices à coefficients dans K, telles que le produit AB ait un sens, on a

$$\Lambda^r(AB) = \Lambda^r(A) \cdot \Lambda^r(B).$$

¶ **14.** Soient A et B deux matrices à p lignes et q colonnes à coefficients dans un anneau commutatif K. On dit que A et B sont **équivalentes** (sur l'anneau de base K) s'il existe des matrices

$$U \in \text{GL}(p, K), \qquad V \in \text{GL}(q, K)$$

telles que $B = UAV$.
S'il en est ainsi, montrer que pour tout $r \leqslant p$, q l'idéal de K engendré par les mineurs d'ordre r de A est égal à l'idéal engendré par les mineurs d'ordre r de B.
[NB — La réciproque est vraie si K est *principal*; cf. § 31, *Exercice* 11, (*e*).]

¶ **15.** Soient K un anneau commutatif et $A \in M_p(K)$, $B \in M_q(K)$; on considère [§ 21, *Exercice* 4, *f*)] la matrice $A \otimes B \in M_{pq}(K)$. Montrer qu'on a

$$\text{dét}\,(A \otimes B) = \text{dét}\,(A)^q \cdot \text{dét}\,(B)^p.$$

¶¶ **16.** Soit A une matrice carrée d'ordre n à coefficients dans un anneau commutatif K. On considère, pour $1 \leqslant r \leqslant n$, la matrice $\Lambda^r(A)$ de l'*Exercice* 14. Montrer que

$$\text{dét}\,(\Lambda^r(A)) = \text{dét}\,(A)^{\binom{n-1}{r-1}}.$$

¶¶ **17.** Soient M un module libre de type fini sur un anneau commutatif, et u un automorphisme de M. Calculer le déterminant de l'automorphisme $T^p_q(u)$ de $T^p_q(M)$ (§ 21, *Exercice* 1) en fonction de celui de u.

¶ **18.** Soit A une matrice carrée d'ordre *impair* à coefficients dans un anneau commutatif K. On suppose A *antisymétrique*, i.e. que ${}^tA = -A$. Montrer que $\text{dét}\,(A) = 0$. (Utiliser l'*Exercice* 17 du § 22).

§ 24

Calculer les déterminants suivants

1. $\begin{vmatrix} a & 3 & 0 & 5 \\ 0 & b & 0 & 2 \\ 1 & 2 & c & 3 \\ 0 & 0 & 0 & d \end{vmatrix}$

2. $\begin{vmatrix} x & a & b & 0 & c \\ 0 & y & 0 & 0 & d \\ 0 & e & z & 0 & f \\ g & h & k & u & l \\ 0 & 0 & 0 & 0 & v \end{vmatrix}$

3. $\begin{vmatrix} a & b & c & d \\ -b & a & d & -c \\ -c & -d & a & b \\ -d & c & -b & a \end{vmatrix}$

4. $\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{vmatrix}$

5. $\begin{vmatrix} 6 & -5 & 8 & 4 \\ 9 & 7 & 5 & 2 \\ 7 & 5 & 3 & 7 \\ -4 & 8 & -8 & -3 \end{vmatrix}$

6. $\begin{vmatrix} 24 & 11 & 13 & 17 & 19 \\ 51 & 13 & 32 & 40 & 46 \\ 61 & 11 & 14 & 50 & 56 \\ 62 & 20 & 7 & 13 & 52 \\ 80 & 24 & 45 & 57 & 70 \end{vmatrix}$

7. $\begin{vmatrix} 1 & 2 & 3 & \dots & n \\ -1 & 0 & 3 & \dots & n \\ -1 & -2 & 0 & \dots & n \\ \dots & \dots & \dots & \dots & \dots \\ -1 & -2 & -3 & \dots & 0 \end{vmatrix}$

8. $\begin{vmatrix} a_0 & a_1 & a_2 & \dots & a_n \\ -x & x & 0 & \dots & 0 \\ 0 & -x & x & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & 0 & x \end{vmatrix}$

¶ **9.** $\begin{vmatrix} 3 & 2 & 0 & 0 & \dots & 0 \\ 1 & 3 & 2 & 0 & \dots & 0 \\ 0 & 1 & 3 & 2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 3 \end{vmatrix}$

Notant D_n ce déterminant d'ordre n, on établira une relation simple entre D_n, D_{n-1} et D_{n-2} et on utilisera le résultat suivant. Soit $(u_n)_{n\geq 1}$ une suite de nombres complexes telle que l'on ait la relation de récurrence

$$u_{n+2} = au_{n+1} + bu_n;$$

soient z_1 et z_2 les racines (distinctes ou non) de l'équation

$$z^2 - az - b = 0;$$

alors, si $z_1 \neq z_2$, il existe des constantes c_1 et c_2 telles que l'on ait

$$u_n = c_1 z_1^n + c_2 z_2^n \text{ pour tout } n,$$

et si $z_1 = z_2$ il existe des constantes c_1 et c_2 telles que l'on ait

$$u_n = (c_1 n + c_2) z_1^n$$

pour tout n. Pour des résultats beaucoup plus généraux, voir § 35, *Exercice* 16.

¶ **10.** $\begin{vmatrix} 1 & 2 & 0 & 0 & 0 & \dots & 0 & 0 \\ 3 & 4 & 3 & 0 & 0 & \dots & 0 & 0 \\ 0 & 2 & 5 & 3 & 0 & \dots & 0 & 0 \\ 0 & 0 & 2 & 5 & 3 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & \dots & 5 & 3 \\ 0 & 0 & 0 & 0 & 0 & \dots & 2 & 5 \end{vmatrix}$ (Même méthode que ci-dessus).

11. $\begin{vmatrix} 1-n & 1 & 1 & \dots & 1 \\ 1 & 1-n & 1 & \dots & 1 \\ 1 & 1 & 1-n & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 1-n \end{vmatrix}$ (déterminant à n lignes et n colonnes)

12. $\begin{vmatrix} 1 & n & n & \dots & n \\ n & 2 & n & \dots & n \\ n & n & 3 & \dots & n \\ \dots & \dots & \dots & \dots & \dots \\ n & n & n & \dots & n \end{vmatrix}$

13. $\begin{vmatrix} x & a_1 & a_2 & \dots & a_{n-1} & 1 \\ a_1 & x & a_2 & \dots & a_{n-1} & 1 \\ a_1 & a_2 & x & \dots & a_{n-1} & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & a_3 & \dots & x & 1 \\ a_1 & a_2 & a_3 & \dots & a_n & 1 \end{vmatrix}$

(Chercher les racines de cette fonction polynomiale de x.)

¶ **14.** Montrer que

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

(déterminant de VanderMonde; on remarque par exemple que le premier membre est un polynôme de degré $n-1$ au plus en x_1, dont $x_2, \dots, x_n$ sont des racines évidentes).

¶ **15.** $\begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-2} & x_1^n \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-2} & x_n^n \end{vmatrix}$

¶ **16.** $\begin{vmatrix} 1 & f_1(x_1) & f_2(x_1) & \dots & f_{n-1}(x_1) \\ \dots & \dots & \dots & \dots & \dots \\ 1 & f_1(x_n) & f_2(x_n) & \dots & f_{n-1}(x_n) \end{vmatrix}$ où $f_k(x) = x^k + a_{k1}x^{k-1} + \dots + a_{kk}$.

¶ **17.** $\begin{vmatrix} 1 & \binom{1}{x_1} & \binom{2}{x_1} & \dots & \binom{n-1}{x_1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \binom{1}{x_n} & \binom{2}{x_n} & \dots & \binom{n-1}{x_n} \end{vmatrix}$ où l'on pose $\binom{x}{k} = \frac{x(x-1)\dots(x-k+1)}{k!}$.

¶¶ 18. Montrer que

$$\begin{vmatrix} a & b & c & d & e & f & g & h \\ b & a & d & c & f & e & h & g \\ c & d & a & b & g & h & e & f \\ d & c & b & a & h & g & f & e \\ e & f & g & h & a & b & c & d \\ f & e & h & g & b & a & d & c \\ g & h & e & f & c & d & a & b \\ h & g & f & e & d & c & b & a \end{vmatrix} = \begin{matrix} (a+b+c+d+e+f+g+h)\,(a+b+c+d-e-f-g-h)\times \\ \times\,(a+b-c-d+e+f-g-h)\,(a+b-c-d-e-f+g+h)\times \\ \times\,(a-b+c-d+e-f+g-h)\,(a-b+c-d-e+f-g+h)\times \\ \times\,(a-b-c+d+e-f-g+h)\,(a-b-c+d-e+f+g-h) \end{matrix}$$

19. Montrer que

$$\begin{vmatrix} 1+x_1y_1 & 1+x_1y_2 & \dots & 1+x_1y_n \\ \dots & \dots & \dots & \dots \\ 1+x_ny_1 & 1+x_ny_2 & \dots & 1+x_ny_n \end{vmatrix} = 0 \quad \text{si } n \geqslant 3.$$

¶ 20. Calculer, par récurrence sur le nombre n de lignes, le déterminant

$$\begin{vmatrix} 1 & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 1 \end{vmatrix}$$

¶ 21. Montrer que

$$\begin{vmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & \binom{2}{1} & \binom{2}{2} & 0 & \dots & 0 \\ 1 & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \binom{n}{1} & \binom{n}{2} & \binom{n}{3} & \dots & \binom{n}{n-1} \end{vmatrix} = 1.$$

¶ 22. En calculant le produit

$$\begin{vmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{vmatrix} \cdot \begin{vmatrix} x & -y & -z & -t \\ y & x & -t & z \\ z & t & x & -y \\ t & -z & y & x \end{vmatrix},$$

établir l'identité d'Euler

$$(a^2+b^2+c^2+d^2)\,(x^2+y^2+z^2+t^2) = (ax+by+cz+dt)^2+(ay-bx+ct-dz)^2 + (az-bt-cx+dy)^2+(at+bz-cy+dx)^2.$$

Voyez-vous un rapport avec les *Exercices* 10 et 11 du § 15?
Calculer les inverses des matrices suivantes :

23. $\begin{pmatrix} 2 & 7 & 3 \\ 3 & 9 & 4 \\ 1 & 5 & 3 \end{pmatrix}$ **24.** $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 2 \\ 1 & 1 & 1 & -1 \\ 1 & 0 & -2 & -6 \end{pmatrix}$ **25.** $\begin{pmatrix} 3 & -2 & -5 & 1 \\ 2 & -3 & 1 & 5 \\ 1 & 2 & 0 & -4 \\ 1 & -1 & -4 & 9 \end{pmatrix}$

26. Calculer le rang des matrices

$$\begin{pmatrix} 17 & -28 & 45 & 11 & 39 \\ 24 & -37 & 61 & 13 & 50 \\ 25 & -7 & 32 & -18 & -11 \\ 31 & 12 & 19 & -43 & -55 \\ 42 & 13 & 29 & -55 & -68 \end{pmatrix}, \qquad \begin{pmatrix} 2 & -1 & 1 & 3 & 4 \\ 2 & -1 & 2 & 1 & -2 \\ 2 & -3 & 1 & 2 & -2 \\ 1 & 0 & 1 & -2 & -6 \\ 1 & 2 & 1 & -1 & 0 \\ 4 & -1 & 3 & -1 & -8 \end{pmatrix}.$$

27. Les vecteurs

$$(1, 0, 0, 2, 5), \quad (0, 1, 0, 3, 4), \quad (0, 0, 1, 4, 7), \quad (2, -3, 4, 11, 12)$$

sont-ils linéairement indépendants dans $\mathbf{R}^5$?

¶¶ 28. Montrer que

$$\begin{vmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 2 \end{vmatrix} = 1.$$

29. Calculer

$$\begin{vmatrix} 1 & 4 & 9 & 16 \\ 4 & 9 & 16 & 25 \\ 9 & 16 & 25 & 36 \\ 16 & 25 & 36 & 49 \end{vmatrix}.$$

30. Combien d'additions et de multiplications doit-on en principe effectuer pour calculer un déterminant d'ordre 10?

31. Résoudre par la théorie des déterminants les *Exercices* 1 à 17 du § 20.

32. Résoudre et discuter les systèmes d'équations linéaires suivants :

a)
$$\begin{aligned} ax+by+z &= 1 \\ x+aby+z &= b \\ x+by+az &= 1 \end{aligned}$$

b)
$$\begin{aligned} ax+by+2z &= 1 \\ ax+(2b-1)y+3z &= 1 \\ ax+by+(b+3)z &= 2b-1 \end{aligned}$$

c)
$$\begin{aligned} 2(a+1)x+3y+az &= a+4 \\ (4a-1)x+(a+1)y+(2a-1)z &= 2a+2 \\ (5a-4)x+(a+1)y+(3a-4)z &= a-1 \end{aligned}$$

¶ **33.** (Développement d'un déterminant suivant la règle de Laplace.) Soient K un anneau commutatif et n un entier > 1. On désigne par

$$D(x_1, \ldots, x_n)$$

le déterminant de n vecteurs $x_i \in K^n$ par rapport à la base canonique (e_i) de K^n. On pose

$$x_i = \xi_{i1}e_1 + \cdots + \xi_{in}e_n.$$

Enfin on choisit un entier p tel que $1 \leqslant p \leqslant n$.

a) Montrer qu'on a la relation

$$D(x_1, \ldots, x_n) = \sum_{i_1 < \cdots < i_p} \begin{vmatrix} \xi_{1i_1} & \cdots & \xi_{pi_1} \\ \cdots & \cdots & \cdots \\ \xi_{1i_p} & \cdots & \xi_{pi_p} \end{vmatrix} . D(e_{i_1}, \ldots, e_{i_p}, x_{p+1}, \ldots, x_n)$$

(regarder $D(x_1, \ldots, x_n)$ comme une fonction multilinéaire alternée de $x_1, \ldots, x_p$).

b) Montrer que, pour $1 \leqslant i_1 < \cdots < i_p \leqslant n$, on a

$$D(e_{i_1}, \ldots, e_{i_p}, x_{p+1}, \ldots, x_n) = \begin{vmatrix} \xi_{p+1, j_1} & \cdots & \xi_{n, j_1} \\ \cdots & \cdots & \cdots \\ \xi_{p+1, j_{n-p}} & \cdots & \xi_{n, j_{n-p}} \end{vmatrix}$$

où l'on désigne par $j_1, \ldots, j_{n-p}$ ceux des entiers $\{1, 2, \ldots, n\}$ qui n'appartiennent pas à l'ensemble $\{i_1, \ldots, i_p\}$, rangés de telle sorte que la permutation $(i_1, \ldots, i_p j_1, \ldots, j_{n-p})$ de $\{1, \ldots, n\}$ soit *paire*.

c) Soit

$$X = (\xi_{ij})_{1 \leqslant i, j \leqslant n}$$

une matrice carrée d'ordre n à coefficients dans K. Pour toute partie I de l'ensemble $\{1, 2, \ldots, n\}$ comprenant p éléments, on désigne par X_I la matrice formée avec les ξ_{ij} tels que l'on ait $i \in I$ et $1 \leqslant j \leqslant p$, et par X'_I la matrice « complémentaire », formée avec les ξ_{ij} tels que l'on ait $i \notin I$ et $p+1 \leqslant j \leqslant n$. Enfin on désigne par $n(I)$ le nombre de couples (i, j) tels que l'on ait $i \in I, j \notin I$ et $i > j$. Montrer que l'on a

$$\det(X) = \sum_{\mathrm{Card}(I)=p} (-1)^{n(I)} . \det(X_I) . \det(X'_I)$$

(Formule de Laplace), où la somme est étendue à toutes les *parties* I à p éléments de l'ensemble $\{1, \ldots, n\}$.

d) Déduire ce résultat de la formule d'associativité du produit extérieur [§ 23, *Exercice* 13, *d*)] Appliquer la règle de Laplace au calcul des déterminants suivants :

34. $\begin{vmatrix} 1 & 1 & 3 & 4 \\ 2 & 0 & 0 & 8 \\ 3 & 0 & 0 & 2 \\ 4 & 4 & 7 & 5 \end{vmatrix}$ **35.** $\begin{vmatrix} 2 & 1 & 4 & 3 & 5 \\ 3 & 4 & 0 & 5 & 0 \\ 3 & 4 & 5 & 2 & 1 \\ 1 & 5 & 2 & 4 & 3 \\ 4 & 6 & 0 & 7 & 0 \end{vmatrix}$ **36.** $\begin{vmatrix} 1 & 2 & 3 & 4 & 5 & 3 \\ 6 & 5 & 7 & 8 & 4 & 2 \\ 9 & 8 & 6 & 7 & 0 & 0 \\ 3 & 2 & 4 & 5 & 0 & 0 \\ 3 & 4 & 0 & 0 & 0 & 0 \\ 5 & 6 & 0 & 0 & 0 & 0 \end{vmatrix}$

37. $\begin{vmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 3 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & a & b & c & d \\ 0 & a^3 & b^3 & c^3 & d^3 \end{vmatrix}$ **38.** $\begin{vmatrix} 3 & 4 & -3 & -1 & 2 \\ -5 & 6 & 5 & 2 & 3 \\ 4 & -9 & -3 & 7 & -5 \\ -1 & -4 & 1 & 1 & -2 \\ -3 & 7 & 5 & 2 & 3 \end{vmatrix}$

§ 26

1. Montrer que les nombres complexes suivants sont algébriques et former pour chacun d'entre eux une équation algébrique à coefficients rationnels :

$$\sqrt{2} + \sqrt{3}; \qquad \sqrt[3]{2} + \sqrt{3}; \qquad \sqrt[4]{2} + \sqrt[3]{3}; \qquad \sqrt{2} + \sqrt{3} + \sqrt{5}.$$

2. Soient L un corps commutatif, K un sous-corps de L, et x un élément de L transcendant sur K. Trouver toutes les relations algébriques à coefficients dans K existant entre les éléments

$$x^2 + 1 \qquad \text{et} \qquad x^3$$

de L. Même question pour

$$x^3 + x + 1 \qquad \text{et} \qquad x^5.$$

¶ **3.** Soient A un anneau d'intégrité commutatif et K un sous-corps de A. On suppose A de dimension finie en tant qu'espace vectoriel sur K; montrer que A est un corps.
Soient L un corps commutatif, K un sous-corps de L, et $x_1, \ldots, x_n$ des éléments de L algébriques sur K. Montrer que le sous-anneau $K[x_1, \ldots, x_n]$ de L est un corps.

¶ ¶ **4.** Soit K un corps commutatif. On appelle **extension** de K tout corps L admettant K pour sous-corps (par exemple, $\mathbf{C}$ est une extension de $\mathbf{R}$, qui est une extension de $\mathbf{Q}$). On peut alors regarder L comme un espace vectoriel sur K; si L est de dimension finie sur K, i.e. s'il existe des éléments $a_1, \ldots, a_r \in L$ en nombre fini tels que tout élément de L puisse s'écrire sous la forme

$$x_1a_1 + \cdots + x_ra_r$$

avec des $x_i \in K$, on dit que L est une **extension de degré fini** de K; la dimension de L comme espace vectoriel sur K s'appelle alors le **degré** de L sur K, et se note

$$[L : K];$$

et on appelle **base** de L sur K toute base de L considéré comme espace vectoriel sur K. Lorsque $K = \mathbf{Q}$, les extensions de degré fini de K sont, par définition, les **corps de nombres algébriques** [historiquement, on imposait aux corps de nombres algébriques d'être des extensions de degré fini de $\mathbf{Q}$ *contenues dans* $\mathbf{C}$, mais il est facile de voir que toute extention de degré fini de $\mathbf{Q}$ peut se « plonger » dans $\mathbf{C}$, de sorte que cette condition est superflue]. On désigne dans ce qui suit

par K un corps commutatif et par L une extention de degré fini n de K. Pour tout $a \in L$, on note u_a l'application de L dans L donnée par

$$u_a(x) = ax \quad \text{pour tout } x \in L.$$

a) Montrer que u_a est un endomorphisme de L considéré comme espace vectoriel sur K, et qu'on a les relations

$$u_a + u_b = u_{a+b}, \qquad u_a \circ u_b = u_{ab}$$

quels que soient a, $b \in L$. Quels sont les endomorphismes de L (regardé comme espace vectoriel sur K) qui commutent à tous les u_a?

b) Pour tout $a \in L$, on pose

$$\mathrm{Tr}_{L/K}(a) = \mathrm{Tr}(u_a), \qquad \mathrm{N}_{L/K}(a) = \det(u_a)$$

(on regarde u_a comme un endomorphisme d'un espace vectoriel de dimension finie sur K; le déterminant de u_a est défini au § 23, n° 5, et la trace au § 19, *Exercice* 22). On dit que $\mathrm{Tr}_{L/K}(a)$ est la **trace** et $\mathrm{N}_{L/K}(a)$ la **norme** de a (relativement au sous-corps K); ce sont donc des éléments de K. Montrer qu'on a

$$\mathrm{Tr}_{L/K}(a+b) = \mathrm{Tr}_{L/K}(a) + \mathrm{Tr}_{L/K}(b), \qquad \mathrm{N}_{L/K}(ab) = \mathrm{N}_{L/K}(a)\mathrm{N}_{L/K}(b)$$

quels que soient a, $b \in L$. Si L est de degré n sur K, on a de plus

$$\mathrm{Tr}_{L/K}(a) = na, \qquad \mathrm{N}_{L/K}(a) = a^n$$

pour tout $a \in K$.

c) Soit $(a_i)_{1 \leqslant i \leqslant n}$ une base de L regardé comme espace vectoriel sur K; tout $x \in L$ s'écrit donc d'une façon et d'une seule sous la forme

$$x = \xi_1 a_1 + \cdots + \xi_n a_n \qquad \text{avec} \qquad \xi_1, \ldots, \xi_n \in K.$$

On pose

$$xa_i = \sum_{1 \leqslant j \leqslant n} \lambda_{ij} a_j$$

où les λ_{ij} sont dans K. Calculer $\mathrm{Tr}_{L/K}(x)$ et $\mathrm{N}_{L/K}(x)$ en fonction des λ_{ij}.

d) On suppose K de caractéristique 0 (i.e. que si $x \in K$ et $r \in \mathbf{Z}$ vérifient $rx = 0$, on a soit $r = 0$ soit $x = 0$; cf. § 30, n° 6). Montrer que si un $a \in L$ vérifie

$$\mathrm{Tr}_{L/K}(ax) = 0 \quad \text{pour tout } x \in L$$

on a $a = 0$. En déduire que, si $(a_i)_{1 \leqslant i \leqslant n}$ est une base de L sur K, on a

$$\det(\mathrm{Tr}_{L/K}(a_i a_j)_{1 \leqslant i,j \leqslant n}) \neq 0.$$

e) Soit $(a_i)_{1 \leqslant i \leqslant n}$ une base de L sur K; on considère n éléments

$$b_i = \sum_{1 \leqslant j \leqslant n} \rho_{ij} a_j \quad (\rho_{ij} \in K, \quad 1 \leqslant i \leqslant n)$$

de L. Montrer que, en introduisant les matrices

$$A = (\mathrm{Tr}_{L/K}(a_i a_j))_{1 \leqslant i,j \leqslant n}$$
$$B = (\mathrm{Tr}_{L/K}(b_i b_j))_{1 \leqslant i,j \leqslant n},$$

on a

$$\det(B) = \det(A) \cdot \det(\rho_{ij})^2.$$

En déduire (si K est de caractéristique 0) le résultat suivant : pour que n éléments $x_1, \ldots, x_n$ de L forment une base de L sur K, il faut et il suffit que le déterminant de la matrice

$$(\mathrm{Tr}_{L/K}(x_i x_j))_{1 \leqslant i,j \leqslant n}$$

soit non nul. Ce déterminant s'appelle le **discriminant** des n éléments $x_1, \ldots, x_n$ de L et se note généralement

$$\mathrm{D}_{L/K}(x_1, \ldots, x_n).$$

f) K étant supposé de caractéristique 0, soit $(u_i)_{1 \leqslant i \leqslant n}$ une base de L sur K; montrer qu'il existe une autre base $(v_i)_{1 \leqslant i \leqslant n}$ de L sur K telle que l'on ait

$$\mathrm{Tr}_{L/K}(u_i v_j) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

(on montrera que les coordonnées des v_i par rapport à la base (u_i) sont données par un système de Cramer). On dit que les bases (u_i) et (v_i) sont **complémentaires**.

g) Les hypothèses et notations étant celles de la question (*f*), montrer que les coordonnées de tout $x \in L$ par rapport à la base (v_i) sont les éléments

$$\mathrm{Tr}_{L/K}(xu_i)$$

de K.

h) On ne suppose plus K de caractéristique 0. On dit que L est une extension **séparable** de K s'il existe un $x \in L$ vérifiant

$$\mathrm{Tr}_{L/K}(x) \neq 0.$$

Montrer que les résultats des questions *d*), *e*), *f*) et *g*) sont encore valables dans ce cas.

