B. CALVO, J. DOYEN
A. CALVO, F. BOSCHET

exercices d'algèbre

1er cycle scientifique, 1re année
préparation aux grandes écoles

Armand Colin _ collection U

Série « Mathématiques » dirigée par André REVUZ

Bernard CALVO, Jacques DOYEN

Maîtres-Assistants à l'Université Paris VII

Adina CALVO, Françoise BOSCHET

Assistantes à l'Université Paris VII

EXERCICES D'ALGÈBRE

1er cycle, 1re année et mathématiques supérieures

LIBRAIRIE ARMAND COLIN

103, boulevard Saint-Michel, Paris 5e

AVANT-PROPOS

Cet ouvrage s'adresse aux étudiants de première année de l'enseignement supérieur. Il intéressera les étudiants travaillant seuls et ceux qui sont suivis par des enseignants. En pensant principalement aux utilisateurs isolés, nous nous sommes attachés à donner la solution détaillée de chaque question et à indiquer plusieurs méthodes de résolution chaque fois que cela a été possible. La plupart des exercices proposés sont du même niveau que ceux couramment traités en M. P. 1 et le dernier chapitre se compose de problèmes ou d'extraits de problèmes donnés à l'examen de M. P. 1 ou de M. G. P. à Paris.

Comme tout travail scientifique, l'utilisation d'un pareil recueil d'exercices nécessite la plus grande honnêteté intellectuelle, ainsi il ne doit être fait usage des solutions qu'après une recherche approfondie des problèmes, suivie d'une rédaction minutieuse, afin de comparer les résultats démontrés aux solutions proposées. La plus grande rigueur doit accompagner cette comparaison.

A l'intérieur de chaque chapitre, les exercices sont classés suivant un ordre de difficulté croissant. Les nouvelles notions apparaissent dans le même ordre que dans le livre d'Algèbre de Michel Queysanne paru dans la même collection. D'ailleurs, afin de faciliter le travail des étudiants isolés, nous nous y référons dans les textes des solutions ; par exemple, *cf.* Q, Ch. 3, § II, n° 51, renvoie au numéro 51 du paragraphe II du chapitre 3 de ce livre. De même, toutes les notations employées sont celles qui sont récapitulées dans l'index du même ouvrage.

La résolution des problèmes de synthèse contenus dans le chapitre 9, nécessite une connaissance préalable de l'ensemble du programme. Pour les huit premiers chapitres, nous donnons ci-après une table qui fournit une classification des exercices autour des thèmes principaux de chaque chapitre.

Certains exercices sont extraits de problèmes donnés en M. P., à la Faculté des Sciences de Paris au cours des dernières années. Nous tenons donc à remercier tous nos collègues qui nous ont ainsi aidés. Nous remercions aussi M. M. Michel Queysanne et André Revuz qui nous ont proposé la rédaction de cet ouvrage et nous ont encouragés durant notre travail.

A. CALVO, F. BOSCHET, B. CALVO, J. DOYEN

OUVRAGES DANS LA MÊME SÉRIE

Michel QUEYSANNE : *Algèbre*, 1er cycle et classes préparatoires (ex. MP et Spéciales AA').

Raymond COUTY et Jacques EZRA : *Analyse*, 2 volumes, 1er cycle et classes préparatoires.

F. BOSCHET, A. et B. CALVO, J. DOYEN :

— *Exercices d'Algèbre*, 1er cycle, 1er année et classes préparatoires.

— *Exercices d'Analyse*, 1er cycle, 1re année et classes préparatoires.

— *Exercices d'Algèbre*, 1er cycle, 2e année et classes préparatoires.

— *Exercices d'Analyse*, 1er cycle, 2e année et classes préparatoires.

— *Cours d'Analyse*, DEUG Sciences des structures et de la matière, DEUG Mathématiques appliquées et sciences sociales, classes préparatoires ; 6 volumes :

I. Suites. Séries. Fonctions.
II. Dérivées. Fonctions élémentaires. Intégrales.
III. Développements limités. Courbes. Équations différentielles.
IV. Fonctions de plusieurs variables. Systèmes différentiels.
V. Intégrales multiples. Intégrales curvilignes.
VI. Fonctions de variable complexe.