¶¶ **5.** Soient L un corps commutatif et K un sous-corps de L; on suppose que L est extension de degré fini de K (*Exercice* 4), et on désigne par E un sous-corps de L contenant K.

a) Montrer que L est extension de degré fini de E, et que E est extension de degré fini de K.

b) Soit $(a_i)_{1 \leqslant i \leqslant r}$ une base de L sur E, et soit $(b_j)_{1 \leqslant j \leqslant s}$ une base de E sur K. Montrer que les rs éléments $a_i b_j$ forment une base de L sur K. En déduire que, si l'on note $[L : K]$ le degré de L sur K (i.e. la dimension de L comme espace vectoriel sur K) on a la relation

$$[L : K] = [L : E]\ [E : K]$$

c) Montrer que, pour tout $x \in L$, on a

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{E/K}(\mathrm{Tr}_{L/E}(x))$$
$$\mathrm{N}_{L/K}(x) = \mathrm{N}_{E/K}(\mathrm{N}_{L/E}(x))$$

(voir l'*Exercice* 4 en ce qui concerne les notations utilisées).

d) Soient x un élément de L et

$$x^s - a_{s-1}x^{s-1} + \cdots + (-1)^s a_0 = 0$$

une équation algébrique à coefficients dans K vérifiée par x, et de degré s *minimum*. Montrer que les éléments

$$1, x, \ldots, x^{s-1}$$

forment une base du corps $K[x]$ sur K. En utilisant la question *c*) de l'*Exercice* 4, et en posant $K[x] = E$, montrer qu'on a

$$\mathrm{Tr}_{E/K}(x) = a_{s-1}, \qquad \mathrm{N}_{E/K}(x) = a_0.$$

En conclure que

$$\mathrm{Tr}_{L/K}(x) = \frac{n}{s} a_{s-1}, \qquad \mathrm{N}_{L/K}(x) = (a_0)^{n/s}$$

où $n = [L : K]$.

§§ 27 et 28

1. Soit K un anneau d'intégrité infini. On dit qu'une partie A de K^n est un **ouvert de Zariski** dans K^n s'il existe des polynômes $f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$, en nombre fini, tels que le complémentaire de l'ensemble A dans K^n soit l'ensemble des $x \in K^n$ qui vérifient les relations

$$f_1(x) = \cdots = f_r(x) = 0.$$

Ceci dit, soient f et g deux polynômes à n indéterminées, à coefficients dans K; on suppose qu'il existe dans K^n un ouvert de Zariski non vide A tel que l'on ait

$$f(x) = g(x) \quad \text{pour tout } x \in A;$$

montrer qu'alors $f = g$ **(principe de prolongement des identités algébriques)**

2. Montrer que si trois polynômes $f, g, h \in \mathbf{R}[X]$ vérifient l'une quelconque des trois relations suivantes, on a $f = g = h = 0$:

$$f(X)^2 - Xg(X)^2 = Xh(X)^2$$
$$f(X)^2 - Xg(X)^2 + h(X)^2 = 0$$
$$f(X)^2 + g(X)^2 + (X+2)h(X)^2 = 0.$$

Peut-on dans ce qui précède remplacer **R** par un corps commutatif quelconque?

3. Soient K un corps commutatif, f un polynôme à une indéterminée à coefficients dans K, et $a_1, \ldots, a_r$ des racines deux à deux distinctes de f dans K. Montrer, à l'aide du lemme 1 du § 28, qu'il existe un polynôme g à coefficients dans K tel que

$$f(X) = (X - a_1) \ldots (X - a_r)g(X).$$

Application : calculer (sans calculs !) le déterminant

$$\begin{vmatrix} 1 & 1 & 2 & 3 \\ 1 & 2 - x^2 & 2 & 3 \\ 2 & 3 & 1 & 5 \\ 2 & 3 & 1 & 9 - x^2 \end{vmatrix}$$

4. Même question pour le déterminant

$$\begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & 1 - x & 1 & \ldots & 1 \\ 1 & 1 & 2 - x & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & 1 & \ldots & n - x \end{vmatrix}$$

5. Soient $f_1, \ldots, f_n$ des polynômes à une variable à coefficients danx un anneau commutatif K, et de degrés $n - 2$ au plus. Montrer qu'on a

$$\begin{vmatrix} f_1(x_1) & f_1(x_2) & \ldots & f_1(x_n) \\ \ldots & \ldots & \ldots & \ldots \\ f_n(x_1) & f_n(x_2) & \ldots & f_n(x_n) \end{vmatrix} = 0$$

quels que soient les $x_i \in K$.

¶ **6.** Soient K un corps commutatif infini et $a_0, \ldots, a_n$ des éléments donnés, deux à deux distincts, de K. Montrer qu'il existe un et un seul polynome $f \in K[X]$ de degré n au plus vérifiant

$$f(a_i) = b_i \quad (0 \leqslant i \leqslant n),$$

où les b_i sont des éléments donnés de K, et que f est fourni par la **formule d'interpolation de Lagrange**

$$f(X) = \sum_{i=0}^{i=n} b_i \frac{(X - a_0) \ldots (X - a_{i-1})(X - a_{i+1}) \ldots (X - a_n)}{(a_i - a_0) \ldots (a_i - a_{i-1})(a_i - a_{i+1}) \ldots (a_i - a_n)}.$$

Exemple : trouver un polynôme f de degré 3 tel que

$$f(1) = 2, \quad f(2) = 1, \quad f(3) = 4, \quad f(4) = 3.$$

¶ **7.** On pose

$$z_k = \cos \frac{2k\pi}{n} + i.\sin \frac{2k\pi}{n};$$

trouver un polynôme f de degré $n - 1$, à coefficients complexes, tel que l'on ait

$$f(z_k) = k + 1 \quad \text{pour } 0 \leqslant k \leqslant n - 1$$

Réponse :

$$f(X) = \frac{n+1}{2} - \frac{1}{2} \sum_{k=1}^{k=n-1} \left(1 - i.\operatorname{cotg} \frac{k\pi}{n}\right) X^k.$$

8. Soit f une fonction définie sur l'ensemble **N** des entiers naturels, et à valeurs complexes. On définit une nouvelle fonction Δf par

$$\Delta f(n) = f(n+1) - f(n),$$

et on définit successivement

$$\Delta^2 f = \Delta(\Delta f), \qquad \Delta^3 f = \Delta(\Delta^2 f), \ \ldots$$

Enfin, on dit que f est *polynomiale de degré r* s'il existe des constantes $a_0, \ldots, a_r$ telles que

$$f(n) = a_r n^r + a_{r-1} n^{r-1} + \cdots + a_0 \quad \text{pour tout } n \in \mathbf{N},$$

avec de plus $a_r \neq 0$.

a) Montrer que si f est polynomiale de degré r on a

$$\Delta^{r+1} f = 0, \qquad \Delta^r f \neq 0.$$

b) Calculer Δf lorsque

$$f(n) = \frac{n(n-1) \ldots (n - r + 1)}{r!} = \binom{n}{r} \quad \text{pour tout } n \in \mathbf{N};$$

en déduire que, si f est une fonction polynomiale quelconque de degré r, on a

$$f(n) = c_0 + c_1\binom{n}{1} + \cdots + c_r\binom{n}{r} \quad \text{avec } c_k = \Delta^k f(0).$$

c) Montrer que si une fonction $f(n)$ vérifie

$$\Delta^{r+1} f = 0, \qquad \Delta^r f \neq 0,$$

alors f est polynomiale de degré r.

d) Soit g une fonction polynomiale de degré $r - 1$ sur $\mathbf{N}$. Montrer qu'il existe une et une seule fonction polynomiale f sur $\mathbf{N}$, de degré r, telle que

$$\Delta f = g, \qquad f(0) = 0.$$

En calculant f par la formule de la question *b*), en déduire une expression de la somme

$$g(0) + g(1) + \cdots + g(n).$$

Application : calculer les sommes

$$1^2 + 2^2 + \cdots + n^2; \qquad 1^3 + 2^3 + \cdots + n^3.$$

¶¶ **9.** (On rappelle que si A est un anneau commutatif, un idéal I de A est dit *premier* si $I \neq A$ et si, pour $x, y \in A$, la relation $xy \in I$ implique $x \in I$ ou $y \in I$; qu'un idéal I de A est dit *maximal* si $I \neq A$ et si les seuls idéaux de A contenant I sont I et A; et qu'enfin tout idéal de A, autre que A tout entier, est contenu dans au moins un idéal maximal). On se propose de prouver que, *si* K *est un anneau commutatif, l'intersection de tous les idéaux premiers de* K *est l'ensemble des éléments nilpotents de* K.

a) Montrer que, si un idéal I de K vérifie $I \neq K$, alors l'idéal I′ de l'anneau de polynômes K[X] engendré par I vérifie $I' \neq K[X]$. En déduire que, pour tout idéal premier de K, il existe un idéal maximal de K[X] qui le contient.

b) On suppose que $u \in K$ appartient à tous les idéaux premiers de K. Montrer que le polynôme $1 - uX$ n'appartient à aucun idéal maximal de l'anneau K[X]; en déduire qu'il est inversible dans l'anneau K[X].

c) Montrer que le polynôme $1 - uX$ ($u \in K$) est inversible dans K[X] si et seulement si u est nilpotent; en déduire le théorème annoncé.

d) Soit I un idéal d'un anneau commutatif K, avec $I \neq K$. Montrer que l'intersection des idéaux premiers de K contenant I est formée des $x \in K$ tels que l'on ait

$$x^n \in I$$

pour au moins un entier n.

10. Soit K un corps commutatif. Pour que le sous-anneau K[f] de K[X] engendré par un polynôme $f \in K[X]$ soit K[X] tout entier, il faut et il suffit que

$$f(X) = aX + b, \qquad a \neq 0.$$

¶ **11.** Soit K un anneau commutatif. On appelle **série formelle à une indéterminée** à coefficients dans K toute suite

$$f = (a_0, a_1, \ldots, a_n, \ldots)$$

d'éléments de K (on ne suppose pas les a_i presque tous nuls). On définit la somme et le produit de deux telles séries formelles à l'aide des formules (2) et (3) du § 27, n° 2, utilisées pour définir la somme et le produit de deux polynômes. Montrer qu'avec ces définitions on obtient un *anneau commutatif* contenant un sous-anneau isomorphe à K[X].

L'anneau ainsi obtenu se note habituellement K[[X]]; au lieu de la notation initiale $f = (a_0, a_1, \ldots, a_n, \ldots)$, on représente les séries formelles par l'écriture

$$(*) \qquad f = a_0 + a_1X + \cdots + a_nX^n + \cdots = \sum_{n=0}^{\infty} a_nX^n,$$

qui permet de retenir plus facilement les formules définissant les opérations fondamentales : pour multiplier deux séries formelles, on les multiplie « terme à terme » puis on groupe ensemble les termes de même degré dans le résultat obtenu. Bien entendu, la formule (*) n'a théoriquement aucun sens, puisqu'elle peut contenir une infinité de termes non nuls; on ne doit la considérer que comme une simple *notation* commode pour représenter la suite des $a_i \in K$.

Démontrer les résultats suivants :

a) Pour que l'anneau K[[X]] soit intègre, il faut et il suffit que K le soit.

b) Pour qu'un élément (*) de K[[X]] soit inversible dans K[[X]], il faut et il suffit que son « terme constant » a_0 soit inversible dans K (différence majeure avec les anneaux de polynômes...).

c) Calculer l'inverse de $1 - X$ dans K[[X]].

¶¶ **12.** Soient K un anneau commutatif et

$$p(X, Y) = p_0(X) + p_1(X)Y + \cdots + p_n(X)Y^n$$

un polynôme à deux variables à coefficients dans K. On suppose $p_0(0) = 0$ et $p_1(0)$ inversible dans K [i.e. $p(0, 0) = 0$ et $p'_Y(0, 0) \neq 0$ si K est un *corps*.]

Montrer qu'il existe une série formelle et une seule

$$y = a_1X + a_2X^2 + \cdots$$

à coefficients dans K, sans terme constant, qui vérifie la relation $p(X, y) = 0$.

[On pourra procéder comme suit : supposant trouvées des constantes $a_1, \ldots, a_r \in K$ telles que le polynôme

$$p(X, a_1X + a_2X^2 + \cdots + a_rX^r)$$

ne contienne aucun terme de degré $\leqslant r$, on montrera qu'il existe $a_{r+1} \in K$ tel que le polynôme

$$p(X, a_1X + a_2X^2 + \cdots + a_{r+1}X^{r+1})$$

ne contienne aucun terme de degré $\leqslant r + 1$.]

Calculer y si $K = \mathbf{C}$ et $f(X, Y) = (X - 1)^p - Y^q$ où p et q sont des entiers positifs. Voyez-vous un rapport entre la série formelle obtenue et le développement en série entière, établi en Analyse, de la fonction

$$(z - 1)^{p/q}?$$

¶ **13.** Soient p un nombre premier, f et g deux polynômes à coefficients entiers rationnels.

a) Montrer que si p divise tous les coefficients de fg, il divise tous les coefficients de f, ou bien tous les coefficients de g.

b) On dit qu'un polynôme à coefficients entiers rationnels est **primitif** si le *pgcd* de ses coefficients est égal à 1. Montrer que si f, g sont primitifs, il en est de même de leur produit.

c) Étant donné un polynôme h à coefficients entiers rationnels, on appelle **contenu** de h le *pgcd*, noté $c(h)$, de ses coefficients. Montrer qu'on a

$$c(fg) = c(f)\,c(g) \qquad \text{quels que soient} \qquad f, g \in \mathbf{Z}[X]$$

(lemme de Gauss).

¶ **14.** Soient K un anneau commutatif, $\mathfrak{p}$ un idéal premier de K, et f, g deux polynômes à coefficients dans K. On suppose que tous les coefficients de fg sont dans $\mathfrak{p}$. Montrer que $\mathfrak{p}$ contient alors tous les coefficients de f, ou tous ceux de g.

¶ **15.** Soit K un anneau d'intégrité commutatif.

a) Soient f et g deux polynômes non constants à une indéterminée, à coefficients dans l'anneau K. Dans l'anneau K[X, Y] des polynômes à deux indéterminées à coefficients dans K, on considère l'idéal I engendré par les polynômes $f(X)$ et $g(Y)$. Montrer qu'on a

$$I \neq K[X, Y]$$

(on supposera qu'on a une relation de la forme

$$u(X, Y)\,f(X) + v(X, Y)\,g(Y) = 1$$

et on examinera les termes homogènes de degré maximum du premier membre).

b) Soient $f_1, \ldots, f_n$ des polynômes à une indéterminée, à coefficients dans K. Montrer que l'idéal de l'anneau $K[X_1, \ldots, X_n]$ engendré par $f_1(X_1), \ldots, f_n(X_n)$ n'est pas l'anneau $K[X_1, \ldots, X_n]$ tout entier si les f_i ne sont pas constants.

c) Montrer que, pour tout entier k tel que $1 \leqslant k \leqslant n$, l'idéal de $K[X_1, \ldots, X_n]$ engendré par $X_1, \ldots, X_k$ est premier. Ces n idéaux sont-ils deux à deux distincts?

¶ **16.** Soit K un anneau commutatif. Montrer que les propriétés suivantes de K sont équivalentes : (*i*) K n'a pas d'élément nilpotent non nul (*ii*) tout élément inversible de l'anneau K[X] est constant (cf. *Exercice* 9 de ce §, et l'*Exercice* 1 du § 8; on pourra aussi examiner les rapports avec l'*Exercice* 11 de ce §).

17. Soient V et W deux espaces vectoriels de dimension finie sur un corps commutatif K. On dit qu'une application f de V dans W est **polynomiale** s'il existe une base de V et une base de W telles que les coordonnées du vecteur $y = f(x) \in W$ soient données, en fonction de celles du vecteur $x \in V$, par des formules de la forme

$$\eta_j = p_j(\xi_1, \ldots, \xi_m) \quad (1 \leqslant j \leqslant n)$$

où les p_j sont des polynômes à $m = \dim(V)$ indéterminées, à coefficients dans K. On dit en outre que f est **homogène de degré** r si les p_j sont homogènes de degré r.
Montrer que ces définitions sont indépendantes des bases choisies dans V et W (i.e. que si les conditions énoncées sont satisfaites pour un choix particulier de ces bases, elles le sont pour tout autre choix). Montrer que, si le corps K est fini, toute application de V dans W est polynomiale (ce qui ôte beaucoup de son intérêt à cette notion dans ce cas...). On suppose K infini dans ce qui suit.
On note S(V, W) l'ensemble des applications polynomiales de V dans W, et $S_r(V, W)$ l'ensemble de celles qui sont homogènes de degré r. On pose enfin

$$S(V) = S(V, K), \qquad S_r(V) = S_r(V, K);$$

les éléments de S(V) [resp. $S_r(V)$] sont appelés les **fonctions polynomiales** [resp. les **fonctions polynomiales homogènes de degré** r] sur V.
Montrer que toute $f \in S(V, W)$ s'écrit d'une façon et d'une seule sous la forme

$$f = f_0 + f_1 + \cdots$$

où f_r est polynomiale et homogène de degré r, avec $f_r = 0$ pour presque tout r.
Montrer que S(V) est un sous-anneau de l'anneau de toutes les applications de l'ensemble V dans le corps K, que S(V) contient les applications linéaires et les applications constantes (qu'on identifie habituellement aux éléments de K, de sorte que K s'identifie canoniquement à un sous-corps de l'anneau S(V)). Soient $f_1, \ldots, f_m$ les fonctions coordonnées de V par rapport à une base de V; montrer que

$$S(V) = K[f_1, \ldots, f_m]$$

et que les éléments $f_1, \ldots, f_m$ sont algébriquement indépendants sur K.
Montrer que S(V, W) est un sous-espace vectoriel de l'espace vectoriel de toutes les applications de l'ensemble V dans l'espace vectoriel W. Montrer que, si $f \in S(V)$ et si $g \in S(V, W)$, l'application $h = fg$ de V dans W définie par

$$h(x) = f(x)g(x) \quad \text{pour tout } x \in V$$

est encore polynomiale. En déduire qu'on peut regarder S(V, W) comme un module sur l'anneau S(V). Soient (a_i) une base de V, (b_j) une base de W, et notons f_{ij} l'application *linéaire* de V dans W qui vérifie

$$f_{ij}(a_k) = \begin{cases} b_j & \text{si } k = i \\ 0 & \text{si } k \neq i; \end{cases}$$

montrer que les f_{ij} forment une *base* du S(V)-module S(V, W).
Soient U, V, W trois espaces vectoriels de dimension finie sur K, et

$$f : U \to V, \qquad g : V \to W$$

deux applications polynomiales. Montrer que l'application composée $g \circ f$ est polynomiale. Si f et g sont homogènes de degrés r et s, alors $g \circ f$ est homogène de degré rs.

18. Soit K un corps commutatif infini. On considère l'application polynomiale f de K dans K^3 donnée par

$$f(t) = (t^2 + t + 1,\ t^3 + t + 1,\ t^4 + t + 1);$$

trouver toutes les fonctions polynomiales sur K^3 qui sont nulles en tout point de $f(K)$. Quel sont les points de K^3 où toutes ces fonctions sont nulles?
Même question pour l'application de K^* dans K^3 donnée par

$$f(t) = \left(\frac{t+1}{t},\ \frac{t^2+1}{t},\ \frac{t^3+1}{t}\right).$$

¶ **19.** Soient K un anneau commutatif et M un K-module; on se propose de « plonger » M dans un module sur l'anneau K[X] des polynômes à une indéterminée à coefficients dans K. Pour cela, on considère l'ensemble, noté M[X], dont les éléments sont les suites

$$(m_0, m_1, \ldots)$$

d'éléments presque tous nuls de M; on définit une addition dans M[X] par la formule

$$(m'_0, m'_1, \ldots) + (m''_0, m''_1, \ldots) = (m'_0 + m''_0, m'_1 + m''_1, \ldots);$$

enfin, on définit le produit d'un élément de M[X] par un élément de K[X] en posant

$$(a_0, a_1, a_2, \ldots).(m_0, m_1, m_2, \ldots) = (a_0m_0, a_0m_1 + a_1m_0, \ldots)$$

Montrer qu'avec ces définitions l'ensemble M[X] est effectivement un K[X]-module; on l'appelle le **module des polynômes à une indéterminée, à coefficients dans** M. On identifie chaque $m \in M$ à l'élément $(m, 0, \ldots)$ de M[X]; montrer qu'on a alors

$$(m_0, m_1, m_2, \ldots) = m_0 + m_1X + m_2X^2 + \cdots$$

dans le K[X]-module M[X] (NB — On écrit ici les scalaires, i.e. les éléments de K[X], à droite des éléments de M[X] pour se conformer à la tradition suivant laquelle, dans un polynôme, on écrit les coefficients à gauche des monômes).
Soient M et N deux K-modules et u un homomorphisme de M dans N; montrer qu'il existe un et un seul homomorphisme

$$\bar{u} : M[X] \to N[X]$$

de K[X]-modules qui coïncide avec u sur M.
On suppose M libre de type fini; montrer qu'alors M[X] est un K[X]-module libre de type fini, et que toute base de M sur K est aussi une base de M[X] sur K[X].
(Pour une application des constructions précédentes, voir § 35, *Exercice* 10)

20. Soient K un anneau commutatif, E un K-module, et u un endomorphisme de E. Étant donné un polynôme

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

à coefficients dans K, on pose

$$f(u) = a_0.j_E + a_1u + \cdots + a_nu^n,$$

d'où un nouvel endomorphisme de E. Ceci fait, on considère l'application de l'ensemble produit K[X] × E dans l'ensemble E donnée par

$$(f, x) \mapsto f(u)(x);$$

montrer que l'ensemble E, muni de la loi de composition $(x, y) \mapsto x + y$ et de l'application qu'on vient de définir, est un *module sur l'anneau* K[X]; on le note E_u.
Réciproquement, soit M un K[X]-module; soit E le K-module déduit de M par restriction des scalaires (*) à l'anneau K; on considère l'homothétie de rapport X dans M comme une application u de E dans E. Montrer que u est un endomorphisme du K-module E, et que $M = E_u$. Autrement dit : *un module sur l'anneau* K[X] *s'identifie à un couple formé d'un module sur l'anneau* K *et d'un endomorphisme u de ce* K*-module.* (Ce résultat montre que l'étude des endomorphismes des K-modules revient à celle des K[X]-modules, ce qui sera confirmé dans les *Exercices* du § 35).
On se donne E et u comme ci-dessus; quels sont les sous-modules du K[X]-module E_u?
On considère deux K-modules E et F, un endomorphisme u de E, et un endomorphisme v de F. Quels sont les homomorphismes du K[X]-module E_u dans le K[X]-module F_v?

(*) Soient L un anneau, K un sous-anneau de L, et M un L-module à gauche. Le module déduit de M par restriction à K des scalaires s'obtient en considérant le groupe additif M et l'application $(a, m) \to am$ de K × M dans M qui coïncide, sur K × M, avec l'application de L × M dans M donnée dans la structure de L-module de M. Autrement dit, on garde les mêmes « vecteurs », l'addition reste la même, mais on ne regarde que les homothéties dont le rapport appartient à K. Par exemple, tout espace vectoriel *complexe* définit aussi un espace vectoriel *réel*.

¶ 21. En imitant les constructions de l'*Exercice* précédent, montrer que, si K est un anneau commutatif, les modules sur l'anneau de polynômes K[X, Y] s'identifient aux triplets (E, u, v) formés d'un K-module E et de deux endomorphismes u et v de E tels que $u \circ v = v \circ u$. Généralisation à n indéterminées?

¶¶ 22. Soient L un corps commutatif et K un sous-corps de L.
a) On considère un système d'équations linéaires

$$(*) \qquad \begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

à coefficients et seconds membres dans K, et un polynôme p à coefficients dans K et à n indéterminées. On suppose qu'il existe une solution

$$(x_1, \ldots, x_n) \in L^n$$

telle que $p(x_1, \ldots, x_n) \neq 0$; montrer que, si K est infini, il existe alors dans K^n une solution de (*) qui n'annule pas p (exemple **R** et **C**).
b) On considère deux matrices $A, B \in M_n(K)$. On suppose qu'il existe une matrice $V \in GL(n, L)$ telle que $B = VAV^{-1}$; montrer qu'alors il existe $U \in GL(n, K)$ telle que $B = UAU^{-1}$ (considérer l'équation $UA = BU$ avec la condition $\det(U) \neq 0$ et appliquer la question précédente). [NB — Ce résultat subsiste si K est un corps fini, mais la démonstration est nettement plus difficile; cf. § 35, *Exercice* 13].

¶ 23. Soient K un anneau commutatif et I l'idéal de K[X] engendré par X^{n+1}. Décrire l'anneau quotient $L = K[X]/I$ (on montrera que L est engendré par K et un élément ε assujetti à vérifier la relation $\varepsilon^{n+1} = 0$).
Trouver ses éléments inversibles. [L'anneau L intervient, pour $K = C$, dans la théorie des développements limités d'ordre n].

§ 29

1. On considère deux fractions rationnelles $f, g \in K(X_1, \ldots, X_n)$ où K est un anneau d'intégrité commutatif *infini*. On suppose qu'il existe dans l'ensemble K^n un ouvert de Zariski (§§ 27, 28, *Exercice* 1) non vide A tel que f et g soient définies et aient la même valeur en tout point $x \in A$. Montrer qu'alors $f = g$. (Ce résultat, notamment dans le cas classique où $K = \mathbf{R}$ ou $\mathbf{C}$, explique pourquoi on a le droit d'identifier toute fraction rationnelle à coefficients dans K à la fonction qu'elle définit sur une partie de K^n.)

2. Une fonction rationnelle à *une* variable ne possède aucun point d'indétermination (si $f = p/q$ où p et q s'annulent simultanément en a, mettre en facteur dans p et q les plus hautes puissances possibles de $X - a$).

3. Soient K un corps commutatif, a un élément de K, et A l'ensemble des fractions rationnelles $f \in K(X)$ qui sont définies en a. Montrer que A est un anneau de valuation du corps $K(X)$ (§ 8, *Exercice* 6) et que l'idéal des éléments non inversibles de A est formé des $f \in A$ telles que $f(a) = 0$.
Montrer que les $f \in K(X)$ qui peuvent s'écrire sous la forme $f = p/q$, où p et q sont des polynômes tels que

$$d^o(p) \leqslant d^o(q),$$

forment également un anneau de valuation de $K(X)$.

4. Soient L un corps commutatif, K un sous-corps de L, et $x_1, \ldots, x_n$ des éléments de L. On désigne par $K(x_1, \ldots, x_n)$ le plus petit sous-corps de L contenant K et les x_i (sous-corps de L **engendré** par K et les x_i); un corps contenant K comme sous-corps et engendré par K et un nombre fini d'éléments s'appelle une **extension de type fini** de K, ou un **corps de fonctions algébriques** sur K). Montrer que c'est l'ensemble des éléments de L qui peuvent s'écrire sous la forme

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

où $f \in K(X_1, \ldots, X_n)$ est définie en $(x_1, \ldots, x_n)$. Montrer que $K(x_1, \ldots, x_n)$ est isomorphe à $K(X_1, \ldots, X_n)$ si les x_i sont algébriquement indépendants sur K.

5. Soit K un corps commutatif. Étant donnée une fraction rationnelle $f \in K(X)$ non dans K, montrer que l'élément X du corps $K(X)$ est algébrique sur le sous-corps $K(f)$ engendré par K et f. En déduire qu'il en est de même de tout $g \in K(X)$.
Montrer qu'*étant donnés deux polynômes $p, q \in K[X]$, il existe une relation algébrique non triviale, à coefficients dans K, entre p et q.*

6. Soient L un corps commutatif et K un sous-corps de L.

a) Soient $x_1, \ldots, x_r, y, z$ des éléments de L; on suppose que z est algébrique sur le sous-corps $K(x_1, \ldots, x_r, y)$ mais non sur $K(x_1, \ldots, x_r)$; montrer qu'alors y est algébrique sur

$$K(x_1, \ldots, x_r, z).$$

b) On suppose que L est de **degré de transcendance fini** sur K, autrement dit qu'il existe un entier n tel que $n + 1$ éléments quelconques de L vérifient une relation algébrique non triviale à coefficients dans K. Montrer qu'on peut alors trouver des éléments $x_1, \ldots, x_r$ de L, en nombre fini, algébriquement indépendants sur K, et tels que tout élément de L soit algébrique sur le sous-corps $K(x_1, \ldots, x_r)$ (on dit alors que les x_i forment une **base de transcendance** de L sur K).

c) Soient $x_1, \ldots, x_r$ et $y_1, \ldots, y_s$ deux bases de transcendance de L sur K. Montrer qu'il existe un indice j tel que y_j ne soit pas algébrique sur $K(x_1, \ldots, x_{r-1})$ (observer que dans le cas contraire tout élément de L serait algébrique sur ce sous-corps, et en particulier x_r). En déduire, à l'aide de la question *a*), que $x_1, \ldots, x_{r-1}, y_j$ forment une base de transcendance de L sur K.

d) Déduire de là que deux bases de transcendance quelconques de L sur K ont le même nombre d'éléments (qu'on appelle le **degré de transcendance** de L sur K). Montrer que ce nombre est le plus grand entier n tel qu'on puisse trouver n éléments de L algébriquement indépendants sur K.

e) Montrer que *si $f_1, \ldots, f_{n+1}$ sont $n + 1$ fractions rationnelles à n indéterminées, à coefficients dans un corps commutatif* K, *il existe une relation algébrique non triviale, à coefficients dans* K, *entre $f_1, \ldots, f_{n+1}$.*

f) On suppose le corps commutatif K *infini*. Soit A un ouvert de Zariski (§§ 27, 28, *Exercice* 1) non vide dans K^p; on dit qu'une application f de A dans K^q est **rationnelle** s'il existe des fractions rationnelles

$$f_1, \ldots, f_q \in K(X_1, \ldots, X_p)$$

telles que $f_1, \ldots, f_q$ soient définies en tout $x \in A$ et que l'on ait

$$f(x) = (f_1(x), \ldots, f_q(x)) \quad \text{pour tout } x \in A$$

(Cette notion généralise celle d'application polynomiale des §§ 27, 28, *Exercice* 17.) Cela dit, montrer que si une application rationnelle de A dans K^q est *surjective*, on a $p \geqslant q$. (Ce résultat montre que les phénomènes « pathologiques » du type de la courbe de Peano — existence d'une application *continue* d'une droite *sur* un plan, par exemple — ne peuvent pas se produire lorsqu'on se limite à des applications définies par des fonctions polynomiales ou rationnelles.)
[La notion de degré de transcendance exposée dans cet *Exercice* est à la base de la définition de la dimension d'une variété algébrique.
Soit V une **variété algébrique** dans $\mathbf{C}^n$, i.e. une partie de $\mathbf{C}^n$ définie par un nombre fini d'équations

$$f_1(x) = \cdots = f_r(x) = 0$$

où $f_1, \ldots, f_r$ sont des polynômes à n variables à coefficients dans $\mathbf{C}$. On appelle *fonction polynomiale* sur V toute application de V dans $\mathbf{C}$ qui est la restriction à V d'une fonction polynomiale sur $\mathbf{C}^n$. Ces fonctions polynomiales sur V forment évidemment un anneau A contenant $\mathbf{C}$ (fonctions constantes), et d'ailleurs engendré sur $\mathbf{C}$ par n éléments convenablement choisis (par exemple les restrictions à V des fonctions coordonnées de $\mathbf{C}^n$). On dit que V est **irréductible** si l'anneau A est intègre; il revient au même, comme on peut le démontrer, d'exiger que V

ne peut pas s'écrire comme réunion de deux autres variétés algébriques distinctes de V. Si V est irréductible, on peut former le corps L des fractions de A; en notant $f_1, \ldots, f_n$ les restrictions à V des fonctions coordonnées de $\mathbf{C}^n$, il est clair que

$$\mathrm{L} = \mathbf{C}(f_1, \ldots, f_n).$$

On dit que L est le **corps des fonctions rationnelles de la variété** V. Cela fait, L est de degré de transcendance fini sur $\mathbf{C}$, et on appelle alors **dimension** de V le degré de transcendance de L sur $\mathbf{C}$. Une « courbe » est de dimension 1, une « surface » de dimension 2, etc...
On démontre que la dimension p d'une variété algébrique irréductible V est aussi le plus grand entier tel que l'on puisse construire une chaîne croissante

$$\mathrm{V}_0 \subset \mathrm{V}_1 \subset \cdots \subset \mathrm{V}_p = \mathrm{V}$$

de variétés algébriques irréductibles non vides et deux à deux distinctes. Une « surface » contient une « courbe » qui contient un « point », ce qui explique (sic) pourquoi une « surface » est de dimension 2.
Les variétés algébriques dans $\mathbf{C}^n$ sont utilisées en Analyse, notamment pour étudier les systèmes d'équations aux dérivées partielles linéaires à coefficients constants. Considérons par exemple l'équation

$$\sum_{i_1, \ldots, i_n \geqslant 0} a_{i_1 \ldots i_n} \frac{\partial^{i_1 + \cdots + i_n} f}{\partial x_1^{i_1} \ldots \partial x_n^{i_n}} = 0$$

où f est une fonction inconnue de n variables réelles, et où les coefficients $a_{i_1 \ldots i_n}$ sont des constantes complexes presque toutes nulles. Si l'on cherche les solutions de la forme

$$f(x_1, \ldots, x_n) = e^{u_1 x_1 + \cdots + u_n x_n}$$

où $u_1, \ldots, u_n$ sont des constantes complexes, on est évidemment ramené à résoudre l'équation

$$\Sigma a_{i_1 \ldots i_n} . u_1^{i_1} \ldots u_n^{i_n} = 0.$$

i.e. à étudier l'hypersurface algébrique de $\mathbf{C}^n$ définie par cette équation.]

7. Trouver les pôles et les points d'indétermination des fractions rationnelles suivantes :

$$\frac{X}{Y}\ ; \quad \frac{X-Y}{XY}\ ; \quad \frac{(X^2-1)(Y^2-1)}{X^2+Y^2-1}\ ; \quad \frac{X+Y+Z}{X-Y}\ ; \quad \frac{X-Z}{Y-Z}$$

(on prendra $\mathbf{C}$ pour corps de base).

¶ **8.** Soit K un corps commutatif; on considère (§§ 27, 28, *Exercice* 11) l'anneau K[[X]] des séries formelles à une variable à coefficients dans K. Comme c'est un anneau d'intégrité on peut former son corps des fractions, qu'on note K((X)). Montrer que tout élément de celui-ci s'écrit d'une façon et d'une seule sous la forme du produit d'une puissance (éventuellement négative) de X par une série formelle dont le terme constant n'est pas nul, i.e. sous la forme d'une « série »

$$(*) \qquad \sum_{n=-\infty}^{n=+\infty} a_n X^n$$

à coefficients a_n dans K, avec la condition que les entiers n *négatifs* tels que $a_n \neq 0$ soient en nombre fini.
On notera que, comme K[X] est un sous-anneau de K[[X]], le corps K((X)) contient un sous-corps isomorphe à K(X), en sorte que toute fraction rationnelle à une variable à coefficients dans K peut se représenter par une série de la forme (*). Trouver les séries formelles (*) représentant les fractions rationnelles suivantes :

$$\frac{1}{X - X^2}\ ; \qquad \frac{X^2 + X + 1}{X^4 - X^2}\ .$$

Montrer que la série (*) représentant une fraction rationnelle f ne comporte aucune puissance négative de X lorsque f est définie en $x = 0$, et réciproquement (*).
Montrer que K[[X]] est un anneau de valuation (§ 8, *Exercice* 6) du corps K((X)).

¶ **9.** Soient A un anneau commutatif et S une partie de A; on suppose que S contient 1 mais ne contient pas 0, et que l'on a $xy \in S$ quels que soient $x \in S$, $y \in S$ (si A est un anneau d'intégrité on peut prendre par exemple pour S l'ensemble des éléments non nuls de A; dans le cas général, un exemple important s'obtient en prenant pour S l'ensemble des $x \in A$ qui n'appartiennent pas à un idéal premier donné de A).

a) Soit F l'ensemble des couples (x, s) avec $x \in A$, $s \in S$; étant donnés deux éléments $y' = (x', s')$ et $y'' = (x'', s'')$ de F, on désigne par $R\{y', y''\}$ la relation

$$\text{il existe un } s \in S \text{ tel que } \quad s(x's'' - x''s') = 0.$$

Montrer que R est une relation d'équivalence sur F. Que se passe-t-il lorsque A est intègre et qu'on prend pour S l'ensemble des éléments non nuls de A?

b) Soient A_S l'ensemble quotient F/R et θ l'application canonique de F sur F/R. Montrer qu'il existe sur A_S une et une seule structure d'anneau commutatif telle que l'on ait les formules

$$\theta(x, s) + \theta(y, t) = \theta(xt + ys, st)$$
$$\theta(x, s) . \theta(y, t) = \theta(xy, st).$$

c) Montrer que l'application j de A dans A_S donnée par

$$j(x) = \theta(x, 1)$$

est un homomorphisme d'anneaux, que $j(s)$ est inversible dans A_S pour tout $s \in S$, et que tout élément de A_S est quotient d'un élément $j(x)$, $x \in A$, par un élément $j(s)$, $s \in S$. Quel est le noyau de l'homomorphisme j? A quelle condition j est-il injectif?

d) Soit f un homomorphisme de A dans un anneau commutatif K. Pour que $f(s)$ soit inversible dans K quel que soit $s \in S$, il faut et il suffit que f soit composé de l'homomorphisme j de la question précédente et d'un homomorphisme de l'anneau A_S dans l'anneau K.

e) Soient A un anneau d'intégrité commutatif, K son corps des fractions, et $\mathfrak{p}$ un idéal premier de A (i.e. tel que $\mathfrak{p} \neq A$ et que la relation $xy \in \mathfrak{p}$ implique $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$); on prend pour S le complémentaire de $\mathfrak{p}$ dans A. Montrer que l'anneau A_S est isomorphe au sous-anneau $A_{\mathfrak{p}}$ de K formé des fractions qui peuvent se mettre sous la forme x/y avec $x, y \in A$ et $y \notin \mathfrak{p}$.

(*) L'opération qui, étant donnés deux polynômes $f, g \in K[X]$, consiste à écrire sous la forme (*) la fraction rationnelle f/g est connue dans les ouvrages anciens sous le nom de *division de f par g suivant les puissances croissantes de* X; elle consiste aussi, pour chaque entier $r \geqslant 0$ (et si le terme constant de g n'est pas nul, cas auquel on peut toujours se ramener trivialement), à trouver un polynôme q de degré $\leqslant r$, tel que $f(X) - q(X)g(X)$ soit multiple de X^{r+1}. Le polynôme q s'obtient en supprimant les termes de degré $> r$ de la série formelle (*) qui représente f/g.
Dans la pratique, on doit effectuer ces opérations lorsqu'on veut développer en série entière ou de Laurent le quotient de deux polynômes ou séries entières, ou en trouver des développements limités.

f) Les hypothèses restant celles de *e*), on associe à chaque idéal $\mathfrak{a}$ de l'anneau $A_{\mathfrak{p}}$, distinct de $A_{\mathfrak{p}}$, l'idéal $A \cap \mathfrak{a}$ de l'anneau A. Montrer qu'on obtient de cette façon une bijection de l'ensemble des idéaux de $A_{\mathfrak{p}}$ distincts de $A_{\mathfrak{p}}$ sur l'ensemble des idéaux de A contenus dans $\mathfrak{p}$. Quelle est l'application réciproque?

g) Soient L un corps commutatif et $a_1, \ldots, a_n$ des éléments de L. On prend

$$A = L[X_1, \ldots, X_n]$$

et pour $\mathfrak{p}$ l'ensemble des polynômes $f \in A$ tels que $f(a_1, \ldots, a_n) = 0$. Montrer que $A_{\mathfrak{p}}$ est l'ensemble des fractions rationnelles $f(X_1, \ldots, X_n)$, à coefficients dans L, qui sont définies au point $(a_1, \ldots, a_n)$ de K^n.

h) Étendre les résultats de la question *f*) au cas d'un anneau de fractions A_S quelconque.

10. Soient A un anneau d'intégrité commutatif et K son corps des fractions. Montrer que le corps des fractions de l'anneau de polynômes A[X] est canoniquement isomorphe au corps de fractions rationnelles K(X).

11. Soient A un anneau d'intégrité commutatif, M un A-module, et K le corps des fractions de A. On se propose de montrer que, *si* M *est sans torsion* (§ 10, *Exercice* 11; les résultats de cet Exercice ne seront pas utilisés ici), *on peut plonger* M *dans un espace vectoriel sur* K (exemple trivial : A^n se plonge dans K^n).
On ne fait aucune hypothèse sur M jusqu'à nouvel ordre.

a) Soit F l'ensemble des couples (m, s) avec $m \in M$, $s \in A$ et $s \neq 0$. Étant donnés deux éléments $x' = (m', s')$ et $x'' = (m'', s'')$ de F, on note $R\{x', x''\}$ la relation

$$\text{il existe un } s \in A \text{ tel que } s(s'm'' - s''m') = 0 \text{ et } s \neq 0.$$

Montrer que R est une relation d'équivalence sur l'ensemble F.

b) Soit V l'ensemble quotient F/R; on note θ l'application canonique de F sur V. Montrer qu'on peut définir la somme de deux éléments de V de telle sorte que l'on ait

$$\theta(m', s') + \theta(m'', s'') = \theta(s''m' + s'm'', s's'')$$

quels que soient (m', s'), $(m'', s'') \in F$, et que V, muni de cette loi de composition, est un groupe commutatif.

c) Montrer qu'il existe une application $(\lambda, x) \to \lambda x$ de $K \times V$ dans V qui vérifie la condition suivante : si $\lambda = u/s$ et si $x = \theta(m, t)$ (avec $u, s, t \in A$, $m \in M$, et s, t non nuls), on a

$$\lambda x = \theta(um, st).$$

Montrer que le groupe commutatif V, muni de cette application, est un espace vectoriel sur K.

d) On définit une application « canonique » j de M dans V par

$$j(m) = \theta(m, 1);$$

montrer que c'est un homomorphisme de A-modules (NB : comme V est un espace vectoriel sur K, on peut *a fortiori* regarder V comme un A-module), dont le noyau est le sous-module de torsion de M (i.e. l'ensemble des m tels que l'on ait $sm = 0$ pour au moins un $s \in A$ *non nul*). En déduire que, si M est sans torsion, j est un isomorphisme de M sur un sous-module de V. Exemple (en prenant $A = \mathbf{Z}$) : tout groupe commutatif sans torsion se plonge dans un espace vectoriel rationnel.

e) On suppose M sans torsion et de type fini. Montrer que V est de dimension finie sur K. Soit $n = \dim(V)$ (on dit que n est le rang de M); montrer qu'il existe deux bases $(a_i)_{1 \leqslant i \leqslant n}$ et $(b_i)_{1 \leqslant i \leqslant n}$ de V telles que, si l'on désigne par P et Q les sous-A-modules (isomorphes à A^n) de V engendrés par les a_i et b_i respectivement, on ait $P \subset M \subset Q$.

f) Déduire de là et du Théorème 3 du § 18 le résultat suivant : *si* A *est un anneau principal, tout* A*-module* M *sans torsion et de type fini est isomorphe à* A^n *où* n *est le rang de* M. Traduction lorsque $A = \mathbf{Z}$?

g) Soit M un module de type fini sur un anneau principal A. Soit T le sous-module de torsion de M. Montrer que M/T est libre de type fini. En déduire (à l'aide de l'*Exercice* 8 du § 17) que M est isomorphe au produit direct de T et d'un A-module libre de type fini. (Ce résultat ramène l'étude des modules de type fini à celle des modules *de torsion* de type fini, qui sera faite au § 31, *Exercices* 8, 9, 10.)

h) Soient M un module libre de type fini sur un anneau principal A et M' un sous-module de M. Montrer que les propriétés suivantes sont équivalentes : *i*) M' est facteur direct dans M *ii*) le module quotient M/M' est sans torsion *iii*) quels que soient $a \in A$ et $x \in M$, la relation $ax \in M'$ implique $a = 0$ ou $x \in M'$. Retrouver à partir de là le résultat du § 18, *Exercice* 2.

i) Soit M' un sous-groupe de $\mathbf{Z}^n$ défini par un système d'équations linéaires et homogènes à coefficients entiers. Montrer que toute base de M' fait partie d'une base de $\mathbf{Z}^n$.

12. On trouve, dans un manuel d'Algèbre destiné aux élèves des Lycées et Collèges, la phrase suivante : « Sous réserve de ne pas donner aux variables des valeurs qui annulent le numérateur ou le dénominateur, l'ensemble des fractions rationnelles muni des lois d'addition et de multiplication présente une structure de corps. » Que pensez-vous de cet énoncé?

§ 30

1. Soit K un corps commutatif de caractéristique 0 (par exemple $K = \mathbf{C}$). Montrer que l'équation

$$\frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + 1 = 0$$

n'a aucune racine multiple dans K.

2. Soit K un corps commutatif. Trouver un polynôme $f \in K[X]$ de degré 7 tel que 1 soit racine multiple d'ordre 4 au moins de $f(X) + 1$, et -1 racine multiple d'ordre 4 au moins de $f(X) - 1$. Généraliser en remplaçant les entiers 4 et 7 par n et $2n - 1$.

3. Chacun des polynômes suivants admet 1 pour racine; déterminer son ordre de multiplicité :

$$X^{2n} - nX^{n+1} + nX^{n-1} - 1; \qquad X^{2n+1} - (2n+1)X^{n+1} + (2n+1)X^n - 1;$$
$$X^{2n} - n^2X^{n+1} + 2(n^2-1)X^n - n^2X^{n-1} + 1.$$

4. Soit f un polynôme à une variable à coefficients dans un corps commutatif K. On suppose $f' = 0$. Montrer que f est constant si K est de caractéristique 0, et que f est un polynôme en X^p si K est de caractéristique $p \neq 0$. Réciproque?

¶ **5.** Soit K un corps commutatif de caractéristique 0. On se propose de trouver toutes les applications

$$t \mapsto U(t)$$

de K dans l'anneau $M_n(K)$ qui vérifient

$$U(x+y) = U(x)U(y) \quad \text{quels que soient } x, y \in K,$$
$$U(0) = 1_n$$

et qui sont de plus polynomiales, i.e. de la forme

$$U(t) = A_0 + A_1 t + \cdots + A_r t^r + \cdots$$

où les matrices $A_r \in M_n(K)$ sont presque toutes nulles.

a) Montrer que la dérivée $U'(t)$ de la fonction polynomiale $U(t)$ vérifie

$$U'(t) = A_1 . U(t).$$

b) Montrer que la matrice $A_1 = N$ est nilpotente et que

$$U(t) = \sum_{r \geq 0} N^r \frac{t^r}{r!} = \exp(tN)$$

(cf. § 8, *Exercice* 2).

c) Montrer inversement que, pour toute matrice nilpotente N, l'application

$$t \mapsto \exp(tN)$$

satisfait aux conditions requises.

d) Trouver la matrice N dans le cas de la fonction $U(t)$ du § 12, *Exercice* 11, et *vérifier* dans ce cas qu'on a bien $U(t) = \exp(tN)$.

6. Soit K un corps commutatif de caractéristique 0. Montrer qu'il n'existe aucun polynôme $f \in K[X]$ non nul tel que l'on ait

$$f(x+y) = f(x)f(y)$$

quels que soient $x, y \in K$. Même question pour la relation

$$f(xy) = f(x) + f(y).$$

Quels sont les polynômes tels que

$$f(x+y) = f(x) + f(y)?$$

¶ **7.** Soit K un corps de caractéristique $p \neq 0$.

a) Montrer qu'on a

$$(x+y)^p = x^p + y^p$$

quels que soient $x, y \in K$. En déduire plus généralement que

$$(x+y)^q = x^q + y^q$$

si q est une puissance de p.

b) Montrer que l'application $x \to x^p$ est un isomorphisme de K sur un sous-corps de K (que l'on note K^p). Montrer que $K^p = K$ si K est fini.

c) Quels sont les polynômes $f \in K[X]$ vérifiant

$$f(x+y) = f(x) + f(y)$$

quels que soient $x, y \in K$?

¶ **8.** Soit K un corps de caractéristique $p \neq 0$. Montrer que, pour $n \in \mathbf{Z}$ et $x \in K$, l'élément $nx \in K$ ne dépend que de x et de la classe de n modulo p. En déduire qu'on peut considérer K comme un espace vectoriel sur le corps $\mathbf{Z}/p\mathbf{Z}$.
Montrer que *le nombre d'éléments d'un corps fini de caractéristique p est une puissance de p.*

9. Soit p un nombre premier. Montrer que le coefficient binômial $\binom{p^n}{r}$ est divisible par p pour tout $n \geq 1$ et tout r tel que $1 \leq r \leq p^n - 1$. (Utiliser l'*Exercice* 7 pour le corps $K = \mathbf{Z}/p\mathbf{Z}$.) Démonstration élémentaire?

10. Soit $f(X_1, \ldots, X_n)$ un polynôme à n variables à coefficients dans un anneau commutatif K. On suppose f homogène de degré r. Montrer que

$$X_1 f'_1(X_1, \ldots, X_n) + \ldots + X_n f'_n(X_1, \ldots, X_n) = r.f(X_1, \ldots, X_n)$$

où f'_i est la dérivée partielle de f par rapport à X_i. Cette relation (connue sous le nom d'identité d'Euler) caractérise-t-elle les polynômes homogènes de degré r?

11. Soit

$$(*) \qquad a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

une équation algébrique à coefficients a_i entiers rationnels; on suppose dans ce qui suit les a_i premiers entre eux (cas auquel on peut évidemment toujours se ramener en divisant les a_i par leur pgcd).
Soit $x = p/q$ une racine rationnelle de l'équation $(*)$; on suppose p et q premiers entre eux. Montrer que p divise a_0 et que q divise a_n.
Application : trouver les racines rationnelles des équations suivantes :

$$6x^4 - 11x^3 - x^2 - 4 = 0$$
$$2x^3 + 12x^2 + 13x + 15 = 0$$
$$6x^5 + 11x^4 - x^3 + 5x - 6 = 0$$
$$x^6 + 3x^5 + 4x^4 + 3x^3 - 15x^2 - 16x + 20 = 0$$
$$2x^6 + x^5 - 9x^4 - 6x^3 - 5x^2 - 7x + 6 = 0.$$

12. Soit K un anneau commutatif. On considère l'anneau $L = K[\varepsilon]$ engendré par K et un élément ε tel que

$$\varepsilon^2 = 0$$

(faire $n = 1$ dans l'*Exercice* 23 du § 28). Pour que l'application

$$x \mapsto x + D(x)\varepsilon$$

de K dans L soit un homomorphisme, il faut et il suffit que D doit une dérivation de l'anneau K.