L. LESIEUR, J. LEFEBVRE, C. JOULAIN, Y. MEYER : *Mathématiques*, 1er cycle, 1re année et mathématiques supérieures ; 2 volumes :

I. Algèbre générale.
II. Algèbre linéaire et Géométrie.

L. LESIEUR, J. LEFEBVRE et R. TEMAM : *Compléments d'Algèbre linéaire*, Mathématiques spéciales, 1er cycle, 2e année.

L. LESIEUR, J. LEFEBVRE : *Mathématiques*, 1er cycle, 1re année et mathématiques supérieures ; analyse.

Pierre BROUSSE : *Cours de Mécanique*, 1er cycle et classes préparatoires.

Michel MANTON : *Exercices et Problèmes de Mécanique*, 1er cycle et classes préparatoires.

Michel ZISMAN : *Topologie algébrique élémentaire* (maîtrise de mathématiques).

A.-M. FRAISSE, G. OPPENHEIM, M. ROY, C. DENICOLA : *Exercices corrigés et notions de probabilité*, 1er cycle et classes préparatoires.

TABLE DES MATIÈRES

1

ENSEMBLES APPLICATIONS RELATIONS ANALYSE COMBINATOIRE LOIS DE COMPOSITION

1.1 1° P, Q, R, S désignant quatre propositions, trouver des propositions équivalentes aux propositions suivantes :

$$(P \text{ ou } Q) \text{ et } (R \text{ ou } S) \qquad (P \text{ et } Q) \text{ ou } (R \text{ et } S).$$

2° x, y étant deux nombres réels, résoudre le système :

$$(S) \begin{cases} (x-1)(y-2) = 0 \\ (x-2)(y-3) = 0. \end{cases}$$

Solution 1° Soit A la proposition (P ou Q) et (R ou S),

$$A \Leftrightarrow [P \text{ et } (R \text{ ou } S)] \text{ ou } [Q \text{ et } (R \text{ ou } S)]$$

or, $[P \text{ et } (R \text{ ou } S)] \Leftrightarrow (P \text{ et } R) \text{ ou } (P \text{ et } S)$, et

$$[Q \text{ et } (R \text{ ou } S)] \Leftrightarrow (Q \text{ et } R) \text{ ou } (Q \text{ et } S).$$

Soit B la proposition (P et R) ou (P et S) ou (Q et R) ou (Q et S) ; nous avons montré que $A \Leftrightarrow B$.

Appliquons le résultat précédent aux propositions $P' = \text{non } P$, $Q' = \text{non } Q$, $R' = \text{non } R$, $S' = \text{non } S$; il vient

$$(P' \text{ ou } Q') \text{ et } (R' \text{ ou } S') \Leftrightarrow (P' \text{ et } R') \text{ ou } (P' \text{ et } S') \text{ ou } (Q' \text{ et } R') \text{ ou } (Q' \text{ et } S'),$$

or

$$(P' \text{ ou } Q') \text{ et } (R' \text{ ou } S') \Leftrightarrow (\text{non } (P \text{ et } Q)) \text{ et } (\text{non } (R \text{ et } S))$$

et

$$\text{non } (P \text{ et } Q) \text{ et } (\text{non } (R \text{ et } S)) \Leftrightarrow \text{non } [(P \text{ et } Q) \text{ ou } (R \text{ et } S)]$$

Si l'on désigne par B' la proposition

$$(P' \text{ et } R') \text{ ou } (P' \text{ et } S') \text{ ou } (Q' \text{ et } R') \text{ ou } (Q' \text{ et } S'),$$

on a

$$B' \Leftrightarrow [(\text{non } (P \text{ ou } R)) \text{ ou } (\text{non } (P \text{ ou } S)) \text{ ou } (\text{non } (Q \text{ ou } R)) \text{ ou } (\text{non } (Q \text{ ou } S))]$$

soit encore $B' \Leftrightarrow \text{non } [(P \text{ ou } R) \text{ et } (P \text{ ou } S) \text{ et } (Q \text{ ou } R) \text{ et } (Q \text{ ou } S)]$, d'où

$$(P \text{ et } Q) \text{ ou } (R \text{ et } S) \Leftrightarrow (P \text{ ou } R) \text{ et } (P \text{ ou } S) \text{ et } (Q \text{ ou } R) \text{ et } (Q \text{ ou } S).$$

2° Le système (S) proposé est équivalent à

$$[(x = 1) \text{ ou } (y = 2)] \quad \text{et} \quad [(x = 2) \text{ ou } (y = 3)].$$

Appliquons le résultat précédent, il vient

$$(S) \Leftrightarrow [(x = 1) \text{ et } (x = 2)] \text{ ou } [(x = 1) \text{ et } (y = 3)] \text{ ou } [(y = 2) \text{ et } (x = 2)] \text{ ou } [(y = 2) \text{ et } (y = 3)].$$