13. Dans quels corps a-t-on l'identité

$$x^4 - x^2 + 1 = (x^2 - 5x + 1)(x^2 + 5x + 1)?$$

¶ **14.** Soit K un corps de caractéristique $p \neq 0$. Si un $x \in K$ vérifie $x^n = 1$ pour un entier n, il existe un entier r *non divisible par* p tel que

$$x^r = 1.$$

¶ **15.** Soit K un anneau commutatif. On définit (par récurrence sur l'entier $n \geqslant 0$) les **opérateurs différentiels d'ordre n au plus sur** K comme suit : ce sont des applications D de K dans K, vérifiant

$$D(x + y) = D(x) + D(y) \quad \text{quels que soient } x, y \in K,$$

et possédant en outre la propriété suivante : si $n = 0$, il existe un $a \in K$ tel que

$$D(x) = ax \quad \text{pour tout } x \in K;$$

si $n \geqslant 1$, il existe, pour tout $x \in K$, un opérateur différentiel D_x d'ordre $n - 1$ au plus sur K tel que l'on ait

$$D(xy) = x.D(y) + D_x(y) \quad \text{pour tout } y \in K.$$

a) Déterminer tous les opérateurs différentiels d'ordre 1 au plus sur K.
b) Montrer que si D′ et D″ sont des opérateurs différentiels d'ordres r et s au plus, l'application composée

$$D'' \circ D'$$

est un opérateur différentiel d'ordre $r + s$ au plus, et le crochet de Jacobi

$$D'' \circ D' - D' \circ D''$$

un opérateur différentiel d'ordre $r + s - 1$ au plus.
c) Soit D un opérateur différentiel d'ordre n au plus. On considère une famille $(x_i)_{i \in I}$ d'éléments de K, avec Card (I) $= n + 1$. Pour toute partie F de I, on pose

$$x_F = \prod_{i \in F} x_i \quad \text{et } x_\varnothing = 1.$$

Montrer qu'on a l'identité

$$\sum_{F \subset I} (-1)^{\mathrm{Card}(F)} x_F D(x_{I-F}) = 0.$$

Montrer réciproquement que toute application D de K dans K, possédant cette propriété et telle que $D(x + y) = D(x) + D(y)$, est un opérateur différentiel d'ordre n au plus dans K.
d) Déduire de là une formule pour calculer les dérivées partielles d'ordre p d'un produit de $n + 1$ polynômes, par récurrence sur n. Cas $p = 1$?
e) On prend

$$K = k[X_1, \ldots, X_r]$$

où k est un anneau commutatif. Construire tous les opérateurs différentiels dans K qui sont nuls sur k.

§ 31

1. Soient $x_1, \ldots, x_n$ des éléments non nuls d'un anneau principal K et d un de leurs pgcd; on choisit $u_1, \ldots, u_n \in K$ tels que $u_1x_1 + \cdots + u_nx_n = d$. Montrer que $u_1, \ldots, u_n$ sont premiers entre eux.

¶ **2.** Soient M un module libre de type fini sur un anneau principal K et a un élément non nul de M. Montrer que les cinq propriétés suivantes sont équivalentes : a fait partie d'une base de M; il existe une forme linéaire f sur M telle que $f(a) = 1$; les coordonnées de a par rapport à *une* base de M sont premières entre elles; les coordonnées de a par rapport à *toute* base de M sont premières entre elles; si $a = ux$ pour un $u \in K$ et un $x \neq 0$ dans M, alors u est inversible; si $ux = va$ avec $u, v \in K$ et $x \in M$ non nul alors v est multiple de u. (On utilisera l'*Exercice* 2 du § 18 et l'*Exercice* 11, *h*), du § 29). Un vecteur $a \in M$ satisfaisant aux conditions précédentes est dit **primitif.**

3. Soit M un module libre de type fini sur un anneau principal K. Montrer que tout $x \in M$ est multiple d'au moins un vecteur primitif de M. Faire le calcul en prenant $K = \mathbf{Z}$, $M = \mathbf{Z}^4$ et $x = (126, 210, 168, 504)$.

4. Soient $a_1, \ldots, a_n$ des éléments d'un anneau principal K; pour qu'il existe une matrice

$$U \in GL(n, K)$$

dont la première ligne (resp. colonne) soit précisément $a_1, \ldots, a_n$, il faut et il suffit que $a_1, \ldots, a_n$ soient premiers entre eux. On peut alors choisir U de telle sorte que dét(U) = 1, i.e. supposer

$$U \in SL(n, K).$$

5. Construire une matrice $U \in SL(3, \mathbf{Z})$ dont la première colonne soit 2, 3, 4.

6. Construire une matrice $U \in SL(3, \mathbf{Z})$ dont la seconde colonne soit 2, 3, 4.

¶ **7.** Soit M un module libre de type fini sur un anneau principal K.

a) Montrer que, si a est un élément non nul de M, le pgcd des coordonnées de a par rapport à une base de M est indépendant du choix de celle-ci. Quelle est l'interprétation « géométrique » de ce résultat (cf. *Exercice* 3) ?

b) Soit M' un sous-module non nul de M. On choisit une base de M et on considère l'idéal de K engendré par toutes les coordonnées de tous les éléments de M'. Montrer que cet idéal est indépendant du choix de la base. Montrer qu'il est engendré par les coordonnées d'un ensemble quelconque de générateurs de M'. [Cet idéal, ou l'un quelconque de ses générateurs, est appelé le *premier facteur invariant* de M' dans M; voir l'*Exercice* suivant.]

¶¶ **8.** Soient M un module libre de type fini sur un anneau principal K et M' un sous-module non nul de M; on note n et r les rangs (nombres d'éléments d'une base) de M et M'. On se propose de démontrer le résultat que voici : *il existe une base* $a_1, \ldots, a_n$ *de* M *et des éléments* $d_1, \ldots, d_r$ *de* K *tels que les vecteurs* $d_1a_1, \ldots, d_ra_r$ *forment une base de* M' *et que* d_i *divise* d_{i+1} *pour* $1 \leqslant i \leqslant r - 1$.

a) Montrer que, pour toute forme linéaire f sur M, l'ensemble $f(M') \subset K$ est un idéal de K.

b) Montrer qu'il existe une forme linéaire f_1 sur M telle que, pour toute forme linéaire f sur M, la relation

$$f_1(M') \subset f(M') \quad \text{implique} f_1(M') = f(M').$$

Montrer qu'on a alors

$$f_1(M) = K.$$

c) On choisit f_1 satisfaisant à *b*); on pose

$$f_1(M') = (d_1)$$

et on choisit un vecteur $u_1 \in M'$ tel que

$$f_1(u_1) = d_1.$$

Montrer qu'on a

$$f(u_1) \in (d_1)$$

pour toute forme linéaire f sur M (en posant $f(u_1) = d$, montrer qu'il existe une combinaison linéaire g de f et f_1 telle que $g(u_1)$ soit un pgcd de d et d_1).

d) Déduire de (*c*) qu'on a

$$u_1 = d_1e_1$$

pour un vecteur $e_1 \in M$, tel que $f_1(e_1) = 1$.

e) Montrer que M est somme directe du sous-module engendré par e_1 et de $\mathrm{Ker}(f_1)$; et que M' est somme directe du sous-module engendré par u_1 et de $M' \cap \mathrm{Ker}(f_1)$. Montrer que $f(M') \subset f_1(M')$ pour toute f.

f) Achever la démonstration par récurrence sur n.

¶¶ **9.** Soit A une matrice à n lignes et p colonnes à coefficients dans un anneau principal K. Montrer à l'aide de l'*Exercice* 8 qu'il existe des matrices

$$U \in GL(n, K) \quad \text{et} \quad V \in GL(p, K)$$

telles que l'on ait

$$UAV = \begin{pmatrix} d_1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & d_2 & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & d_r & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix},$$

où $d_1, \ldots, d_r$ sont des éléments non nuls de K tels que chacun divise le suivant. Les éléments

$d_1, \ldots, d_r$ sont appelés les **facteurs invariants** de la matrice A; on verra (*Exercice* 11) que les idéaux $(d_1), \ldots, (d_r)$ sont entièrement déterminés par A.

¶¶ **10.** Montrer que *tout groupe commutatif de type fini est isomorphe au produit direct d'un groupe* $\mathbf{Z}^q$ *et de groupes cycliques finis* $\mathbf{Z}/d_1\mathbf{Z}, \ldots, \mathbf{Z}/d_r\mathbf{Z}$ *où chaque* d_i *divise* d_{i+1}. (Observer qu'un K-module de type fini, où K est un anneau arbitraire, est isomorphe à un quotient M/M′ où M est libre de type fini — et appliquer *l'Exercice* 8). Comment ce résultat se généralise-t-il à un anneau principal quelconque?

¶¶ **11.** On reprend les hypothèses et notations de l'*Exercice* 8, dont on utilise les résultats.

a) Soient $j_1, \ldots, j_h$ des entiers tels que

$$1 \leqslant j_1 < j_2 < \ldots < j_h \leqslant r;$$

montrer que $d_1 \ldots d_h$ divise $d_{j_1} \ldots d_{j_h}$.

b) Soit h tel que $1 \leqslant h \leqslant r$; montrer que, si f est une forme h-linéaire alternée sur M, le produit $d_1 \ldots d_h$ divise $f(x_1, \ldots, x_h)$ quels que soient $x_1, \ldots, x_h \in \mathrm{M}'$; montrer qu'on peut en outre choisir f et $x_1, \ldots, x_h \in \mathrm{M}'$ de telle sorte que

$$d_1 \ldots d_h = f(x_1, \ldots, x_h);$$

en déduire que $d_1 \ldots d_h$ est un pgcd des éléments de K de la forme $f(x_1, \ldots, x_h)$ et en conclure que *les idéaux* (d_i) *sont entièrement déterminés par le module* M *et le sous-module* M′ (i.e. ne dépendent pas du choix des bases construites dans l'*Exercice* 8).

c) Soient $(a_i)_{1 \leqslant i \leqslant n}$ une base quelconque de M et $(b_j)_{1 \leqslant j \leqslant p}$ un système quelconque de générateurs de M′; on note A la matrice (à n lignes et p colonnes) formée avec les coordonnées des b_j par rapport à la base (a_i) de M.
Montrer que, pour $1 \leqslant h \leqslant r$, *l'élément* $d_1 \ldots d_h$ *est un pgcd des mineurs d'ordre* h *de la matrice* A.

d) En déduire que les facteurs $d_1, \ldots, d_r$ de *l'Exercice* 9 se calculent de même.

e) Soient A et B deux matrices à n lignes et p colonnes à coefficients dans un anneau principal K. Pour que A et B soient **équivalentes** (i.e. pour qu'il existe des matrices U et V *inversibles* telles que B = UAV) il faut et il suffit que A et B aient le même rang et les mêmes facteurs invariants.

(NB. — On exprime souvent ce résultat en introduisant, au lieu des facteurs invariants de A, ses **diviseurs élémentaires**

$$e_1 = d_1, e_2 = d_2/d_1, \ldots, e_r = d_r/d_{r-1})$$

¶¶ **12.** Soient K un anneau principal et

$$a_j = (\alpha_{1j}, \ldots, \alpha_{nj}) \quad (1 \leqslant j \leqslant p)$$

des éléments de K^n. Pour qu'ils fassent partie d'une base de K^n, il faut et il suffit que les mineurs d'ordre p de la matrice

$$\begin{pmatrix} \alpha_{11} & \ldots & \alpha_{1p} \\ \ldots & \ldots & \ldots \\ \alpha_{n1} & \ldots & \alpha_{np} \end{pmatrix}$$

formée avec les composantes des vecteurs donnés soient *premiers entre eux* (et en particulier non tous nuls).

¶¶ **13.** Soient K un anneau principal et n et p deux entiers tels que $1 \leqslant p \leqslant n$. Soit A une matrice à n lignes et p colonnes à coefficients dans K. Pour qu'on puisse compléter A en une matrice carrée d'ordre n et *inversible* sur l'anneau K, il faut et il suffit que le pgcd des mineurs d'ordre p de A soit égal à 1.

14. Trouver toutes les matrices à coefficients entiers rationnels, de la forme

$$\begin{pmatrix} 1 & 4 & * \\ 2 & 5 & * \\ 1 & 6 & * \end{pmatrix},$$

et de déterminant 1.

¶ **15.** Soit A une matrice à coefficients dans un anneau commutatif K; on appelle **opération élémentaire** sur A une opération consistant soit à permuter deux lignes (resp. colonnes) de A, soit à ajouter à une ligne (resp. colonne) une combinaison linéaire des autres lignes (resp. colonnes), soit à multiplier une ligne (resp. colonne) par un élément inversible de K.

a) Montrer que toute matrice déduite de A par une succession d'opérations élémentaires est équivalente à A (i.e. de la forme UAV avec U, V inversibles sur K).

b) On suppose $\mathrm{K} = \mathbf{Z}$, et $\mathrm{A} \neq 0$. Soit d_1 le plus petit entier strictement positif possédant la propriété suivante : il existe une matrice qui se déduit de A par une succession d'opérations élémentaires, et dont d_1 est un coefficient. Montrer qu'il existe alors une matrice de la forme

$$\begin{pmatrix} d_1 & 0 \\ 0 & \mathrm{A}_1 \end{pmatrix}$$

(où A_1 possède une ligne et une colonne de moins que A) qui se déduit de A par une succession d'opérations élémentaires, et de plus que tous les coefficients de A_1 sont multiples de d_1.

c) Déduire de là, pour $\mathrm{K} = \mathbf{Z}$, une nouvelle démonstration du résultat de l'*Exercice* 9 (donc aussi de l'*Exercice* 8), et une méthode pratique pour réduire une matrice à coefficient dans $\mathbf{Z}$ à la forme canonique de l'*Exercice* 9.

d) Appliquer cette méthode aux matrices suivantes :

$$\begin{pmatrix} 0 & 2 & 4 & -1 \\ 6 & 12 & 14 & 5 \\ 0 & 4 & 14 & -1 \\ 10 & 6 & -4 & 11 \end{pmatrix}, \quad \begin{pmatrix} 0 & 6 & -9 & -3 \\ 12 & 24 & 9 & 9 \\ 30 & 42 & 45 & 27 \\ 66 & 78 & 81 & 63 \end{pmatrix},$$

$$\begin{pmatrix} 17 & -28 & 45 & 11 & 39 \\ 24 & -37 & 61 & 13 & 50 \\ 25 & -7 & 32 & -18 & -11 \\ 31 & 12 & 19 & -43 & -55 \\ 42 & 13 & 29 & -55 & -68 \end{pmatrix}.$$

16. Soit A une matrice à coefficients dans un anneau commutatif K quelconque, et soit B une matrice équivalente à A (i.e. de la forme UAV avec U et V inversibles sur l'anneau K). Montrer que, pour tout entier p inférieur au nombre de lignes et au nombre de colonnes de A, l'idéal de K engendré par les mineurs d'ordre p de A est égal à celui qui est engendré par les mineurs d'ordre p de B.

¶ **17.** Soit A une matrice carrée d'ordre n à coefficients dans un anneau principal K. Montrer qu'il existe une matrice $\mathrm{U} \in \mathrm{GL}(n, \mathrm{K})$ telle que UA soit triangulaire (utiliser les *Exercices* 1 et 4 et raisonner par récurrence sur n). Interprétation géométrique?

18. On considère un système d'équations linéaires

$$\begin{cases} a_{11}x_1 + \cdots + a_{1p}x_p = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1}x_1 + \cdots + a_{np}x_p = b_n \end{cases}$$

à coefficients, seconds membres et inconnues dans un anneau principal K. Montrer que, pour que ce système possède au moins une solution, il faut et il suffit d'une part que les deux matrices

$$\mathrm{A} = \begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \cdots\cdots & & \cdots\cdots \\ a_{n1} & \cdots & a_{np} \end{pmatrix}, \qquad \mathrm{B} = \begin{pmatrix} a_{11} & \cdots & a_{1p} & b_1 \\ \cdots\cdots & & \cdots\cdots & \cdots\cdots \\ a_{n1} & \cdots & a_{np} & b_n \end{pmatrix}$$

aient le même rang r, d'autre part qu'un pgcd des mineurs d'ordre r de A soit égal à un pgcd des mineurs d'ordre r de B.

19. Soient K un anneau principal, f une forme p-linéaire sur le module K^n et soit d un pgcd des coefficients de f par rapport à la base canonique; montrer qu'il existe $x_1, \ldots, x_p \in \mathrm{K}^n$ tels que

$$f(x_1, \ldots, x_p) = d.$$

20. Démontrer que tout nombre rationnel peut s'écrire, d'une façon et d'une seule, sous la forme d'une somme finie de fractions de la forme

$$a/p^n$$

avec p premier, $n \geqslant 1$, et $1 \leqslant a \leqslant p - 1$.
Effectuer cette décomposition pour les nombres

$$\frac{1887}{5400}, \qquad \frac{122}{1323}.$$

21. Soit K un anneau d'intégrité commutatif. On dit qu'un $p \in \mathrm{K}$ est **irréductible** s'il n'est pas inversible et s'il n'a pas d'autres diviseurs dans K que ceux qui sont évidents (à savoir les éléments inversibles de K, et les up où $u \in \mathrm{K}$ est inversible).
On dit que K est **factoriel** s'il possède les deux propriétés suivantes :

(UFD 1) : Tout élément non inversible de K est produit d'un nombre fini d'éléments irréductibles.

(UFD 2) : Si $p_1 \ldots p_r = q_1 \ldots q_s$ où les p_i et les q_j sont des éléments irréductibles de K, alors on a $r = s$, et on peut changer l'ordre des q_j de telle sorte que l'on ait

$$\mathrm{K}p_i = \mathrm{K}q_i \quad \text{pour} \quad 1 \leqslant i \leqslant r$$

(ou, ce qui revient au même, $q_i = u_i p_i$ avec u_i inversible).
Ces propriétés expriment que *tout élément de* K *s'écrit, d'une façon essentiellement unique, sous la forme d'un produit d'éléments irréductibles de* K.

a) Montrer que tout anneau principal est factoriel (la réciproque est fausse; cf. § 32, *Exercice* 31).

b) Montrer que, dans la définition d'un anneau factoriel, on peut remplacer la condition (UFD 2) par

(UFD 3) : Si un élément irréductible p de K divise un produit xy, il divise l'un au moins des facteurs de ce produit.

c) Montrer qu'on peut aussi remplacer (UFD 2) par

(UFD 4) Pour tout élément irréductible p de K, l'idéal $\mathrm{K}p$ est premier.

d) Soit K un anneau factoriel. Montrer que, quels que soient $x, y \in \mathrm{K}$ il existe un $d \in \mathrm{K}$ tel que les diviseurs communs à x et y soient exactement les diviseurs de d (on dit que d est un **pgcd de x et y**), et que d est unique modulo la possibilité de le multiplier par un élément inversible de K.

e) Soient K un anneau factoriel, L son corps des fractions, et $\mathfrak{p}$ l'idéal premier de K engendré par un élément irréductible p de K. Montrer que l'anneau local $\mathrm{K}_{\mathfrak{p}}$ [§ 8, *Exercice* 7, (*g*)] est l'anneau d'une valuation discrète (§ 8, *Exercice* 6) de L.

f) Si un anneau d'intégrité commutatif est à la fois factoriel et de Dedekind, il est principal.

g) Soit K un anneau d'intégrité commutatif noethérien. Montrer que tout élément non inversible de K est produit d'éléments irréductibles — autrement dit que K vérifie (UFD 1). [Mais un anneau noethérien n'est pas nécessairement factoriel, i.e. la décomposition en éléments irréductibles peut ne pas être unique : prendre un anneau de Dedekind non principal; ce dernier phénomène se produit notamment pour l'anneau des entiers d'un corps de nombres algébriques, et a longtemps bloqué les progrès dans l'étude de ces anneaux — jusqu'à Dedekind, qui reconnut le premier que la notion importante, dans ce cas, était celle d'*idéal* premier et non d'*élément* irréductible, contrairement à ce qu'indiquait une analogie trompeuse avec les entiers rationnels.]

§ 32

1. Trouver le quotient et le reste de la division de

$$2X^4 - 3X^3 + 4X^2 - 5X + 6 \quad \text{par} \quad X^2 - 3X + 1$$
$$4X^3 + X^2 \quad \text{par} \quad X + 1 + i$$
$$X^4 - 2X^3 + 4X^2 - 6X + 8 \quad \text{par} \quad X - 1.$$

2. Calculer le pgcd des polynômes suivants :

a) $X^6 - 7X^4 + 8X^3 - 7X + 7$ et $3X^5 - 7X^3 + 3X^2 - 7$;

b) $X^5 + X^4 - X^3 - 3X^2 - 3X - 1$ et $X^4 - 2X^3 - X^2 - 2X - 1$;

c) $X^6 + X^5 - X^4 - 2X^3 - X^2 + X + 1$, $X^5 + X^3 - X^2 - 1$ et $X^4 - 2X^3 - X + 2$.

3. Pour chacun des couples de polynômes p, q indiqués ci-dessous, trouver des polynômes u et v tels que $up + vq$ soit un pgcd de p et q :

a) $X^5 + 3X^4 + X^3 + X^2 + 3X + 1$ et $X^4 + 2X^3 + X + 2$;

b) $3X^5 + 5X^4 - 16X^3 - 6X^2 - 5X - 6$ et $3X^4 - 4X^3 - X^2 - X - 6$;

c) $X^5 + 5X^4 + 9X^3 + 7X^2 + 5X + 3$ et $X^4 + 2X^3 + 2X^2 + X + 1$;

d) X^4 et $(1 - X)^4$

4. Trouver un polynôme de degré aussi petit que possible dont le reste de la division par $X^4 - 2X^3 - 2X^2 + 10X - 7$ soit égal à $X^2 + X + 1$, et dont le reste de la division par $X^4 - 2X^3 - 3X^2 + 13X - 10$ soit égal à $2X^2 - 3$.

¶ **5.** Montrer que le pgcd des polynômes

$$X^m - 1 \quad \text{et} \quad X^n - 1$$

est $X^d - 1$, où d est le pgcd des entiers m et n.

6. Soient p et q deux polynômes à une indéterminée. Si le polynôme $p(X^3) + Xq(X^3)$ est divisible par $X^2 + X + 1$, alors $p(1) = q(1) = 0$.

7. Soit

$$f(X) = \frac{p(X)}{q(X)}$$

une fraction rationnelle à une variable à coefficients dans un corps K, et soit a une racine *simple* de son dénominateur q, de sorte que la contribution du pôle a dans la décomposition de f en éléments simples est

$$\frac{A}{X - a}$$

pour un certain $A \in K$. Montrer qu'on a

$$A = \frac{p(a)}{q'(a)}$$

[Écrire

$$\frac{p(X)}{q(X)} = \frac{A}{X - a} + \frac{r(X)}{s(X)}$$

avec $r(a) \neq 0$, $s(a) \neq 0$, réduire au même dénominateur, dériver, et faire $X = a$ dans le résultat obtenu. Le processus de « passage à la limite » qu'on utilise en général dans les cours d'Analyse pour démontrer ce résultat ne s'étend pas à un corps quelconque].

8. Décomposer en éléments simples (sur **C**, puis sur **R**) les fractions rationnelles suivantes :

$$\frac{X^2 + 1}{X(X^2 - 1)}, \quad \frac{2}{(X - 1)(X - 2)(X - 3)}, \quad \frac{X^5 - X^3 - X^2}{X^2 - 1}, \quad \frac{4X^3}{(X^2 + 1)^2},$$
$$\frac{X^6 - X^2 + 1}{(X - 1)^3}, \quad \frac{3X^2 + 3}{X^3 - 3X - 2}, \quad \frac{X^5}{(X^4 - 1)^2}.$$

Le lecteur qui estimerait ces exemples insuffisants pourra facilement en construire autant qu'il en désire : la méthode consiste à choisir au hasard deux polynômes (en s'arrangeant tout de même pour que les racines du dénominateur soient évidentes, ou en tous cas calculables, si l'on désire avoir des résultats explicites).

¶ **9.** Soient L un corps commutatif, K un sous-corps de L, et x un élément de L algébrique sur K. Soit I l'ensemble des polynômes $f \in K[X]$ tels que $f(x) = 0$; montrer que c'est un idéal de K[X]. En déduire qu'il existe un et un seul polynôme

$$(*) \qquad f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

à coefficients dans K qui vérifie $f(x) = 0$ et tel que tout polynôme $g \in K[X]$ vérifiant $g(x) = 0$ soit un multiple de f. Montrer que

$$(**) \qquad x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

est l'équation (à coefficients dans K) de plus petit degré possible vérifiée par x. On dit que $(*)$ est le **polynôme minimal** et $(**)$ l'**équation minimale** de x sur K; son degré n s'appelle le **degré de x sur K**. Montrer que, considéré comme espace vectoriel sur K, le sous-corps K[x] est de dimension n et admet pour base les éléments

$$1, x, \ldots, x^{n-1}.$$

Autrement dit, on a

$$[K[x] : K] = n$$

avec les notations du § 26, *Exercice* 5.

On prend $L = \mathbf{C}$, $K = \mathbf{Q}$ dans ce qui précède. Trouver les équations minimales des éléments suivants de L :

$$\sqrt{2} + \sqrt{3}; \qquad \sqrt[3]{2} + \sqrt{5}$$

¶ **10.** Soit K un corps commutatif.

a) Soient L un sur-corps de K et x un élément de L algébrique sur K. Montrer que le polynôme minimal de x sur K est irréductible (sur K).

b) Soit f un polynôme irréductible à une variable à coefficients dans K, et de coefficient dominant égal à 1. Soit x une racine de f dans une extension de K. Montrer que f est le polynôme minimal de x sur K.

c) Le polynôme f étant comme dans la question précédente, soient x et y deux racines de f dans un sur-corps L de K. Montrer qu'il existe un et un seul isomorphisme j du corps $K(x)$ sur le corps $K(y)$ vérifiant

$$j(x) = y, \qquad j(a) = a \text{ pour tout } a \in K.$$

d) On suppose de plus que K est le corps des fractions d'un anneau A. Avec les notations de la question *c*), montrer que si x est entier sur A (§ 26, *Exercice* 6) il en est de même de y.