Les propositions $[(x = 1) \text{ et } (x = 2)]$, $[(y = 2) \text{ et } (y = 3)]$ étant toujours fausses, les solutions du système (S) sont donc

$$[(x = 1) \text{ et } (y = 3)] \text{ ou } [(y = 2) \text{ et } (x = 2)].$$

1.2 Soient A, B deux ensembles et f une application de A dans B.
Démontrer que les propositions suivantes sont équivalentes :
a) pour toute partie X de A, $f^{-1}(f(X)) = X$;
b) f est injective.
Même question pour les propositions :
a') pour toute partie Y de B, $f(f^{-1}(Y)) = Y$;
b') f est surjective.

Solution Rappelons que pour toute partie X de A et toute partie Y de B on a

$$X \subset f^{-1}(f(X)) \quad \text{et} \quad f(f^{-1}(Y)) \subset Y$$

(*cf.* Q., Ch. 1, § IV, n° 13).

Nous allons d'abord montrer l'équivalence des propositions (*a*) et (*b*) en démontrant que non (*a*) $\Leftrightarrow$ non (*b*).

Supposons qu'il existe une partie X de A telle que $f^{-1}(f(X)) \neq X$ alors il existe un élément y de $f^{-1}(f(X))$ qui n'appartient pas à X ; or, $[y \in f^{-1}(f(X))] \Leftrightarrow [f(y) \in f(X)]$, donc il existe un élément x de X tel que $f(x) = f(y)$ et comme $y \notin X$, $x \neq y$, par suite f n'est pas injective et non (*a*) $\Rightarrow$ non (*b*).

Réciproquement si l'on suppose f non injective, alors il existe deux éléments x et y de A tels que $x \neq y$ et $f(x) = f(y)$. Soit X la partie de A contenant pour seul élément x, alors $f(X) = \{f(x)\}$ et $\{x, y\} \subset f^{-1}(f(X))$ donc

$$X \neq f^{-1}(f(X)),$$

ce qui prouve que non (*b*) $\Rightarrow$ non (*a*), donc non (*a*) $\Leftrightarrow$ non (*b*).

Nous montrerons maintenant de manière directe que (*a'*) $\Leftrightarrow$ (*b'*). Supposons (*a'*) vraie et appliquons cette proposition à la partie B de B ; il vient $f(f^{-1}(B)) = B$, or $f^{-1}(B) = A$, donc $f(A) = B$. Cette dernière égalité signifie que f est surjective, donc (*a'*) $\Rightarrow$ (*b'*). Supposons (*b'*) vraie ; alors si y est un élément de Y, il existe un élément x de A tel que $y = f(x)$ et $x \in f^{-1}(Y)$ car $f(x) \in Y$; par suite $y \in f(f^{-1}(Y))$ et comme ceci est vrai pour tout $y \in Y$, on a

$$Y \subset f(f^{-1}(Y)),$$

or on a rappelé au début que $f(f^{-1}(Y)) \subset Y$, donc $Y = f(f^{-1}(Y))$

et (*b'*) $\Rightarrow$ (*a'*) d'où (*a'*) $\Leftrightarrow$ (*b'*).

1.3 Soit f une application d'un ensemble A dans un ensemble B. Démontrer l'équivalence des propositions suivantes :

a) pour toutes parties X_1, X_2 de A, on a $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$,

b) f est injective.

Solution Supposons la proposition (*a*) vérifiée. Soient x_1, x_2 deux éléments distincts de A. Appliquons (*a*) aux deux parties suivantes de A : $X_1 = \{x_1\}$ et $X_2 = \{x_2\}$; il vient

$$f(X_1) = \{f(x_1)\}, \qquad f(X_2) = \{f(x_2)\}$$

et

$$\varnothing = f(X_1 \cap X_2) = \{f(x_1)\} \cap \{f(x_2)\}$$

par suite $f(x_1) \neq f(x_2)$. L'application f est donc injective et nous avons montré que $(a) \Rightarrow (b)$.