¶¶ *e*) Soient A un anneau d'intégrité commutatif, K son corps des fractions et L un sur-corps de K. Soit $x \in L$ entier sur A; montrer que les coefficients du polynôme minimal f de x sur K sont entiers sur A (plonger L dans un corps algébriquement clos, observer que toutes les racines de f sont des entiers sur A et appliquer le § 33, n° 6). En déduire que f est à coefficients dans A si A est intégralement clos (i.e. si tout élément de K entier sur A est dans A).

¶¶ *f*) On suppose dans ce qui précède que L est une extension algébrique de degré fini de K (§ 26, *Exercice* 4). Montrer que, si $x \in L$ est entier sur A, et si A est intégralement clos, on a

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

(utiliser l'*Exercice* 5 du § 26).

¶¶ **11.** Soient L un corps commutatif, K un sous-corps de L, et x un élément de L algébrique sur K. On dit que x est **séparable** sur K s'il est racine *simple* de son polynôme minimal f sur K.

a) Pour que x soit séparable sur K, il faut et il suffit que x soit racine simple d'au moins une équation algébrique à coefficients dans K.

b) On a $f' = 0$ si x n'est pas séparable sur K, et réciproquement.

c) Si K est de caractéristique 0, tout x algébrique sur K est séparable sur K, et toutes les racines de tout polynôme irréductible à coefficients dans K sont simples.

d) Si K est de caractéristique $p \neq 0$, pour tout $x \in L$ algébrique sur K il existe un entier $n \geqslant 0$ tel que

$$x^{p^n}$$

soit séparable sur K.

e) Soit L une extension algébrique de degré fini de K (§ 26, *Exercice* 4). Pour que L soit séparable sur K (§ 26, *Exercice* 4, (*h*)) il faut et il suffit que tout $x \in L$ soit séparable sur K.

¶ **12.** Si un polynôme $f \in \mathbf{Z}[X]$ non constant n'est pas irréductible dans l'anneau $\mathbf{Q}[X]$, alors on peut le décomposer de façon non triviale en produit de polynômes à coefficients *entiers* rationnels (utiliser le lemme de Gauss, § 27, *Exercice* 13).

13. Parmi les polynômes

$$X^3 + X + 1, \qquad X^4 + X + 1, \qquad X^4 + X^3 + 1, \qquad X^3 + 7X + 7, \qquad X^6 + 3X + 2,$$

quels sont ceux qui sont irréductibles sur $\mathbf{Q}$?

¶ **14.** Soit $f(X) = a_0 + a_1X + \cdots + a_nX^n$ un polynôme à coefficients dans $\mathbf{Z}$. On suppose qu'un certain nombre premier p divise $a_0, \ldots, a_{n-1}$, ne divise pas a_n, et de plus que a_0 n'est pas divisible par p^2. Montrer que f est irréductible sur $\mathbf{Q}$ **(critère d'irréductibilité d'Eisenstein**; utiliser l'*Exercice* 12).

¶ **15.** (Diviseurs élémentaires d'une matrice à coefficients polynomiaux). Soient k un corps commutatif et $K = k[X]$ l'anneau des polynômes à une indéterminée à coefficients dans k.

a) Montrer que $GL(n, K)$ est l'ensemble des matrices $U \in M_n(K)$ dont le déterminant est un élément non nul du corps k (le déterminant d'une telle matrice est donc « constant »).

b) On utilise dans ce qui suit, pour les matrices à coefficients dans K, la notion d'opération élémentaire du § 31, *Exercice* 15. Soit A une matrice rectangulaire non nulle à coefficients dans K et soit $a_{ij}(X)$ le coefficient situé à l'intersection de la i^e colonne et de la j^e ligne de A. Montrer qu'on peut, à l'aide d'un nombre fini d'opérations élémentaires, remplacer les coefficients situés sur la i^e colonne ou la j^e ligne de A par les restes de leur division par $a_{ij}(X)$.

c) Soit $d_1(X)$ un polynôme non nul, de coefficient dominant égal à 1, et de plus petit degré possible parmi tous les coefficients non nuls de toutes les matrices déduites de A par une succession d'opérations élémentaires. Montrer qu'on peut déduire de A, par une succession d'opérations élémentaires, une matrice de la forme

$$\begin{pmatrix} d_1 & 0 \\ 0 & A_1 \end{pmatrix}$$

où A_1 a une ligne et une colonne de moins que A, et pour coefficients des polynômes tous divisibles par d_1. Montrer que d_1 est un pgcd des coefficients non nuls de A (et est par suite entièrement déterminé par la connaissance de A).

d) Montrer qu'on peut déduire de A, par une succession d'opérations élémentaires, une matrice de la forme

$$\begin{pmatrix} d_1(X) & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & d_2(X) & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & d_r(X) & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

où les d_i sont des polynômes non nuls tels que chacun divise le suivant. Montrer, à l'aide de l'*Exercice* 16 du § 31, que pour tout entier i inférieur au nombre de lignes et au nombre de colonnes de A, le polynôme $d_1(X) \ldots d_i(X)$ (où l'on pose $d_i = 0$ pour $i \geqslant r + 1$) est un pgcd des mineurs d'ordre i de A. En déduire que l'entier r est égal au rang de A, et que pour $1 \leqslant i \leqslant r$ les polynômes $d_i(X)$ sont entièrement déterminés par A si on impose à leurs coefficients dominants d'être égaux à 1.

e) On appelle $d_1, \ldots, d_r$ les **facteurs invariants** de la matrice A, et **diviseurs élémentaires** de A les quotients $d_i(X)/d_{i+1}(X)$. Enfin, on dit que deux matrices A et B à coefficients dans $K = k[X]$, et ayant toutes deux p lignes et q colonnes, sont **équivalentes** s'il existe des matrices

$$U \in GL(p, K) \qquad \text{et} \qquad V \in GL(q, K)$$

telles que $B = UAV$. Montrer que, pour que A et B soient équivalentes, il faut et il suffit que A et B aient même rang et mêmes facteurs invariants, et qu'on peut alors passer de A à B par une succession d'opérations élémentaires.

¶¶ *f*) Soient M un K-module isomorphe à K^p et M' un sous-module de M. Montrer qu'il existe une base $(a_1, \ldots, a_p)$ de M, et des polynômes $d_1, \ldots, d_p \in K$ tels que d_i divise d_{i+1} et que M'

soit engendré par $d_1a_1, \ldots, d_pa_p$ (on n'interdit pas à certains des d_i d'être nuls). [Appliquer la question *d*) à la matrice, par rapport à une base de M, d'un endomorphisme de M ayant M′ pour image].

¶ *g*) Soit E un K-module de type fini (mais non nécessairement libre). Montrer que E est isomorphe au produit direct d'un module de la forme K^s et de modules de la forme $K/d_1K, \ldots, K/d_rK$ où $d_1, \ldots, d_r$ sont des polynômes non nuls tels que d_i divise d_{i+1} pour $1 \leqslant i \leqslant r-1$. [Choisir un homomorphisme f de K^p *sur* E et appliquer la question précédente à Ker (f)]. Montrer que les entiers r et s, et les polynômes d_i (dont on supposera qu'ils ont 1 pour coefficient dominant), sont entièrement déterminés par E et les conditions qu'on leur a imposées. [On dit que $d_1, \ldots, d_r$ sont les **facteurs invariants** du K-module E; l'entier s est le rang de E au sens du § 29, *Exercice* 11, *e*)]. Montrer que deux K-modules de type fini sont isomorphes si et seulement si leurs rangs et leurs facteurs invariants sont égaux.

¶ *h*) Déduire les résultats précédents du § 31, *Exercices* 8, 9, 10 et 11 et du fait que l'anneau K est principal.
[Les résultats de cet *Exercice*, qui constituent l'analogue pour les anneaux de polynômes à une variable sur un corps de la théorie des diviseurs élémentaires des matrices à coefficients dans **Z** (§ 31, *Exercice* 17), ont des applications importantes, notamment à la théorie des systèmes d'équations différentielles linéaires d'ordre quelconque à coefficients constants; on trouvera d'excellents exposés de ces résultats dans certains des ouvrages cités dans la Bibliographie (notamment dans Albert, Gelfand, Schreier-Sperner); mais la véritable explication de ces résultats est évidemment la théorie des modules de type fini sur un anneau principal.]
Dans les *Exercices* **16** à **21** qui suivent (*), on demande de réduire la matrice donnée à la forme canonique de l'*Exercice* 15, *d*), et d'en calculer les diviseurs élémentaires (le corps de base est **C**).

16. $\begin{pmatrix} X & 1 \\ 0 & X \end{pmatrix}$

17. $\begin{pmatrix} X^2-1 & X+1 \\ X+1 & X^2+2X+1 \end{pmatrix}$

18. $\begin{pmatrix} 1-X & X^2 & X \\ X & X & -X \\ 1+X^2 & X^2 & -X^2 \end{pmatrix}$

19. $\begin{pmatrix} X & 1 & 0 & 0 \\ 0 & X & 1 & 0 \\ 0 & 0 & X & 1 \\ 0 & 0 & 0 & X \end{pmatrix}$

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

21. $\begin{pmatrix} X & 1 & 1 & \ldots & 1 \\ 0 & X & 1 & \ldots & 1 \\ 0 & 0 & X & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & X \end{pmatrix}$ (n lignes et colonnes)

Dans les *Exercices* **22** et **23** qui suivent, on demande de trouver des matrices U et V à coefficients polynomiaux, de déterminant constant non nul, telles que, A désignant la matrice donnée, UAV soit mise sous la forme canonique de l'*Exercice* 15.

22. $\begin{pmatrix} X^4+4X^3+4X^2+X+2, & X^3+4X^2+4X \\ X^4+5X^3+8X^2+5X+2, & X^3+5X^2+8X+4 \end{pmatrix}$

23. $\begin{pmatrix} X^4+3X^3-5X^2+X+1, & 2X^4+3X^3-5X^2+X-1, & 2X^4+2X^3-4X^2 \\ X^4-X^3+1, & 2X^4-X^3-X^2, & 2X^4-2X^3 \\ X^4+2X^3-4X^2+X+1, & 2X^4+2X^3-4X^2+X-1, & 2X^4+X^3-3X^2 \end{pmatrix}$

(*) Les *Exercices* 16 à 26 sont extraits du recueil de Proskurjakov, où le lecteur trouvera de nombreux autres énoncés semblables.

24. Vérifier que les deux matrices suivantes, à coefficients dans $\mathbf{C}[X]$, sont équivalentes :

$$\begin{pmatrix} X^3+6X^2+6X+5, & X^3+4X^2+4X+3 \\ X^3+3X^2+3X+2, & X^3+2X^2+2X+1 \\ 2X^3+3X^2+3X+1, & 2X^3+2X^2+2X \end{pmatrix} = A$$

$$\begin{pmatrix} X^3+X^2+X, & 2X^3+X^2+X-1 \\ 3X^3+2X^2+2X-1, & 6X^3+2X^2+2X-4 \\ X^3-X^2-X-2, & 2X^3-X^2-X-3 \end{pmatrix} = B$$

(on calculera des matrices U, V telles que $B = UAV$).

25. Calculer les facteurs invariants de la matrice

$$\begin{pmatrix} X^3+X^2-X+3, & X^3-X^2+X, & 2X^3+X^2-X+4, & X^3+X^2-X+2 \\ X^3+3X^2-3X+6, & X^3-3X^2+3X-2, & 2X^3+3X^2-3X+7, & X^3+3X^2-3X+4 \\ X^3+2X^2-2X+4, & X^3-2X^2+2X-1, & 2X^3+2X^2-2X+5, & X^3+2X^2-2X+3 \\ 2X^3+X^2-X+5, & 2X^3-X^2+X+1, & 4X^3+X^2-X+7, & 2X^3+X^2-X+3 \end{pmatrix}$$

26. Calculer les diviseurs élémentaires de la matrice

$$\begin{pmatrix} X^4+1, & X^7-X^4+X^3-1, & X^4-4X^3+4X-5 \\ 2X^4+3, & 2X^7-2X^4+4X^3-2, & 3X^4-10X^3+X^2+10X-14 \\ X^4+2, & X^7-X^4+2X^3-2, & 2X^4-6X^3+X^2+6X-9 \end{pmatrix}$$

en prenant pour anneau de base soit $\mathbf{Q}[X]$, soit $\mathbf{R}[X]$, soit $\mathbf{C}[X]$.

¶ **27.** On se propose de démontrer que *si* K *est un anneau commutatif noethérien, l'anneau de polynômes* K[X] *est noethérien.* On désigne par I un idéal de K[X].

a) Pour tout entier $n \geqslant 0$, soit $J_n \subset K$ l'ensemble formé de 0 et des $a \in K$ vérifiant la condition suivante : il existe un polynôme $f \in I$, de degré n, dont le coefficient dominant est égal à a. Montrer que les J_n forment une suite croissante d'idéaux de K. En conclure qu'on a

$$J_r = J_{r+1} = \cdots$$

pour un certain entier r.

b) Pour tout entier i tel que $0 \leqslant i \leqslant r$, on choisit dans I des polynômes f_{ij} $(1 \leqslant j \leqslant n_i)$ en nombre fini, de degré i, dont les coefficients dominants a_{ij} engendrent l'idéal J_i. Montrer que, pour tout $f \in I$, il existe des polynômes $q_{ij} \in K[X]$ tels que l'on ait

$$f = \sum_{\substack{1 \leqslant j \leqslant n_i \\ 0 \leqslant i \leqslant r}} q_{ij} f_{ij} + g \qquad \text{avec} \qquad d^o(g) < d^o(f).$$

c) En déduire, par récurrence sur le degré de f, que les $n_0 + \cdots + n_r$ polynômes f_{ij} engendrent l'idéal I.

d) Déduire du résultat précédent que si un anneau commutatif L contient un sous-anneau noethérien K et des éléments $x_1, \ldots, x_n$ en nombre fini tels que $L = K[x_1, \ldots, x_n]$, alors L est noethérien. (Observer que L est un quotient d'un anneau de polynômes à coefficients dans K).

¶ **28.** Soit K un corps commutatif infini. On rappelle qu'une partie V de K^n est appelée une *variété algébrique* s'il existe un nombre *fini* de polynômes $p_1, \ldots, p_r \in K[X_1, \ldots, X_n]$ tels que V soit l'ensemble des $x \in K^n$ où l'on a $p_1(x) = \cdots = p_r(x) = 0$; et qu'une partie A de K^n est appelée un *ouvert de Zariski* si l'ensemble complémentaire $K^n - A$ est une variété algébrique

(§§ 27, 28, *Exercice* 1). En utilisant le fait que l'anneau $K[X_1, \ldots, X_n]$ est noethérien, démontrer les propriétés suivantes :

a) L'intersection d'une famille (finie ou infinie) de variétés algébriques dans K^n est une variété algébrique dans K^n. Toute réunion (finie ou non) d'ouverts de Zariski est un ouvert de Zariski.

b) Toute suite décroissante de variétés algébriques dans K^n est stationnaire. Toute suite croissante d'ouverts de Zariski est stationnaire.
Montrer en outre qu'on a

c) La réunion d'une famille *finie* de variétés algébriques dans K^n est encore une variété algébrique dans K^n. L'intersection d'une famille *finie* d'ouverts de Zariski est encore un ouvert de Zariski.

d) L'intersection de deux ouverts de Zariski non vides est non vide. Si U et V sont deux variétés algébriques dans K^n, telles que $U \neq K^n$ et $V \neq K^n$, alors on a $U \cup V \neq K^n$.
(On aura intérêt, pour chaque variété algébrique V dans K^n, à introduire l'idéal $I(V) \subset K[X_1, \ldots, X_n]$ formé des polynômes qui sont nuls en tout $x \in V$, et à interpréter en termes d'idéaux les opérations qu'on demande d'effectuer sur les variétés algébriques).

¶¶ **29.** Soit K un anneau commutatif noethérien. Montrer que l'anneau de séries formelle $K[[X]]$ (§§ 27, 28, *Exercice* 11) est noethérien. (Étant donné un idéal I de $K[[X]]$, considérer pour tout $n \geqslant 0$ l'idéal J_n de K formé des coefficients du terme en X^n dans les $f \in I$ qui ne comportent aucun terme de degré $\leqslant n-1$).

¶¶¶ **30.** Soient V un espace vectoriel de dimension finie sur un corps commutatif K de caractéristique 0, et G un groupe fini, d'ordre r, d'automorphismes de V. On désigne par A l'anneau des fonctions polynomiales sur V (§§ 27, 28, *Exercice* 17; ou bien § 28, n° 2 dans le cas où $V = K^n$, auquel on peut évidemment se ramener).
Étant donnés un $s \in G$ et une fonction polynomiale f sur V, on définit une nouvelle application f_s de V dans K par

$$f_s(x) = f(s^{-1}(x)) \quad \text{pour tout } x \in V.$$

On dit que f est un **invariant** du groupe G si $f_s = f$ pour tout $s \in G$. On note $I \subset A$ l'ensemble de ces invariants, qui est un sous-anneau de A.

a) Montrer qu'on a $f_s \in A$ pour toute $f \in A$ et tout $s \in G$, et que I est un sous-anneau de A.

b) Pour toute fonction polynomiale $f \in A$, on définit la fonction polynomiale

$$f^\natural = \frac{1}{r} \sum_{s \in G} f_s;$$

montrer que $f^\natural$ est un invariant de G. Montrer qu'on a les relations

$$(f+g)^\natural = f^\natural + g^\natural \quad \text{quels que soient } f, g \in A$$
$$f^\natural = f \quad \text{si et seulement si } f \in I$$
$$(fg)^\natural = f^\natural g \quad \text{quels que soient } f \in A \text{ et } g \in I.$$

c) Montrer que si f est un invariant de G, il en est de même de toutes les composantes homogènes de f (*Exercice* 17, §§ 27, 28).

d) Soit J l'idéal de l'anneau A engendré par I. En tenant compte de la question *c*) et du fait que A est noethérien (*Exercices* 14 et 15), montrer qu'il existe dans I des polynômes homogènes

$$f_1, \ldots, f_p$$

le nombre fini qui engendrent J. On pose dans ce qui suit $q_i = d^0(f_i)$.

e) Pour tout $f \in I$ homogène de degré q, montrer qu'il existe des $u_i \in A$ homogènes de degrés $q - q_i$ (on prendra $u_i = 0$ si $q - q_i < 0$) tels que $f = \sum f_i u_i$. Montrer qu'on peut même prendre les u_i dans I (Ecrire que $f = f^\natural$).

f) En raisonnant par récurrence sur le degré de f, déduire de là que *tout* $f \in I$ *est un polynôme en les* f_i, *à coefficients dans* K, autrement dit que les invariants du groupe G forment un anneau engendré sur K par un nombre *fini* d'éléments (*théorème des invariants* de Hilbert).

¶¶ **31.** (La résolution de cet *Exercice* suppose acquis les résultats de l'*Exercice* 21 du § 31). On se propose de démontrer que *si* A *est un anneau factoriel, l'anneau* A[X] *est factoriel.*

a) Étant donnés des polynômes $f, g \in A[X]$, soit p un élément irréductible de A qui divise tous les coefficients de fg; montrer que p divise tous les coefficients de f, ou bien tous ceux de g. (Raisonner comme dans l'*Exercice* 13 du § 27).

b) On dit qu'un polynôme $f \in A[X]$ est **primitif** si le pgcd de ses coefficients est 1. Montrer que si f et g sont primitifs, il en est de même de fg.

c) Pour tout $f \in A[X]$ non nul, on note $c(f)$ un pgcd de ses coefficients. Montrer que

$$c(fg) = c(f)c(g)$$

(lemme de Gauss pour les anneaux factoriels).

d) Soit K le corps des fractions de A. Montrer que si un $f \in A[X]$ n'est pas irréductible dans $K[X]$, il n'est pas non plus irréductible dans $A[X]$.

e) Déduire de là et de la question *a*) que les éléments irréductibles de l'anneau A[X] sont les éléments irréductibles de l'anneau factoriel A, et les polynômes non constants qui sont primitifs, et irréductibles dans l'anneau $K[X]$.

f) Déduire de là et des résultats du § 32, n° 3 (qu'on appliquera à $K[X]$) que tout élément de A[X] s'écrit, d'une façon essentiellement unique, sous la forme d'un produit d'éléments irréductibles de A[X], et par suite que A[X] est factoriel comme annoncé.

g) Montrer que, si A est un anneau factoriel (par exemple si A est un corps, ou bien si $A = \mathbf{Z}$), l'anneau $A[X_1, \ldots, X_n]$ est factoriel.
En particulier, *tout polynôme* (à n variables) *à coefficients dans un corps* K *se décompose, d'une façon essentiellement unique, en un produit de polynômes irréductibles* à coefficients dans K (un polynôme f à coefficients dans K étant dit **irréductible** s'il est non constant, et si chacun de ses diviseurs est constant, ou est proportionnel à f).

h) Montrer que l'anneau $\mathbf{Z}[X]$ (qui est factoriel d'après ce qui précède) *n'est pas* principal (examiner l'idéal engendré par 2 et X). Même question pour $K[X, Y]$ où K est un corps.

i) Montrer que, pour tout corps commutatif K, le polynôme $Y^2 - X^3$ est irréductible dans l'anneau $K[X, Y]$. (On écrira $K[X, Y] = A[Y]$ où $A = K[X]$ et on appliquera la question *d*) ci-dessus).

j) Montrer que toute fraction rationnelle f à n variables, à coefficients dans un corps K, peut se mettre sous la forme $f = p/q$ où p et q sont des polynômes à n variables, à coefficients dans K, et premiers entre eux (i.e. n'ayant aucun diviseur commun en dehors des constantes); et que, de plus, p et q sont uniques à des facteurs constants près. Montrer que les points d'indétermination de f sont les éléments de K^n où p et q s'annulent simultanément, et que les pôles de f sont les $x \in K^n$ où l'on a $p(x) \neq 0$ et $q(x) = 0$.

k) Soient p et q deux polynômes non constants à $n \geqslant 2$ indéterminées et à coefficients dans un corps commutatif K. On suppose p et q premiers entre eux; s'ensuit-il qu'il existe des polynômes u et v à n indéterminées, à coefficients dans K, tels que

$$up + vq = 1\,?$$

[L'interprétation géométrique du fait que l'anneau $\mathbf{C}[X_1, \ldots, X_n]$, par exemple, est factoriel est la suivante. Soit $f \in \mathbf{C}[X_1, \ldots, X_n]$ non constant et soit V l'hypersurface de $\mathbf{C}^n$ définie

par l'équation $f(x) = 0$. Soit

$$f(X) = \prod_{i=1}^{i=s} p_i(X)^{r_i}$$

la décomposition de f en produit de facteurs irréductibles, et soit V_i l'hypersurface $p_i(x) = 0$. Alors V_i est irréductible (i.e. ne peut pas se représenter de façon non triviale comme réunion de deux autres variétés algébriques), on a

$$V = V_1 \cup \ldots \cup V_s,$$

et cette décomposition de V en hypersurfaces irréductibles est unique à l'ordre près.
On peut encore se placer au point de vue suivant. Soit V une variété algébrique dans $\mathbf{C}^n$ et soit $\mathfrak{a}$ l'idéal de $\mathbf{C}[X_1, \ldots, X_n]$ formé des polynômes f tels que $f(x) = 0$ pour tout $x \in V$. Comme $\mathbf{C}[X_1, \ldots, X_n]$ est noethérien, l'*Exercice* 9, *b*), du § 18 montre que $\mathfrak{a}$ est intersection finie d'idéaux primaires de $\mathbf{C}[X_1, \ldots, X_n]$ (et même d'idéaux *premiers* : appliquer l'*Exercice* 11 du § 18 en remarquant que l'idéal $\mathfrak{a}$ est identique à son radical, attendu que la relation

$$f(x)^q = 0 \text{ sur } V \quad \text{implique} \quad f(x) = 0 \text{ sur } V$$

pour des raisons triviales) ; écrivons donc

$$\mathfrak{a} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_s$$

où les $\mathfrak{p}_i$ sont les idéaux premiers minimaux de $\mathfrak{a}$, et soit V_i la variété algébrique de $\mathbf{C}^n$ formée des x tels que

$$f(x) = 0 \quad \text{pour tout } f \in \mathfrak{p}_i$$

(V_i est définie par un nombre fini d'équations si l'on veut : prendre des générateurs de $\mathfrak{p}_i$). Comme $\mathfrak{p}_i$ est premier, chaque V_i est irréductible, et l'on a

$$V = V_1 \cup \ldots \cup V_s;$$

on dit que les V_i sont les **composantes irréductibles** de V. Ceci dit, le fait que l'anneau $\mathbf{C}[X_1, \ldots, X_n]$ soit factoriel montre que si V est une hypersurface (i.e. peut être définie par une seule équation) il en est de même de ses composantes irréductibles ; ou encore : si une variété *irréductible* W est contenue dans une hypersurface V, il existe une *hypersurface* irréductible W′ telle que $W \subset W' \subset V$, résultat « évident » géométriquement...
Comme autre exemple important d'anneau factoriel, citons (Weierstrass) l'anneau des séries entières *convergentes* (i.e. à domaine de convergence non réduit à 0) à n variables complexes ; cet anneau intervient dans l'étude « locale » des « variétés analytiques » dans $\mathbf{C}^n$ (parties de $\mathbf{C}^n$ définies par des équations dont les premiers membres sont des fonctions holomorphes). Cet anneau est aussi noethérien].

¶¶ **32.** Étendre le critère d'irréductibilité d'Eisenstein (*Exercice* 11) aux anneaux factoriels.

¶ **1.** Soit G_n l'ensemble des nombres complexes z tels que $z^n = 1$.

a) Montrer que G_n est un sous-groupe d'ordre n du groupe multiplicatif $\mathbf{C}^*$ des nombres complexes non nuls.

b) Soit

$$z = \cos(2k\pi/n) + i.\sin(2k\pi/n)$$

un élément de G_n ; pour que z soit un générateur du groupe G_n (i.e. pour que toute racine n^e de l'unité soit une puissance de z) il faut et il suffit que k soit premier à n (on dit alors que z est une **racine primitive** n^e de l'unité).

c) Sans supposer k et n premiers entre eux, montrer que l'**ordre** de z dans le groupe G_n (i.e. le plus petit entier $d \geqslant 1$ tel que $z^d = 1$) est $n/\text{pgcd}(k, n)$, et qu'alors z est racine primitive d^e de l'unité.

d) Soit $\varphi(n)$ le nombre des racines primitives n^e de l'unité. Montrer que $\varphi(n)$ est le nombre d'entiers k tels que $1 \leqslant k \leqslant n$ qui sont premiers à n, et que c'est aussi le nombre des éléments inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$. Montrer que

$$n = \sum_{d|n} \varphi(d),$$

la somme étant étendue à tous les diviseurs d et n (la notation $d|n$ signifie que d divise n). Montrer que

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_r}\right)$$

où $p_1, \ldots, p_r$ sont les divers diviseurs premiers de n.

e) Classer d'après leur ordre les racines n^e de l'unité pour $n = 2, 3, 4, 6, 8, 12, 16, 20, 24$. Calculer les parties réelles et imaginaires de toutes les racines 24^e de l'unité.

¶ **2.** Soient K un corps commutatif et n un entier tel que l'équation $x^n = 1$ possède n racines dans K. Montrer que le sous-groupe d'ordre n du groupe multiplicatif K^* formé par les racines de cette équation est *cyclique* (utiliser l'*Exercice* 20 du § 7).
En déduire que si K est un corps fini à q éléments le groupe multiplicatif K^* est cyclique (considérer l'équation

$$x^{q-1} = 1$$

dans K).
En particulier, pour tout nombre premier p, le groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique.

¶ **3.** Soit K un corps commutatif fini à q éléments. Soient $a_1, \ldots, a_{q-1}$ les éléments non nuls de K. Montrer que si X désigne une indéterminée sur K on a

$$(X - a_1) \ldots (X - a_{q-1}) = X^{q-1} - 1$$

(utiliser le Théorème 1 du § 33). En déduire que

$$a_1 \ldots a_{q-1} = -1$$

(on utilisera, pour déterminer le signe, le fait que q est une puissance de la caractéristique p de K : § 30, *Exercice* 8).
En prenant $K = \mathbf{Z}/p\mathbf{Z}$, déduire de là le théorème de Wilson, à savoir que

$$(p-1)! \equiv -1 \pmod{p}$$

pour tout nombre premier p.

¶ **4.** Soient p un nombre premier et r un entier ; on dit qu'un entier n premier à p est une **puissance r^e modulo p** (si $r = 2$, on dit un **reste quadratique** modulo p) s'il existe des entiers x tels que l'on ait

$$x^r \equiv n \pmod{p}.$$

En utilisant le fait que le groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique (*Exercice* 2) montrer que tout x premier à p est une puissance r^e modulo p si r est premier à $p - 1$. Si r divise $p - 1$ (exemple : $r = 2$ et p impair, cas le plus important), pour qu'un entier n premier à p soit puissance r^e modulo p il faut et il suffit que

$$n^{\frac{p-1}{r}} \equiv 1 \pmod{p}.$$

Les classes modulo p des puissances r^e mod p sont alors en nombre égal à $\frac{p-1}{r}$ (par exemple si p est impair il y a $\frac{p-1}{2}$ restes quadratiques modulo p).
On prend $p = 31$. Pour chaque diviseur r de $p - 1 = 30$, trouver les puissances r^e modulo p.

¶ **5.** (Cet Exercice repose sur l'*Exercice* 1). Pour tout entier $n \geqslant 1$, on appelle **polynôme cyclotomique** d'indice n le polynôme

$$\Phi_n(X) = (X - \xi_1) \ldots (X - \xi_h)$$

dont les racines sont les $h = \varphi(n)$ racines *primitives* n^e de l'unité dans le corps $\mathbf{C}$; ce polynôme est, en apparence, à coefficients dans $\mathbf{C}$, mais on va montrer qu'en fait il est à coefficients *entiers rationnels*. On convient de poser $\Phi_1(X) = X - 1$.
a) Montrer que

$$\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$$

si p est premier.
b) Vérifier que

$$\Phi_{12}(X) = X^4 - X^2 + 1.$$

c) Montrer que, pour tout entier $n \geqslant 1$, on a

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

où le produit figurant au second membre est étendu à tous les diviseurs d de n (y compris 1 et n). (Utiliser la décomposition du polynôme $X^n - 1$ en produit de facteurs du premier degré).
d) En utilisant la relation

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)}$$

et en raisonnant par récurrence sur n, montrer que Φ_n est à coefficients entiers rationnels.
(Ces résultats s'étendent à tout corps algébriquement clos K, pourvu qu'on se limite aux entiers n qui ne sont pas divisibles par la caractéristique p de K, restriction qui n'en est d'ailleurs pas une en vertu du § 30, *Exercice* 14).

¶¶ **6.** Montrer qu'il existe, sur l'ensemble des entiers $n \geqslant 1$, une et une seule fonction μ (**fonction de Möbius**) à valeurs entières, vérifiant la relation

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$$

(la somme est étendue aux diviseurs d de n tels que $1 \leqslant d \leqslant n$).
Montrer qu'on a

$$\mu(1) = 1$$
$$\mu(p) = -1 \quad \text{si } p \text{ est premier}$$
$$\mu(p^r) = 0 \quad \text{si } p \text{ est premier et si } r \geqslant 2.$$

Montrer qu'on a

$$(*) \qquad \mu(mn) = \mu(m)\,\mu(n) \quad \text{si } m \text{ et } n \text{ sont premiers entre eux}$$

(on observera que tout diviseur de mn, lorsque m et n sont premiers entre eux, s'écrit d'une façon et d'une seule comme produit d'un diviseur de m et d'un diviseur de n ; on raisonnera alors par récurrence en supposant (*) déjà établi pour les couples m', n' tels que $m'n' < mn$).
Déduire des résultats précédents que l'on a

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n \text{ est produit de } r \text{ facteurs premiers distincts} \\ 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier.} \end{cases}$$

Calculer $\mu(n)$ pour $1 \leqslant n \leqslant 100$.

¶¶ **7.** Soit f une fonction sur l'ensemble des entiers $n \geqslant 1$, et à valeurs dans un groupe additif A. On définit une nouvelle fonction g en posant

$$g(n) = \sum_{d|n} f(d)$$

où la somme est étendue aux diviseurs d de n tels que $1 \leqslant d \leqslant n$. Montrer qu'on a inversement

$$f(n) = \sum_{d|n} g(d)\,\mu\left(\frac{n}{d}\right)$$

où μ est la fonction de Möbius de l'*Exercice* précédent. (On utilisera exclusivement la propriété ayant servi à définir μ).

Comment modifier les formules précédentes si A est un groupe commutatif écrit multiplicativement ?

¶¶ **8.** (Cet Exercice repose sur les *Exercices* 5, 6 et 7). Montrer que les polynômes cyclotomiques sont donnés par la relation

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu\left(\frac{n}{d}\right)}.$$

Calculer les polynômes Φ_n pour $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 15$, et montrer que

$$\begin{aligned}\Phi_{105}(X) = {} & X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} - X^{40} - X^{39} + X^{36} + X^{35} + X^{34} + X^{33} \\ & + X^{32} + X^{31} - X^{28} - X^{26} - X^{24} - X^{22} - X^{20} + X^{17} + X^{16} + X^{15} + X^{14} + X^{13} \\ & + X^{12} - X^9 - X^8 - 2X^7 - X^6 - X^5 + X^2 + X + 1,\end{aligned}$$

en supposant que Faddeev et Sominskii aient raison, ce que l'auteur n'a pas vérifié...

9. Décomposer en éléments simples complexes la fraction rationnelle

$$\frac{f(X)}{X^n - 1}$$

où f est un polynôme quelconque à coefficients complexes.

¶ **10.** Soient $z_1, \ldots, z_n$ les racines n^e de l'unité dans $\mathbf{C}$. Montrer qu'on a

$$z_1^h + \ldots + z_n^h = \begin{cases} n & \text{si } h \equiv 0 \pmod{n} \\ 0 & \text{si } h \not\equiv 0 \pmod{n} \end{cases}$$

(multiplier le premier membre par z_1^h).

11. On désigne par $z_1, \ldots, z_n$ les racines n^e de l'unité dans $\mathbf{C}$. Démontrer les relations suivantes :

$$\prod_{k=1}^{k=n} (a + bz_k) = a^n + (-1)^{n-1} b^n$$

$$\prod_{k=1}^{k=n} (z_k^2 - 2z_k \cos\theta + 1) = 2(1 - \cos n\theta)$$

$$\prod_{k=1}^{k=n} \frac{(1 + z_k)^n - 1}{t} = \prod_{k=1}^{k=n-1} [t^n - (z_k - 1)^n].$$

12. Soient u, v, w les trois racines (distinctes ou non) d'une équation

$$ax^3 + bx^2 + cx + d = 0$$

de degré 3 à coefficients complexes. En utilisant les résultats du § 33, n° 6, *Exemple* 4, calculer à l'aide de a, b, c, d les expressions

$$u^3 + v^3 + w^3, \qquad u^3 + v^3 + w^3,$$

¶ **13.** Soient $X_1, \ldots, X_n$ des indéterminées sur un anneau commutatif K. On appelle **fonctions symétriques élémentaires** de $X_1, \ldots, X_n$ les polynômes

$$\begin{aligned} s_1 &= X_1 + X_2 + \cdots + X_n = \Sigma X_i \\ s_2 &= X_1X_2 + \cdots + X_{n-1}X_n = \sum_{1 \leqslant i < j \leqslant n} X_iX_j \\ s_3 &= X_1X_2X_3 + \cdots = \sum_{1 \leqslant i < j < k \leqslant n} X_iX_jX_k \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ s_n &= X_1X_2 \ldots X_n \end{aligned}$$

(ces expressions interviennent, cf. n° 6 du § 33, dans le calcul des coefficients d'une équation algébrique en fonction de ses racines). D'autre part, on dit qu'un polynôme $f \in K[X_1, \ldots, X_n]$ est **symétrique** si l'on a

$$f(X_{s(1)}, \ldots, X_{s(n)}) = f(X_1, \ldots, X_n)$$

pour toute permutation s des entiers $1, \ldots, n$.

a) Démontrer que *tout polynôme symétrique* $f(X_1, \ldots, X_n)$ *est un polynôme en* $s_1, \ldots, s_n$ *à coefficients dans* K. [On pourra procéder par récurrence sur l'entier $n + d^\circ(f)$. Observer d'abord que $f(X_1, \ldots, X_{n-1}, 0)$ est symétrique en $X_1, \ldots, X_{n-1}$, donc est un polynôme en les fonctions symétriques élémentaires de $X_1, \ldots, X_{n-1}$, lesquelles s'obtiennent en remplaçant X_n par 0 dans les fonctions symétriques élémentaires de $X_1, \ldots, X_n$. En déduire qu'il existe un polynôme $p(s_1, \ldots, s_{n-1})$, de degré au plus égal au degré de f, tel que le polynôme

$$g(X_1, \ldots, X_n) = f(X_1, \ldots, X_n) - p(s_1, \ldots, s_{n-1})$$

s'annule pour $X_n = 0$; en déduire, compte-tenu de la symétrie de g, que

$$g(X_1, \ldots, X_n) = X_1 \ldots X_n h(X_1, \ldots, X_n)$$

avec h symétrique et $d^\circ(h) < d^\circ(f)$].

b) Démontrer que si un polynôme $p \in K[X_1, \ldots, X_n]$ vérifie $p(s_1, \ldots, s_n) = 0$, alors $p = 0$ (raisonner par récurence sur n; prendre p de plus petit degré possible par rapport à s_n et faire $X_n = 0$ dans le résultat).

c) En conclure que *l'expression d'un polynôme symétrique* f *à l'aide de* $s_1, \ldots, s_n$ *est unique.*

d) On suppose f homogène de degré total k en $X_1, \ldots, X_n$, et on pose

$$f(X_1, \ldots, X_n) = p(s_1, \ldots, s_n);$$

montrer que les seuls monômes

$$s_1^{r_1} \ldots s_n^{r_n}$$

figurant effectivement dans p sont ceux pour lesquels on a

$$r_1 + 2r_2 + \cdots + nr_n = k.$$

e) Calculer à l'aide des fonctions symétriques élémentaires les polynômes suivants :

$$\begin{array}{l} X_1^2X_2 + X_1X_3^2 + X_1^2X_3 + X_1X_2^2 + X_2^2X_3 + X_2X_3^2 \quad (n = 3) \\ (2X_1 - X_2 - X_3)(2X_2 - X_1 - X_3)(2X_3 - X_1 - X_2) \quad (n = 3) \\ (X_1X_2 + X_3X_4)(X_1X_3 + X_2X_4)(X_1X_4 + X_2X_3) \quad (n = 4) \end{array}$$

$$\sum_{i \neq j} X_i^2X_j; \quad \sum_{i \neq j \neq k} X_i^2X_j^2X_k; \quad \sum_{i \neq j \neq k} X_i^2X_jX_k; \quad \sum_{s \in \mathfrak{S}_n} (a_1X_{s(1)} + a_2X_{s(2)} + \cdots + a_nX_{s(n)})^2;$$

$$\sum_{\substack{j \neq k \\ j \neq i,\ j \neq k}} (X_i + X_k - X_j)^2 \quad (n \text{ quelconque}).$$

¶ **14.** Les notations étant celles de l'*Exercice* précédent, on considère les **sommes de Newton**

$$\sigma_k(X_1, \ldots, X_n) = X_1^k + X_2^k + \cdots + X_n^k \quad (k = 0, 1, \ldots)$$

Montrer qu'on peut les exprimer en fonction de $s_1, \ldots, s_n$ à l'aide des formules suivantes :

$$\sigma_k - s_1\sigma_{k-1} + s_2\sigma_{k-2} - \cdots + (-1)^{k-1}s_{k-1}\sigma_1 + (-1)^k s_k\sigma_0 = 0 \quad \text{pour } k < n$$
$$\sigma_k - s_1\sigma_{k-1} + \cdots + (-1)^n s_n\sigma_{k-n} = 0 \quad \text{pour } k \geqslant n.$$

Calculer complètement, à l'aide des fonctions symétriques élémentaires, les sommes de Newton σ_k pour $0 \leqslant k \leqslant 6$.

¶ **15.** Soit

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

une équation algébrique à coefficients dans un corps commutatif K. Soient $x_1, \ldots, x_n$ ses racines dans une extension algébriquement close de K (on pourra prendre **C** en supposant que K est un sous-corps de **C**, mais bien entendu cette hypothèse ne simplifie rien !). Soit f un polynôme symétrique à n indéterminées, à coefficients dans K. Montrer qu'il existe un polynôme p à n indéterminées, à coefficients dans K, tel que l'on ait

$$f(x_1, \ldots, x_n) = p(a_{n-1}, \ldots, a_0)$$

et que p ne dépend que de f (utiliser l'*Exercice* 13). Applications :

a) Calculer la somme des puissances 5e des racines de l'équation

$$x^6 - 4x^5 + 3x^3 - 4x^2 + x + 1 = 0.$$

b) Calculer la somme

$$\sum x_i^2 x_j^2 x_k x_h$$

où $x_1, \ldots, x_5$ désignent les racines de l'équation

$$x^5 - 4x^3 + x^2 + 3x + 1 = 0.$$

c) On désigne par x_1, x_2, x_3 les racines de l'équation

$$x^3 + ax^2 + bx + c = 0;$$

former les équations dont les racines sont les quantités suivantes :

i) $x_1 + x_2, x_3 + x_3, x_3 + x_1$;

ii) $x_1^2 - x_2x_3, x_2^2 - x_3x_1, x_3^2 - x_1x_2$

iii) $(x_1 + jx_2 + j^2x_3)^3$, $(x_1 + j^2x_2 + jx_3)^3$ où $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

¶ **16.** Soit

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

une équation algébrique à coefficients dans un corps commutatif K. On désigne par $x_1, \ldots, x_n$ ses racines (distinctes ou non) dans une extension algébriquement close de K. On appelle **discriminant** de l'équation donnée l'expression

$$D = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)^2.$$

a) Montrer qu'il existe un polynôme p à n indéterminées, à coefficients dans K, et indépendant de l'équation (*), tel que l'on ait

$$D = p(a_{n-1}, \ldots, a_0).$$

b) Calculer le discrimimant d'une équation de degré 2, 3 ou 4.

c) Pour que l'équation (*) possède au moins une racine double, il faut et il suffit que son discriminant soit nul.

d) Déterminer les valeurs de λ pour lesquelles les équations suivantes possèdent au moins une racine double :

$$x^3 - 3x + \lambda = 0; \qquad x^3 - 8x^2 + (13 - \lambda)x - 6 - 2\lambda = 0;$$
$$x^4 - 4x^3 + (2 - \lambda)x^2 + 2x - 2 = 0.$$

¶¶ *e*) Montrer que le discriminant de l'équation

$$x^n + px + q = 0$$

est égal à

$$(-1)^{\frac{n(n-1)}{2}} n^n q^{n-1} + (-1)^{\frac{(n-1)(n-2)}{2}} (n-1)^{n-1} p^n.$$

f) On désigne par f le polynôme figurant au premier membre de l'équation (*). Montrer que le discriminant D de l'équation (*) est encore donné par la formule

$$(-1)^{\frac{n(n-1)}{2}} D = \prod_{1 \leqslant i \leqslant n} f'(x_i).$$

g) Montrer que le discriminant de l'équation

$$\frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + 1 = 0$$

est égal à

$$(-1)^{\frac{n(n-1)}{2}}.$$

¶¶ *h*) On considère (*Exercice* 5) l'équation cyclotomique

$$\Phi_n(x) = 0.$$

Montrer que son discriminant est égal à

$$(-1)^{\frac{\varphi(n)}{2}} \frac{n^{p(n)}}{\prod_{p \mid n} p^{\frac{\varphi(n)}{p-1}}}$$

(utiliser la question (*f*) et l'*Exercice* 8).

¶ **20.** Soient K un corps commutatif et f un polynôme à une indéterminée, à coefficients dans K. On se propose de prouver qu'il existe un corps L, extension de K (i.e. dont K est un sous-corps), dans lequel f admet au moins une racine (ce résultat est le premier pas dans la démonstration du théorème de Steinitz).

a) Montrer qu'on peut se ramener au cas où f est irréductible sur K.

b) Dans l'anneau de polynôme $A = K[X]$, on considère l'idéal $I = (f)$ engendré par f et on forme l'anneau quotient $L = A/I$ (§ 8, *Exercice* 7). Montrer que c'est un corps.

e) Soit j l'application de K dans L qui, à chaque $c \in K$, associe la classe mod I du polynôme constant c. Montrer que c'est un isomorphisme de K sur un sous-corps de L (dans ce qui suit, on convient d'identifier chaque $c \in K$ à son image $j(c)$ dans L).

d) Soit $z \in L$ l'image du polynôme X par l'application canonique de K[X] sur L. Montrer que z est racine de f, et que $L = K[z]$. (Ce qui démontre le résultat annoncé).

e) On prend $f(X) = X^2 - d$ où $d \in K$ n'est pas un carré dans K. Montrer que les constructions précédentes se réduisent alors à celles du § 9. On vérifiera en particulier que le corps $\mathbf{C}$ est le quotient de l'anneau $\mathbf{R}[X]$ par l'idéal engendré par le polynôme $X^2 + 1$ (cette méthode de construction de $\mathbf{C}$ est due à Cauchy).

f) On prend $f(X) = X^3 + pX + q$, supposé irréductible sur K. Donner du corps L correspondant une description analogue à celle qu'on a donnée au § 9 pour les anneaux $K[\sqrt{d}]$.

g) Que se passe-t-il, dans les constructions précédentes, si le polynôme f n'est pas irréductible?

¶¶ **21.** Soient $f_1, \ldots, f_n$ des polynômes non constants à une indéterminée à coefficients dans un corps commutatif K. Montrer qu'il existe dans l'anneau $K[X_1, \ldots, X_n]$ un idéal maximal qui contient $f_1(X_1), \ldots, f_n(X_n)$ (utiliser l'*Exercice* 15 du § 27). En raisonnant comme dans l'*Exercice* précédent, en déduire l'existence d'une extension algébrique L de K dans laquelle chaque f_i possède au moins une racine.
(La démonstration complète du théorème de Steinitz est une extension directe du raisonnement de cet *Exercice*; on introduit un anneau de polynômes à une infinité de variables, comportant autant (sic) de variables qu'il y a de polynômes irréductibles à coefficients dans K et de coefficient dominant égal à 1, puis on prend le quotient de cet anneau par un idéal maximal bien choisi)

¶¶ **22.** Les notations restant celles de l'*Exercice* précédent, montrer que tout idéal premier de l'anneau $K[X_1, \ldots, X_n]$ contenant $f_1(X_1), \ldots, f_n(X_n)$ est maximal (cf. § 26, *Exercice* 3).

¶ **23.** Soit K un corps commutatif. On dit qu'une extension L de K (i.e. un corps commutatif admettant K pour sous-corps) est **algébrique** si tout $x \in L$ est algébrique sur K. Montrer que, pour que K soit algébriquement clos, il faut et il suffit qu'on ait $L = K$ pour toute extension algébrique de K.

24. Un corps algébriquement clos possède toujours une infinité d'éléments.

¶ **25.** (Démonstration du théorème de d'Alembert-Gauss). Cet *Exercice* suppose connues les propriétés des fonctions continues dans le plan (en particulier et tout spécialement le fait qu'une fonction continue positive sur un ensemble compact y atteint effectivement son minimum). On désigne par

$$f(z) = a_0 + \cdots + a_n z^n$$

un polynôme non constant à coefficients complexes; on suppose $a_n \neq 0$.

a) Montrer que le rapport

$$f(z)/a_n z^n$$

tend vers 1 quand $|z|$ augmente indéfiniment, i.e. que pour tout $\varepsilon > 0$ il existe $r > 0$ tel que

$$|z| > r \qquad \text{implique} \qquad \left|1 - \frac{f(z)}{a_n z^n}\right| < \varepsilon.$$

b) Soit

$$m = \inf_{z \in \mathbf{C}} |f(z)|;$$

montrer qu'il existe un nombre $r' > 0$ tel que

$$|z| \geqslant r' \qquad \text{implique} \qquad |f(z)| \geqslant m + 1.$$

En appliquant le théorème du minimum à la fonction continue $|f(z)|$ sur l'ensemble compact $|z| \leqslant r'$, montrer qu'il existe un $z_0 \in \mathbf{C}$ tel que

$$|f(z_0)| = m.$$

[Si le théorème de d'Alembert est vrai, il est clair que $m = 0$; pour montrer que le théorème en question est vrai, il est donc nécessaire, et bien entendu suffisant, de montrer que $m = 0$. C'est le but de la question suivante.]

c) On suppose $m \neq 0$; en remplaçant z par $z - z_0$ et f par $f/f(z_0)$ on se ramène au cas où l'on a

$$f(0) = 1, \qquad |f(z)| \geqslant 1 \qquad \text{pour tout} \quad z \in \mathbf{C}.$$

Soit

$$f(z) = 1 + b_q z^q + b_{q+1} z^{q+1} + \cdots + b_n z^n \qquad \text{avec} \qquad b_q \neq 0;$$

montrer qu'il existe un nombre $M > 0$ tel que

$$|z| \leqslant 1 \qquad \text{implique} \qquad |f(z) - 1 - b_q z^q| \leqslant M.|z|^{q+1};$$

déduire de là qu'on a $|f(z)| < 1$ (contradiction avec l'hypothèse, ce qui achèvera la démonstration) pourvu que z soit choisi de telle sorte qu'on ait

$$|z| \leqslant 1, \qquad |z| < |b_q|/M, \qquad \operatorname{Arg}(b_q) + q.\operatorname{Arg}(z) = \pi.$$

¶¶ **26.** Soient E un corps commutatif algébriquement clos, L un corps commutatif quelconque, et σ un isomorphisme de L sur un sous-corps L' de E. On considère une extension M de L et on suppose $M = L[z]$ où z est algébrique sur L. Soit

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

le polynôme minimal de z sur L; on note

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

le polynôme, à coefficients dans L', qui s'en déduit par σ, et on considère une racine z' de f^σ dans E; soit $M' = L'[z']$. Montrer qu'il existe un et un seul isomorphisme σ' de M sur M' qui coïncide avec σ sur L, et applique z sur z'.
Déduire de là le résultat suivant : soient E une extension algébriquement close d'un corps commutatif K, et L une extension de degré fini de K. Alors il existe un isomorphisme j de L sur un sous-corps de E, tel que $j(x) = x$ pour tout $x \in K$. (Raisonner par récurence sur le degré de L sur K. On peut en fait démontrer que le résultat subsiste pour toute extension *algébrique*, de degré fini ou non, de K).

¶¶ **27.** Soient K un corps commutatif, E une extension algébriquement close de K, et L une extension de degré fini de K; on suppose L *séparable sur* K (§ 26, *Exercice* 4, *h*)) et on pose $n = [L : K]$. Montrer que le nombre d'isomorphismes j de L dans E, tels que $j(x) = x$ pour tout $x \in K$, est exactement n (raisonner comme dans l'*Exercice* 26 en utilisant l'*Exercice* 11 du § 32).
On désigne par $j_1, \ldots, j_n$ les isomorphismes en question. Pour $h \neq h$, on note L_{hh} l'ensemble des $z \in L$ tels que $j_h(z) = j_h(z)$; montrer que c'est un sous-corps de L contenant K, et distinct de L.

On suppose K *infini*; montrer que la réunion des L_{kh} n'est pas L tout entier et qu'il existe un $z \in L$ tel que les n éléments $j_k(z)$ soient deux à deux distincts. En déduire que si L est une extension séparable de degré fini d'un corps K infini, il existe un $z \in L$ tel que $L = K[z]$ (**théorème de l'élément primitif,** démontré d'abord par Dedekind pour les corps de nombres algébriques, i.e. pour $K = \mathbf{Q}$; en fait, il est encore valable pour K fini vu l'*Exercice* 2 ci-dessus).

¶ **28.** On considère l'extension

$$L = \mathbf{Q}[\sqrt{3}, \sqrt[3]{2}]$$

de $\mathbf{Q}$. Construire un nombre algébrique z tel que $L = \mathbf{Q}[z]$.

¶¶ **29.** Soient K un corps commutatif, L une extension séparable et de degré fini n de K, E une extension algébriquement close de K, et $j_1, \ldots, j_n$ les n isomorphismes de L dans E tels que $j_h(x) = x$ pour tout $x \in K$ (*Exercice* 27). On se propose de montrer que

$$\mathrm{Tr}_{L/K}(z) = j_1(z) + \cdots + j_n(z)$$
$$\mathrm{N}_{L/K}(z) = j_1(z) \ldots j_n(z)$$

pour tout $z \in L$.

a) Soit $(a_i)_{1 \leqslant i \leqslant n}$ une base de L sur K. Montrer que la matrice

$$A = (j_k(a_h))_{1 \leqslant k, h \leqslant n}$$

(à coefficients dans E) est inversible (utiliser l'*Exercice* 16 des §§ 10, 11 ainsi que la caractérisation des systèmes de Cramer).

b) Pour tout $z \in L$ on pose

$$za_i = \sum_j \xi_{ij} a_j$$

avec des $\xi_{ij} \in K$; on introduit les matrices

$$U_z = (\xi_{ij})_{1 \leqslant i, j \leqslant n}$$

et

$$D_z = \begin{pmatrix} j_1(z) & 0 & \ldots & 0 \\ 0 & j_2(z) & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & j_n(z) \end{pmatrix};$$

montrer qu'on a la relation

$$U_z = A D_z A^{-1}.$$

c) Achever la démonstration en observant que $\mathrm{Tr}_{L/K}(z) = \mathrm{Tr}(U_z)$ et que $\mathrm{N}_{L/K}(z) = \det(U_z)$ (cf. § 26, *Exercice* 4).

[Le lecteur notera que ce raisonnement montre aussi que les valeurs propres dans E de l'endomorphisme

$$u_z : x \to zx$$

de L, où l'on regarde L comme un espace vectoriel de dimension n sur K, sont précisément les $j_k(z)$, $1 \leqslant k \leqslant n$].

30. Démontrer que le polynôme

$$X^{n_1} + X^{n_2} + \ldots + X^{n_k},$$

où

$$n_r \equiv r - 1 \pmod{k},$$

est divisible par le polynôme

$$1 + X + X^2 + \cdots + X^{k-1}.$$

¶ **31.** Pour quelles valeurs de r le polynôme $\Phi_n(X^r)$ est-il divisible par le polynôme $\Phi_n(X)$?

32. Soit f un polynôme à une indéterminée à coefficients dans un corps commutatif. Si $f(X^n)$ est divisible par $X - 1$, alors $f(X^n)$ est divisible par $X^n - 1$.

¶¶ **33.** (Démonstration du Nullstellensatz de Hilbert).

a) Soient L un corps commutatif et A un sous-anneau de L; on suppose qu'il existe des éléments $y_1, \ldots, y_q$ de L, en nombre fini, tels que

$$L = A[y_1, \ldots, y_q],$$

et de plus que chaque y_j vérifie une relation algébrique non triviale à coefficients dans A. Montrer qu'il existe un élément $b \neq 0$ de A tel que

Kcorps des fractions de A $K = A[b^{-1}]$

(choisir b de telle sorte que L soit un $A[b^{-1}]$-module de type fini et appliquer l'*Exercice* 24 du § 19).

b) Montrer que tout idéal premier non nul de l'anneau A contient b.

c) On suppose qu'il existe un sous-corps K de L tel que A soit le sous-anneau de L engendré par K et par un nombre fini d'éléments de L algébriquement indépendants sur K. Montrer qu'alors $A = K$ et que L est une extension algébrique de degré fini de K (observer que, dans un anneau de polynômes sur un corps, l'intersection des idéaux premiers non nuls se réduit à 0).

d) Soient K un corps commutatif et L une extension de K; on suppose qu'il existe un nombre fini d'éléments $z_1, \ldots, z_r$ de L tels que

$$L = K[z_1, \ldots, z_r];$$

montrer qu'alors L est une extension algébrique de degré fini de K, et qu'en particulier $L = K$ si K est algébriquement clos [extraire de la famille $z_1, \ldots, z_r$ les éléments algébriquement indépendants en nombre aussi grand que possible et appliquer *c*) à l'anneau A engendré par K et ces éléments].

e) Soient K un corps commutatif et $\mathfrak{m}$ un idéal maximal de l'anneau de polynômes $K[X_1, \ldots, X_r]$; montrer que l'anneau quotient $L = K[X_1, \ldots, X_r]/\mathfrak{m}$ est un corps, extension algébrique de degré fini de K [appliquer la question *d*), et l'*Exercice* 7 du § 8]. En déduire le Nullstellensatz [Voir une autre démonstration au § 35, *Exercice* 51].

¶¶ **34.** Soit p un nombre premier et soit $k = \mathbf{Z}/p\mathbf{Z}$ le corps des entiers modulo p. Si

$$f(X) = f(X_1, \ldots, X_n)$$

est un polynôme en n variables, à coefficients dans k, on note $S(f)$ la somme des valeurs de f, autrement dit on pose

$$S(f) = \sum_{x_i \in k} f(x_1, \ldots, x_n).$$

a) On suppose que f est un monôme $X_1^{m_1} \ldots X_n^{m_n}$. Montrer que l'on a alors $S(f) = 0$,

sauf si tous les m_i sont divisibles par $p-1$ et $\geqslant 1$, auquel cas on a $S(f) = (-1)^n$. (Se ramener au cas d'une variable.)

b) Utiliser *a*) pour prouver que $S(f) = 0$ si $\deg(f) < n(p-1)$.

c) Soit $\varphi(X) = \varphi(X_1, \ldots, X_n)$ un polynôme à coefficients dans k. On pose

$$f(X) = 1 - \varphi(X)^{p-1}.$$

Montrer que l'on a

$$f(x) = 1 \quad \text{si} \quad \varphi(x) = 0, \qquad x \in k^n$$
$$f(x) = 0 \quad \text{si} \quad \varphi(x) \neq 0, \qquad x \in k^n.$$

En déduire que le nombre $N(\varphi)$ de zéros de φ dans k^n vérifie la congruence

$$N(\varphi) \equiv S(f) \pmod{p}.$$

d) On suppose que $\deg(\varphi) < n$. Déduire de *b*) et *c*) que l'on a $N(\varphi) \equiv 0 \pmod{p}$. En particulier, si φ est sans terme constant, φ a au moins un zéro distinct de $(0, \ldots, 0)$ (*théorème de Chevalley*).

e) Étendre ce qui précède au cas d'un nombre fini d'équations $\varphi_\alpha(x) = 0$, avec $\Sigma \deg \varphi_\alpha < n$. (Prendre pour f le produit des $1 - \varphi_\alpha^{p-1}$.)

§ 34

Pour chacune des matrices figurant dans les *Exercices* **1** à **14** ci-dessous, répondre aux questions suivantes : *a*) Calculer les valeurs propres (on prendra $\mathbf{C}$ 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 $\mathbf{C}$, déterminer le plus petit sous-corps de $\mathbf{C}$ sur lequel elle est diagonalisable. *e*) Si la matrice considérée n'est pas diagonalisable sur $\mathbf{C}$, 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. $\begin{pmatrix} 1 & 0 & 0 & 0 & \ldots & 0 \\ 1 & 2 & 0 & 0 & \ldots & 0 \\ 1 & 2 & 3 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 2 & 3 & 4 & \ldots & n \end{pmatrix}$

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

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, ..., 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 endomorphises 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 **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

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

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 $K = C$), 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 $K = C$), *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

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

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 $\overline{z} = x - y\sqrt{d}$).

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

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

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 $A = k[X]$ 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

$$f(Z_1 + c_1 Y, \ldots, Z_{n-1} + c_{n-1} Y, Y) = \sum_{0 \leqslant k \leqslant r} p_k(Z_1, \ldots, Z_{n-1})\, Y^k;$$

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

$$\begin{pmatrix} 4 & 10 & -19 & 4 \\ 1 & 6 & -8 & 3 \\ 1 & 4 & -6 & 2 \\ 0 & -1 & 1 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 41 & -4 & -96 & -7 \\ 14 & -13 & -91 & -18 \\ 40 & -4 & -95 & -8 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

¶¶ **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 $GL(n, K)$ une matrice *diagonalisable* D et une matrice *unipotente* U telles que l'on ait

$$A = DU = UD,$$

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 $K = \mathbf{R}$, il est clair que si $D, U \in M_n(\mathbf{C})$ 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 $D, U \in M_n(\mathbf{R})$ dans ce cas. Naturellement, si K n'est pas algébriquement clos, D est semi-simple mais non nécessairement diagonalisable sur K.]

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

$$X = D + N, \qquad D.N = N.D,$$

et que ces matrices sont entièrement déterminées par ces conditions. On prend $K = \mathbf{C}$ 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 $f \in E$ 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 $\mathbf{N}$ dans $\mathbf{C}$.

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 $f \in E$, 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,

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

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 $f \in E$ 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 $\mathbf{N}$ dans $\mathbf{C}$ soit dans E, i.e. vérifie la relation de récurence (*), il faut et il suffit qu'il existe des polynômes

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

vérifiant

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

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 $A = (a_{ij})_{1 \leqslant i,\, j \leqslant p}$ 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

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

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.

§ 36

(Les *Exercices* **1** à **21** sont relatifs à des propriétés valables sur un corps de base K quelconque, à ceci près que le lecteur devra parfois exclure les corps de caractéristique 2, ce que nous n'avons pas mentionné explicitement dans les énoncés en question. Les *Exercices* **22** à **51** supposent par contre que le corps de base est **R** ou **C**, ce qu'on a indiqué dans les énoncés. Il va de soi par ailleurs que les énoncés valables sur un corps de base quelconque, notamment ceux des *Exercices* **1**, **2**, **9** à **21**, sont tout aussi utiles lorsque le corps de base est **R** ou **C**.)

1. Soit V un espace vectoriel de dimension finie sur un corps commutatif K; on appelle **forme quadratique** sur V toute fonction polynomiale homogène de degré 2 sur V (§§ 27, 28, *Exercice* 17); i.e. toute application q de V dans K donnée par une relation de la forme

$$q(x) = \sum a_{ij} x_i x_j$$

où les a_{ij} sont des éléments donnés de K, et où les $x_i \in K$ sont les coordonnées du vecteur $x \in V$ par rapport à une base de V.

a) Montrer que si $f(x, y)$ est une forme bilinéaire symétrique sur V, la fonction

$$q(x) = f(x, x)$$

est une forme quadratique sur V (dite **associée** à f).

b) On suppose K de caractéristique $\neq 2$. Montrer que la donnée de q permet de reconstituer f, à l'aide de la formule

$$f(x, y) = \frac{q(x+y) - q(x-y)}{4}.$$

c) Inversement, si q est une forme quadratique sur V, la formule précédente définit une forme bilinéaire symétrique f sur V, et on a $q(x) = f(x, x)$.

d) Pour qu'une base de V soit orthogonale par rapport à f, il faut et il suffit que l'expression de q par rapport à cette base soit de la forme

$$q(x) = c_1 x_1^2 + c_2 x_2^2 + \cdots + c_r x_r^2$$

(on dit alors que q est **réduite à une somme de carrés**).

[Les résultats précédents montrent que l'étude des formes bilinéaires symétriques est équivalente, en caractéristique $\neq 2$, à celle des formes quadratiques. On utilisera souvent le langage des formes quadratiques dans les *Exercices* suivants.]

2. Soit K un corps commutatif de caractéristique $\neq 2$. On considère une forme quadratique

$$q(x) = \sum_{1 \leqslant i,j \leqslant n} a_{ij} x_i x_j$$

sur K^n.

a) On suppose $a_{11} \neq 0$; montrer qu'il existe alors une forme linéaire f_1 sur K^n telle que l'on ait

$$q(x) = a_{11} . f_1(x)^2 + q_1(x)$$

où la forme quadratique q_1 ne dépend plus de la variable x_1 (écrire $q(x)$ comme un trinôme du second degré en x_1, dont les coefficients dépendent de $x_2, \ldots, x_n$, et mettre ce trinôme sous la forme canonique des Lycées et Collèges).

b) On suppose $a_{11} = 0$ mais $a_{12} \neq 0$, et on choisit comme nouvelles coordonnées dans K^n les formes linéaires

$$\begin{aligned} y_1 &= x_1 + x_2 \\ y_2 &= x_1 - x_2 \\ y_i &= x_i \qquad (3 \leqslant i \leqslant n). \end{aligned}$$

Montrer qu'on a

$$q(x) = \sum_{1 \leqslant i,j \leqslant n} b_{ij} y_i y_j$$

avec $b_{11} \neq 0$, et par suite qu'on peut, dans le nouveau système de coordonnées, appliquer la question *a*).

c) Déduire de ce qui précède une méthode pratique pour réduire une forme quadratique à une somme de carrés *Exercice* [1, *d*)], ou pour construire une base orthogonale pour une forme bilinéaire symétrique donnée.

Dans les *Exercices* 3 à 8, on demande de mettre la forme quadratique donnée sous forme d'une somme de carrés en utilisant la méthode indiquée dans l'*Exercice* 2; on prendra $\mathbf{Q}$ pour corps de base, et on indiquera dans chaque cas le changement de coordonnées qui conduit au résultat cherché

3. $x_1^2 + x_2^2 + 3x_3^2 + 4x_1x_2 + 2x_1x_3 + 2x_2x_3$.

4. $x_1^2 + 5x_2^2 - 4x_3^2 + 2x_1x_2 - 4x_1x_3$.

5. $2x_1^2 + 18x_2^2 + 8x_3^2 - 12x_1x_2 + 8x_1x_3 - 27x_2x_3$.

6. $x_1^2 + 2x_2^2 + x_4^2 + 4x_1x_2 + 4x_1x_3 + 2x_1x_4 + 2x_2x_3 + 2x_2x_4 + 2x_3x_4$.

7. $3x_1^2 + 2x_2^2 - x_3^2 - 2x_4^2 + 2x_1x_2 - 4x_2x_3 + 2x_2x_4$.

8. $3x_1^2 - 2x_2^2 + 2x_3^2 + 4x_1x_2 - 3x_1x_3 - x_2x_3$.

9. Soit f une forme bilinéaire sur un espace vectoriel E de dimension finie sur un corps K.

a) Soit

$$A = (f(a_i, a_j))_{1 \leqslant i,j \leqslant n}$$

la matrice de f par rapport à une base (a_i) de E. On identifie chaque vecteur $x \in E$ à la matrice colonne formée avec les composantes de x par rapport à la base en question. Montrer qu'on a

alors

$$f(x, y) = {}^t y . A . x$$

quels que soient $x, y \in E$.

b) Soit B la matrice de f par rapport à une autre base (b_i) de E. On note P la matrice de passage de la base (a_i) à la base (b_i). Montrer que

$$B = {}^t PAP.$$

c) Déduire de là que, pour toute matrice symétrique $S \in M_n(K)$, il existe une matrice diagonale D et une matrice $P \in GL(n, K)$ telles que

$$S = {}^t PDP,$$

et réciproquement; montrer de plus que, si K est algébriquement clos, on peut supposer tous les coefficients de D égaux à 1 ou 0, et que si $K = \mathbf{R}$ on peut supposer qu'ils sont égaux à 0, + 1 ou − 1.

10. Pour toute matrice symétrique S d'ordre n, à coefficients dans un corps algébriquement clos K, il existe une matrice $X \in M_n(K)$ telle que

$$S = {}^t XX,$$

et réciproquement.

11. Soit f une forme hermitienne sur un espace vectoriel E de dimension finie sur un corps commutatif K (muni d'une involution, cf. l'introduction du § 36).

a) Soit $A = (f(a_i, a_j))_{1 \leqslant i,j \leqslant n}$ la matrice de f par rapport à une base (a_i) de E. Montrer que, si l'on identifie chaque $x \in E$ à la matrice colonne formée avec les composantes de x par rapport à la base en question, on a

$$f(x, y) = y^* . A . x$$

quels que soient $x, y \in E$.

b) Soit u une endomorphisme de E, dont la matrice par rapport à la base (a_i) est U; montrer que la matrice par rapport à cette base de l'adjoint de u relativement à f (on suppose maintenant f non dégénérée) est

$$A^{-1}U^*A.$$

c) En utilisant l'existence pour toute forme hermitienne d'une base orthogonale, montrer que, pour toute matrice hermitienne $A \in M_n(K)$, il existe une matrice hermitienne diagonale $D \in M_n(K)$ et une matrice inversible $P \in GL(n, K)$ telles que

$$A = P^*DP.$$

12. Pour que le produit de deux matrices hermitiennes soit une matrice hermitienne, il faut et il suffit que les deux matrices données commutent.

13. Soient E un espace vectoriel complexe de dimension finie et f une forme hermitienne définie positive sur E.

a) Montrer que, pour tout sous-espace vectoriel M de E, l'opérateur de projection orthogonale p_M est autoadjoint relativement à f.

b) Inversement, pour tout endomorphisme p de E tel que

$$p = p^* = p^2,$$

il existe un sous-espace vectoriel M tel que $p = p_M$.

c) Soient M et N deux sous-espaces vectoriels de E; soit M′ (resp. N′) le sous-espace formé des $x \in M$ (resp. $x \in N$) orthogonaux à $M \cap N$. Montrer que, pour que p_M et p_N commutent, il faut et il suffit que M′ et N′ soient orthogonaux (la situation généralise alors celle de deux plans perpendiculaires dans l'espace usuel). Si cette condition est réalisée, on a

$$p_{M\cap N} = p_M \circ p_N,$$
$$p_{M+N} = p_M + p_N - p_M \circ p_N.$$

d) Généralisation à un corps de base quelconque? (Considérer des sous-espaces non isotropes).

14. Soit f une forme bilinéaire symétrique sur un espace vectoriel E de dimension finie sur un corps commutatif K. Soient $a_1, \ldots, a_r$ des éléments de E et U le sous-espace vectoriel qu'ils engendrent. Les deux propriétés suivantes sont équivalentes: (*i*) U est non isotrope et les a_i forment une base de U; (*ii*) le déterminant des $f(a_i, a_j)$ n'est pas nul. Corollaire: si f ne possède aucun vecteur isotrope (exemple : $K = \mathbf{R}$ et f définie positive), pour que des vecteurs $a_1, \ldots, a_r$ soient linéairement indépendants il faut et il suffit que le déterminant des $f(a_i, a_j)$ soit non nul.

¶ **15.** Soit

$$S = (a_{ij})_{1 \leqslant i,\, j \leqslant n}, \qquad a_{ij} = a_{ji},$$

une matrice symétrique à coefficients dans un corps commutatif K. On suppose que les **mineurs principaux**

$$D_p = \begin{vmatrix} a_{11} & \cdots & a_{1p} \\ \cdots & \cdots & \cdots \\ a_{p1} & \cdots & a_{pp} \end{vmatrix} \quad (1 \leqslant p \leqslant n)$$

de S ne sont pas nuls. Montrer qu'il existe alors une matrice diagonale

$$D = \begin{pmatrix} c_1 & 0 & 0 & \cdots & 0 \\ 0 & c_2 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & c_n \end{pmatrix}$$

et une matrice triangulaire de la forme

$$T = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ t_{21} & 1 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ t_{n1} & t_{n2} & t_{n3} & \cdots & t_{n,n-1} & 1 \end{pmatrix},$$

à coefficients dans K, telles que

$$S = TD{}^tT;$$

que D et T sont entièrement déterminées par S; et que les termes diagonaux de D sont donnés par les relations

$$c_1 = D_1, \quad c_2 = D_2/D_1, \quad \ldots, \quad c_n = D_n/D_{n-1}.$$

Corollaire (Jacobi) : soit

$$q(x) = \Sigma a_{ij} x_i x_j \quad (a_{ij} = a_{ji})$$

une forme quadratique telle que les mineurs principaux de la matrice (a_{ij}) ne soient pas nuls; alors on peut réduire q à une somme de carrés à l'aide d'un changement *triangulaire* de coordonnées.

(Pour établir l'existence de T et D on pourra utiliser le § 23, *Exercice* 11, ou bien raisonner par récurrence sur n, en écrivant

$$S = \begin{pmatrix} S_1 & {}^tu \\ u & a_{nn} \end{pmatrix}$$

où S_1 est une matrice carrée d'ordre $n - 1$, u une matrice colonne à $n - 1$ éléments, et utiliser une décomposition en blocs analogues pour D et T).

¶ **16.** Les notations restant celles de l'*Exercice* précédent, on suppose S de rang r quelconque, et on cherche à mettre S sous la forme

$$S = TD{}^tT$$

avec $c_1 \neq 0, \ldots, c_r \neq 0, c_{r+1} = \cdots = c_n = 0$. Montrer que, pour que le problème admette une solution, il faut et il suffit qu'on ait

$$D_p \neq 0 \quad \text{pour } 1 \leqslant p \leqslant r.$$

17. Soient E un espace vectoriel de dimension finie sur un corps commutatif K, et f une forme bilinéaire symétrique non dégénérée sur E; on note q la forme quadratique $f(x, x)$. On suppose qu'il existe des vecteurs isotropes non nuls pour f. Montrer alors que, pour tout $c \in K$, il existe $x \in E$ tel que

$$q(x) = c.$$

¶ **18.** Soient E un espace vectoriel de dimension finie n sur un corps commutatif K, et f une forme bilinéaire symétrique non dégénérée sur E.

a) Soit H un sous-espace vectoriel de E, non isotrope pour f. Montrer qu'il existe un et un seul automorphisme s_H de f pour lequel on ait

$$s_H(x) = \begin{cases} x & \text{si } x \in H \\ -x & \text{si } x \in H^\perp \end{cases}$$

(symétrie par rapport à H).

b) Soient u un automorphisme de f et x un vecteur non isotrope pour f. Montrer que l'un au moins des vecteurs $u(x) - x$, $u(x) + x$ est non isotrope. En déduire qu'il existe dans E un sous-espace H non isotrope tel que l'on ait $s_H(u(x)) = x$. [Prendre pour H soit le sous-espace orthogonal à $u(x) + x$, soit le sous-espace engendré par $u(x) - x$].

c) En déduire, par récurence sur n, que *tout automorphisme de f est produit d'au plus n symétries par rapport à des sous-espaces non isotropes de* E.

¶¶ **19.** Soient E un espace vectoriel de dimension finie sur un corps commutatif K et f une forme bilinéaire symétrique sur E. On dit qu'un sous-espace vectoriel U de E est **totalement isotrope** pour f si $f(x, x) = 0$ pour tout $x \in U$; on dit que U est un sous-espace totalement isotrope **maximal** s'il n'est contenu dans aucun autre sous-espace totalement isotrope pour f. On se propose d'établir que *tous les sous-espaces totalement isotropes maximaux de f ont la même dimension*, qu'on appelle l'**indice** de f (ou de la forme quadratique correspondante).

a) Pour que U soit totalement isotrope pour f, il faut et il suffit que

$$f(x, y) = 0 \quad \text{quels que soient } x, y \in U$$

i.e. que $U \subset U^\perp$ (utiliser l'*Exercice* 1).

b) Soient U et V deux sous-espaces totalement isotropes pour f. Montrer que pour tout, $x \in U \cap V^\perp$, le sous-espace $V + Kx$ est totalement isotrope.

c) Soient U et V deux sous-espaces totalement isotropes pour f; soient M un supplémentaire de $U \cap V$ dans U, et N un supplémentaire de $U \cap V$ dans V. Montrer que

$$U \cap V^\perp = (U \cap V) \oplus (M \cap N^\perp).$$

Montrer que les éléments de $M \cap N^\perp$ s'obtiennent en résolvant un système de $s = \dim(N)$ équations linéaires et homogènes à $r = \dim(M)$ inconnues. En déduire que, si

$$\dim(V) < \dim(U),$$

il existe un $x \in U$ non dans V tel que le sous-espace $V + Kx$ soit totalement isotrope.

d) Montrer que tout sous-espace totalement isotrope est contenu dans au moins un sous-espace totalement isotrope maximal. En déduire, à l'aide de la question *c*), le résultat annoncé.

¶¶ **20.** (Démonstration du **théorème de Witt**). Soit f une forme bilinéaire symétrique non dégénérée sur un espace vectoriel E de dimension finie sur un corps commutatif K de caractéristique différente de 2. Soient M et N deux sous-espaces de même dimension de E, et u une application linéaire bijective de M sur N. On se propose de montrer que les deux propriétés suivantes sont équivalentes : (*i*) il existe un automorphisme de f qui coïncide avec u sur M; (*ii*) on a $f[u(x), u(y)] = f(x, y)$ quels que soient $x, y \in M$. Comme il est trivial que (*i*) implique (*ii*), on se borne ci-dessous à montrer que (*ii*) implique (*i*).

a) Soient x et y deux éléments de E tels que

$$f(x, x) = f(y, y) \neq 0;$$

montrer qu'il existe un automorphisme de f appliquant x sur y (montrer que $x - y$ et $x + y$ ne sont pas tous les deux isotropes, et prendre la symétrie par rapport à H, où H est soit l'hyperplan orthogonal à $x - y$, soit la droite engendrée par $x + y$).

b) On suppose que M et N ne sont pas totalement isotropes. Montrer à l'aide de la question *a*) qu'on peut supposer $u(x) = x$ pour un $x \in M$ non isotrope. Soit E' l'hyperplan orthogonal à x; montrer que, pour construire un automorphisme de f prolongeant u, il suffit de construire un automorphisme de la restriction f' de f à E' égal à u sur $E' \cap M$. En déduire dans ce cas le théorème de Witt par récurence sur $\dim(E)$.

c) On suppose dorénavant M et N totalement isotropes. On choisit un $x \notin M^\perp$. Montrer qu'il existe un $y \notin N^\perp$ tel que l'on ait

$$f[y, u(z)] = f(x, z) \quad \text{pour tout } z \in M.$$

Montrer qu'on peut en outre supposer

$$f(y, y) = f(x, x)$$

(remplacer y par $y + tn$ avec $t \in K$ et $n \in N$ convenablement choisis).

d) Déduire de la question *c*) qu'il existe des sous-espaces non totalement isotropes $M' \supset M$ et $N' \supset N$, ainsi qu'un isomorphisme u' de M' sur N', tels que l'on ait

$$f[u'(x), u'(y)] = f(x, y) \quad \text{quels que soient } x, y \in M'$$
$$u' = u \text{ sur } M,$$

et achever à partir de là la démonstration du théorème de Witt.

¶¶ **21.** Soient E un espace vectoriel de dimension finie n sur un corps commutatif K, f une forme bilinéaire symétrique non dégénérée sur E, et M un sous-espace totalement isotrope de dimension r de E.

a) Montrer qu'il existe dans E des vecteurs non isotropes non orthogonaux à M.

b) Montrer qu'il existe un sous-espace totalement isotrope N tel que

$$E = M^\perp \oplus N$$

(prendre le symétrique de M par rapport à la droite engendrée par l'un des vecteurs construits dans la question précédente).

c) Soit $H = M^\perp \cap N^\perp$; montrer que

$$E = M \oplus H \oplus N,$$

et que H ne contient aucun vecteur isotrope non nul si M est totalement isotrope maximal. On forme une base de E en réunissant des bases de M, H et N; montrer que la matrice de f par rapport à cette base est de la forme

$$S = \begin{pmatrix} 0 & 0 & A \\ 0 & S_1 & 0 \\ {}^tA & 0 & 0 \end{pmatrix}$$

où A est une matrice carrée inversible d'ordre r, et S_1 une matrice symétrique d'ordre $n - 2r$.

d) Trouver à quelles conditions une matrice de la forme

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

(où U et W sont carrées d'ordre r, et V carrée d'ordre $n - 2r$) représente, par rapport à la base considérée dans E, un automorphisme de f. En déduire que pour tout automorphisme u de l'espace vectoriel M, il existe un automorphisme de f qui se réduit à u sur M. Pouvez-vous déduire ce résultat du théorème de Witt?

22. Soit $q(x)$ une forme quadratique sur un espace vectoriel réel (resp. complexe) E de dimension finie; montrer qu'il existe une base de E par rapport à laquelle l'expression de q est de la forme

(*) $$x_1^2 + \cdots + x_p^2 - (x_{p+1}^2 + \cdots + x_{p+q}^2)$$

(resp.

$$x_1^2 + \cdots + x_r^2).$$

Trouver une telle base (dans le cas réel et dans le cas complexe) pour les formes quadratiques des *Exercices* 3 à 8.

23. Soient $f_1, \ldots, f_{p+q}$ des formes linéaires sur un espace vectoriel réel U de dimension finie; on suppose que, sur U, la forme quadratique

$$q(x) = f_1(x)^2 + \cdots + f_p(x)^2 - f_{p+1}(x)^2 - \cdots - f_{p+q}(x)^2$$

soit définie positive, i.e. vérifie

$$q(x) > 0 \quad \text{pour tout} \quad x \neq 0.$$

Montrer qu'on a alors

$$\dim(U) \leqslant p.$$

(Remarquer que dans le cas contraire il existerait un $x \neq 0$ où $f_1, \ldots, f_p$ seraient toutes nulles).

¶ **24.** Soit $q(x)$ une forme quadratique sur un espace vectoriel réel E de dimension finie. On choisit une base de E par rapport à laquelle q est mise sous la forme (*) de l'*Exercice* 22; montrer, à l'aide de l'*Exercice* précédent, que tout sous-espace vectoriel U de E sur lequel $q(x)$ est définie positive est de dimension p au plus. En déduire (**loi d'inertie** des formes quadratiques) que les entiers p et q de l'*Exercice* 22 sont indépendants du choix de la base de E par rapport à laquelle $q(x)$ se met sous la forme (*).
[Le couple (p, q) formé du nombre p de carrés positifs et du nombre q de carrés négatifs dans la formule (*) s'appelle la **signature** de la forme quadratique considérée ou de la forme bilinéaire symétrique correspondante. Le nombre p est la dimension maximum des sous-espaces sur lesquelles la forme donnée est définie positive, et le nombre q la dimension maximum des sous-espaces sur lesquels elle est définie négative].

¶ **25.** Deux formes quadratiques q et q' sur un espace vectoriel E de dimension finie sur un corps commutatif sont dites **équivalentes** s'il existe un automorphisme u de E tel que l'on ait

$$q'(x) = q(u(x)) \qquad \text{pour tout } x \in E.$$

On suppose que le corps de base soit $\mathbf{R}$; montrer que, pour que q et q' soient équivalentes, il faut et il suffit qu'elles aient même signature.

26. Montrer que les deux formes quadratiques suivantes sur $\mathbf{R}^3$ sont équivalentes, et construire un automorphisme de $\mathbf{R}^3$ transformant la première en la seconde :

$$2x^2 + 9y^2 + 3z^2 + 8xy - 4xz - 10yz$$
$$3x^2 + 3y^2 + 6z^2 - 4xy - 4xz + 8yz.$$

Même problème pour les formes

$$5x^2 + 5y^2 + 2z^2 + 8xy + 6xz + 6yz \qquad \text{et} \qquad 4x^2 + y^2 + 9z^2 - 12xz.$$

¶ **27.** On considère sur $\mathbf{R}^n$ la forme bilinéaire symétrique f correspondant à la forme quadratique

$$q(x) = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$$

et on suppose $p \quad q$. Montrer que le sous-espace engendré par les vecteurs

$$e_1 + e_{p+1},\ e_2 + e_{p+2},\ \ldots,\ e_p + e_{2p},\ e_{p+q+1},\ \ldots,\ e_n$$

est totalement isotrope maximal pour f (*Exercice* 19).
En déduire que si f est une forme bilinéaire symétrique de signature (p, q) sur un espace vectoriel réel de dimension n, l'indice de f (*Exercice* 14) est $r + n - p - q$ où r est le plus petit des deux entiers p et q.
Quelle est la dimension des sous-espaces totalement isotropes maximaux de la forme de Lorentz?

¶ **28.** Soit f une forme bilinéaire symétrique non dégénérée sur un espace vectoriel réel E de dimension finie. Soient M et N deux sous-espaces vectoriels de E, tels que $\dim(M) = \dim(N)$. Pour qu'il existe un automorphisme de f appliquant M sur N, il faut et il suffit que les restrictions de f à M et N aient la même signature (utiliser le théorème de Witt et les *Exercices* 24 et 25)
On prend pour f la forme de Lorentz et on considère, sur l'ensemble de tous les sous-espaces vectoriels de E, la relation d'équivalence « il existe un automorphisme u de f tel que $u(M) = N$ ». Combien d'éléments l'ensemble quotient comporte-t-il?
Même question pour la forme quadratique

$$x^2 + y^2 + z^2 - t^2 - u^2$$

sur $\mathbf{R}^5$.

29. Pour qu'une matrice hermitienne complexe $H \in M_n(\mathbf{C})$ soit positive, il faut et il suffit qu'il existe une matrice $X \in M_n(\mathbf{C})$ telle que

$$H = X^*X;$$

si de plus H est réelle on peut supposer X réelle [utiliser l'*Exercice* 11, *c*), et noter que les termes diagonaux de D sont positifs si H est positive].
En déduire que si

$$H = (a_{ij})_{1 \leqslant i,j \leqslant n}$$

est une matrice hermitienne complexe positive, on a

$$D_p = \begin{vmatrix} a_{11} & \cdots & a_{1p} \\ \cdots & \cdots & \cdots \\ a_{p1} & \cdots & a_{pp} \end{vmatrix} \geqslant 0 \quad \text{pour } 1 \leqslant p \leqslant n$$

et que

$$D_p = 0 \quad \text{implique} \quad D_{p+1} = \cdots = D_n = 0$$

(Montrer d'abord que $D_n \geqslant 0$, puis remplacer H par la matrice dont D_p est le déterminant, et utiliser l'*Exercice* 16). Cas $n = 2$? (Retrouver l'inégalité de Cauchy-Schwarz, et le « signe du trinôme ».)

¶ **30.** Soit

$$H = (h_{ij})_{1 \leqslant i,j \leqslant n}$$

une matrice hermitienne complexe positive. Montrer qu'il existe une matrice triangulaire complexe

$$T = \begin{pmatrix} t_{11} & t_{12} & \cdots & t_{1n} \\ 0 & t_{22} & \cdots & t_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & t_{nn} \end{pmatrix} \quad \text{avec } t_{ii} \text{ réel positif}$$

telle que

$$H = T^*T$$

(utiliser les *Exercices* 15 et 16). Si H est inversible, T est unique.
Déduire de ce qui précède que pour toute matrice hermitienne positive H on a l'inégalité

$$0 \leqslant \det(H) \leqslant h_{11}h_{22}\ldots h_{nn};$$

si H est inversible, on ne peut, de plus, avoir l'égalité que si H est diagonale.

¶ **31.** Soit A une matrice carrée inversible à coefficients complexes. Montrer qu'il existe une matrice unitaire U et une matrice triangulaire $T = (t_{ij})$, avec $t_{ii} > 0$ pour tout i, telles que

$$A = U.T,$$

et que U et T sont uniques (appliquer l'*Exercice* précédent à A^*A). Montrer que U et T sont réelles si A est réelle.

¶ **32.** Soit $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$ une matrice complexe; montrer qu'on a

$$|\det(A)|^2 \leqslant \prod_{j=1}^{j=n} (|a_{1j}|^2 + \cdots + |a_{nj}|^2),$$

¶ **33.** Pour qu'une matrice hermitienne complexe soit définie positive, il faut et il suffit que tous ses mineurs principaux soient strictement positifs (utiliser l'*Exercice* 30 et calculer les t_{ii} en fonction des mineurs principaux de la matrice donnée).

34. Trouver, à l'aide de l'*Exercice* précédent, les valeurs réelles de t pour lesquelles les formes quadratiques suivantes sont définies positives :

$$5x_1^2 + x_2^2 + tx_3^2 + 4x_1x_2 - 2x_1x_3 - 2x_2x_3$$
$$2x_1^2 + x_2^2 + 3x_3^2 + 2tx_1x_2 + 2x_1x_3$$
$$2x_1^2 + 2x_2^2 + x_3^2 + 2tx_1x_2 + 6x_1x_3 + 2x_2x_3$$
$$t(x_1^2 + x_2^2 + x_3^2) + 4x_1x_2 + 6x_1x_3 + 8x_2x_3$$

¶¶ **35.** Montrer que toute matrice hermitienne positive est somme de matrices de la forme

$$\begin{pmatrix} c_1\bar{c}_1 & \cdots & c_1\bar{c}_n \\ \cdots & \cdots & \cdots \\ c_n\bar{c}_1 & \cdots & c_n\bar{c}_n \end{pmatrix},$$

et réciproquement.
En déduire que si deux matrices complexes $(a_{ij})_{1\leqslant i,\,j\leqslant n}$ et $(b_{ij})_{1\leqslant i,\,j\leqslant n}$ sont hermitiennes positives, il en est de même de la matrice

$$(a_{ij}b_{ij})_{1\leqslant i,\,j\leqslant n}$$

obtenue en multipliant les termes de mêmes indices des deux matrices données.

36. Soit H une matrice hermitienne complexe. Montrer que $1 - iH$ est inversible, que

$$U = (1 + iH)(1 - iH)^{-1} = (i - H)(i + H)^{-1}$$

est unitaire, et que -1 n'est pas valeur propre de U. Inversement, toute matrice unitaire U dont -1 n'est pas valeur propre peut s'obtenir de cette façon **(transformation de Cayley)**.

¶ **37.** Soit H une matrice complexe hermitienne positive. Montrer (en réduisant H à la forme diagonale à l'aide d'une matrice unitaire) qu'il existe une et une seule matrice hermitienne positive H′ telle que

$$H = H'^2.$$

(On dit que H′ est la **racine carrée positive** de H, et on écrit $H' = H^{\frac{1}{2}}$).

¶ **38.** Soient S et T deux matrices hermitiennes complexes; on suppose S définie positive. Montrer que les valeurs propres de ST sont réelles, et même positives si T est positive (utiliser l'*Exercice* 37).

¶ **39.** Soit A une matrice carrée inversible à coefficients complexes; montrer que la matrice

$$A^*A$$

est hermitienne et définie positive. En considérant sa racine carrée positive, montrer qu'on peut écrire

$$A = U.H$$

avec U unitaire, et H hermitienne définie positive; montrer de plus que le problème n'admet qu'une solution.
Montrer que, si A est réelle, il en est de même de U et de H.

¶¶ **40.** Soit $F \subset M_n(\mathbf{C})$ un ensemble de matrices normales deux à deux permutables. Montrer qu'il existe une matrice unitaire $U \in M_n(\mathbf{C})$ telle que UAU^{-1} soit diagonale pour toute $A \in F$. Interprétation géométrique? (Utiliser l'*Exercice* 22 du § 34).

Dans les *Exercices* **41** à **47** on demande de ramener la matrice symétrique réelle donnée à une matrice diagonale à l'aide d'une matrice orthogonale réelle.

41. $\begin{pmatrix} 6 & -2 & 2 \\ -2 & 5 & 0 \\ 2 & 0 & 7 \end{pmatrix}$ **42.** $\begin{pmatrix} 11 & 8 & 2 \\ 8 & 5 & -10 \\ 2 & -10 & 2 \end{pmatrix}$ **43.** $\begin{pmatrix} 8 & 4 & -1 \\ 4 & -7 & 4 \\ -1 & 4 & 8 \end{pmatrix}$

44. $\begin{pmatrix} 17 & -2 & -2 \\ -2 & 14 & -4 \\ -2 & -4 & 14 \end{pmatrix}$ **45.** $\begin{pmatrix} 0 & 1 & -3 & 0 \\ 1 & 0 & 0 & -3 \\ -3 & 0 & 0 & 1 \\ 0 & -3 & 1 & 0 \end{pmatrix}$

46. $\begin{pmatrix} 5 & -5 & 1 & 3 \\ -5 & 5 & 3 & 1 \\ 1 & 3 & 5 & -5 \\ 3 & 1 & -5 & 5 \end{pmatrix}$ **47.** $\begin{pmatrix} 9 & 0 & 0 & 0 \\ 0 & 5 & 4 & -2 \\ 0 & 4 & 5 & 2 \\ 0 & -2 & 2 & 8 \end{pmatrix}$

¶ **48.** Soient E un espace vectoriel réel de dimension finie, f une forme bilinéaire symétrique définie positive sur E, et u un automorphisme de f. On suppose que les seuls sous-espaces vectoriels de E stables par u sont E et $\{0\}$. Montrer qu'on est alors dans l'une des situations suivantes : (*i*) E est de dimension *un* et u est égal à $+1$ ou à -1; (*ii*) E est de dimension *deux*, et il existe une base orthonormale pour f par rapport à laquelle la matrice de u est de la forme

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

où φ est un nombre réel non multiple de π.

¶ **49.** Soient E un espace vectoriel réel de dimension finie, f une forme bilinéaire symétrique définie positive sur E, et u un automorphisme de f. Montrer qu'il existe une base de E, orthonormale relativement à f, et par rapport à laquelle la matrice de u est de la forme

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & -1 & & & \\ & & & & \ddots & & \\ & & & & & -1 & \\ & & & & & & \begin{matrix} \cos\varphi_1 & -\sin\varphi_1 \\ \sin\varphi_1 & \cos\varphi_1 \end{matrix} \\ & & & & & & & \ddots \\ & & & & & & & & \begin{matrix} \cos\varphi_h & -\sin\varphi_h \\ \sin\varphi_h & \cos\varphi_h \end{matrix} \end{pmatrix}$$

où les φ_i sont des nombres réels non multiples de π.

50. Pour tout nombre réel t, on pose

$$U(t) = \begin{pmatrix} \cos t & \sin t & 0 \\ -\sin t & \cos t & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad V(t) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos t & \sin t \\ 0 & -\sin t & \cos t \end{pmatrix}.$$

Montrer que, pour toute matrice orthogonale réelle X d'ordre 3 et de déterminant 1 (matrice d'une rotation dans l'espace usuel) il existe des nombres réels φ, ψ, θ tels que

$$X = U(\varphi)V(\theta)U(\psi).$$

(Observer que si l'on a deux bases orthonormales i, j, k et u, v, w, on passe de la première à la seconde en effectuant d'abord une rotation autour de k de façon à amener i dans le plan engendré par u et v, puis une rotation autour de l'intersection des plans ij et uv de façon à amener k sur w, et enfin une rotation autour de w). Les nombres φ, ψ et θ sont appelés les **angles d'Euler** de la matrice X (ou de la rotation correspondante).

¶¶ **51.** On considère la matrice hermitienne

$$S = \begin{pmatrix} 1_p & 0 \\ 0 & -1_q \end{pmatrix}$$

d'ordre $p + q$ et de signature (p, q). Montrer que le groupe des automorphismes de S, i.e. le groupe des matrices $W \in GL(p + q, \mathbf{C})$ telles que

$$W^*SW = S,$$

est l'ensemble des matrices

$$W = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

possédant la propriété suivante : il existe une matrice complexe Z à p colonnes et q lignes, telle que la matrice

$$1_p - Z^*Z$$

soit définie positive, et deux matrices unitaires U et V, d'ordres p et q, telles que l'on ait les relations

$$A = (1 - Z^*Z)^{-\frac{1}{2}}U, \qquad B = Z^*(1 - ZZ^*)^{-\frac{1}{2}}V,$$
$$C = Z(1 - Z^*Z)^{-\frac{1}{2}}U, \qquad D = (1 - ZZ^*)^{-\frac{1}{2}}V,$$

et de plus U, V et Z sont entièrement déterminées par W. Si W est réelle, il en est de même de U, V et Z. [NB — On pose

$$H^{-\frac{1}{2}} = \left(H^{\frac{1}{2}}\right)^{-1}$$

lorsque H est définie positive].

¶ **52.** Soit V un espace vectoriel de dimension paire $n = 2m$ sur un corps commutatif k.

a) Soit f une forme bilinéaire alternée (§ 22) non dégénérée sur V. On choisit deux vecteurs a et b tels que $f(a, b) = 1$ et on considère le plan $P \subset V$ engendré par a et b. Montrer que la restriction de f à P est non dégénérée, et en déduire de V est somme directe de P et du sous-espace V' des vecteurs orthogonaux à P pour f. En déduire que V admet une base par rapport

à laquelle l'expression de $f(x, y)$ en fonction des coordonnées de x et y est

$$f(x, y) = \sum_{i=1}^{i=m} x_i y_{2m-i} - y_i x_{2m-i}.$$

En déduire que deux formes bilinéaires alternées non dégénérées sur V peuvent être transformées l'une en l'autre par un automorphisme de V. Existe-t-il des formes bilinéaires alternées non dégénérées sur un espace de dimension impaire ?

b) On choisit une forme bilinéaire alternée non dégénérée f sur V, et on appelle plan non dégénéré de V tout sous-espace P de dimension 2 de V sur lequel f n'est pas identiquement nulle. Soit $Sp(V)$ le groupe des automorphismes u de V tels que

$$f(u(x), u(y)) = f(x, y)$$

quels que soient $x, y \in V$ (« groupe symplectique »). Montrer que $Sp(V)$ opère transitivement sur l'ensemble X des plans non dégénérés, et que si $P \in X$ le sous-groupe de $Sp(V)$ qui laisse fixe P (i.e. l'ensemble des $u \in Sp(V)$ tels que $u(P) = P$) est isomorphe au produit

$$SL(2, k) \times Sp(W),$$

où W est l'orthogonal de P dans V par rapport à f.

c) On suppose maintenant que k est fini à q éléments. Soit x un élément non nul de V. Montrer que x appartient à q^{n-2} plans non dégénérés. En déduire la formule

$$\text{Card}(X) = \begin{matrix} q^n & -1 \\ q^2 & -1 \end{matrix} q^{n-2}.$$

Soient P un plan non dégénéré et W son orthogonal dans V. Montrer que l'on a

$$\text{Card}(Sp(V)) = (q^n - 1)q^{n-1}\,\text{Card}(Sp(W)).$$

En déduire, par récurrence sur n, la formule

$$\text{Card}(Sp(V)) = q^{m(2m+1)} \prod_{i=1}^{i=m} (1 - 1/q^{2i}).$$

¶ **53.** Soit X un ensemble ayant 6 éléments. Soit Y l'ensemble des parties de X ayant 0 ou 2 éléments. On définit une loi de composition symétrique sur Y en posant :

$A + \varnothing = A$ pour tout $A \in Y$
$A + A = \varnothing$ pour tout $A \in Y$
$A + B = A \cup B - A \cap B$ si $A \cap B$ a un élément
$A + B = X - (A \cup B)$ si A et B sont disjoints et non vides.

a) Montrer que cette loi de composition fait de Y un groupe commutatif, d'ordre 16 et d'élément neutre $\varnothing$. Montrer que Y peut être muni (de façon unique) d'une structure d'espace vectoriel sur le corps $k = Z/2Z$ et que sa dimension est égale à 4.

b) Si $A, B \in Y$, on désigne par $f(A, B)$ l'élément de k défini par la congruence

$$f(A, B) \equiv \text{Card}(A \cap B) \pmod 2.$$

Montrer que f est une forme bilinéaire alternée non dégénérée sur Y.

c) Soient A, B, C trois parties de X, disjointes, et ayant chacune deux éléments. Montrer que $\{\varnothing, A, B, C\}$ est un sous-espace totalement isotrope de dimension 2 de Y (relativement à la forme f).

d) Soit S_X le groupe des permutations de X ; c'est un groupe isomorphe au groupe symétrique

S_6. Soit d'autre part $Sp(Y)$ le groupe des automorphismes de Y qui conservent la forme f (ce groupe est souvent noté $Sp_4(F_2)$). Montrer que tout élément de S_X définit un élément de $Sp(Y)$, et que l'homomorphisme $\varepsilon : S_X \to Sp(Y)$ ainsi obtenu est un isomorphisme. (On montrera d'abord que ε est injectif, puis on comparera les ordres de S_X et $Sp(Y)$.)

e) Soit F le k-espace vectoriel des fonctions $f : X = k$ telles que $\sum_{x \in X} f(x) = 0$. Soit $V = F/\{0,1\}$ le quotient de F par le sous-espace de dimension 1 engendré par la fonction constante 1. A tout $A \in Y$, on associe sa fonction caractéristique θ_A (égale à 1 sur A et à 0 sur $X - A$). Montrer que $A \to \theta_A$ définit un *isomorphisme* de l'espace vectoriel Y sur l'espace vectoriel V. Montrer que cet isomorphisme transforme la forme bilinéaire f de *b*) en la forme

$$u(\theta, \theta') = \sum_{x \in X} \theta(x)\ \theta'(x).$$