Pour toutes parties X_1, X_2 de A, nous avons :

$$f(X_1 \cap X_2) \subset f(X_1) \cap f(X_2) \qquad (cf.\ \text{Q., Ch. 1, § IV, n° 13}).$$

Supposons non (a) réalisée, c'est-à-dire supposons qu'il existe deux parties X_1, X_2 de A telles que $f(X_1 \cap X_2) \neq f(X_1) \cap f(X_2)$
alors il existe un élément y de $f(X_1) \cap f(X_2)$ qui n'appartient pas à $f(X_1 \cap X_2)$, or, $(y \in f(X_1) \cap f(X_2)) \Leftrightarrow [(y \in f(X_1)) \text{ et } (y \in f(X_2))]$, et

$$(y \in f(X_1)) \Leftrightarrow (\exists x_1 \in X_1)\ (y = f(x_1)),$$

$$(y \in f(X_2)) \Leftrightarrow (\exists x_2 \in X_2)\ (y = f(x_2)).$$

Nécessairement $x_1 \neq x_2$ car si $x_1 = x_2$ alors $x_1 \in X_1 \cap X_2$, et $y \in f(X_1 \cap X_2)$ ce qui est exclu par hypothèse. L'application f n'est donc pas injective, par suite non $(a) \Rightarrow$ non (b) soit encore $(b) \Rightarrow (a)$, d'où $(a) \Leftrightarrow (b)$.

1.4 A étant une partie fixée d'un ensemble E, on considère les applications f et g de $\mathfrak{P}(E)$ dans lui-même, définies par :

$$f(X) = A \cap X \qquad \text{et} \qquad g(X) = A \cup X \qquad \text{pour tout } X \in \mathfrak{P}(E).$$

Déterminer les décompositions canoniques de ces applications (*cf.* Q., Ch. 1, § V, n° 19). Montrer qu'il existe une bijection de $g(\mathfrak{P}(E))$ sur $\mathfrak{P}(E - A)$.

Solution La relation d'équivalence associée à f est la relation R sur $\mathfrak{P}(E)$ définie par

$$(\forall (X, Y) \in \mathfrak{P}(E) \times \mathfrak{P}(E)) \qquad XRY \Leftrightarrow f(X) = A \cap X = A \cap Y = f(Y).$$

La classe $\widetilde{X}$ d'un élément X de $\mathfrak{P}(E)$, modulo R, est formée de toutes les parties Y de E dont l'intersection avec A est $A \cap X$. On voit facilement que $f(\mathfrak{P}(E)) = \mathfrak{P}(A)$. L'application b de $\mathfrak{P}(E)/R$ dans $\mathfrak{P}(A)$ définie par $b(\widetilde{X}) = f(X)$ est une bijection et on décompose f en $f = i \circ b \circ s$ où s représente la surjection canonique de $\mathfrak{P}(E)$ sur $\mathfrak{P}(E)/R$ et i l'injection canonique de $\mathfrak{P}(A)$ dans $\mathfrak{P}(E)$ (*cf.* Q., Ch. 1, § V, n° 19).

De même, la relation d'équivalence associée à g est la relation S sur $\mathfrak{P}(E)$ définie par

$$(\forall (X, Y) \in \mathfrak{P}(E) \times \mathfrak{P}(E)) \qquad XSY \Leftrightarrow g(X) = A \cup X = A \cup Y = g(Y).$$

La classe $\overline{X}$ d'un élément X de $\mathfrak{P}(E)$, modulo S, est formée de toutes les parties de E dont la réunion avec A est $X \cup A$. $g(\mathfrak{P}(E))$ est l'ensemble des parties de E qui contiennent A. Désignons par s' la surjection canonique

de $\mathfrak{P}(E)$ sur $\mathfrak{P}(E)/S$, par i' l'injection canonique de $g(\mathfrak{P}(E))$ dans $\mathfrak{P}(E)$ et par b' l'application de $\mathfrak{P}(E)/S$ dans $g((\mathfrak{P}E))$ définie par $b'(\dot{X}) = g(X)$ si $X \in \mathfrak{P}(E)$; alors b' est une bijection et g se décompose en $g = i' \circ b' \circ s'$.

Soit j l'application de $g(\mathfrak{P}(E))$ dans $\mathfrak{P}(E - A)$ définie en posant, pour tout élément Z de $g(\mathfrak{P}(E))$, $j(Z) = Z - A$. Cette application est bien définie car si $Z \in g(\mathfrak{P}(E))$, Z contient A donc $Z = (Z - A) \cup A$ et $(Z - A) \cap A = \varnothing$. Soient Z, Z' deux éléments de $g(\mathfrak{P}(E))$ tels que $j(Z) = Z - A = Z' - A = j(Z')$; alors on a $Z = (Z - A) \cup A = (Z' - A) \cup A = Z'$ donc $Z = Z'$ ce qui prouve que j est injective. De plus, j est surjective car pour tout élément Y de $\mathfrak{P}(E - A)$, on a $Y \cup A \in g(\mathfrak{P}(E))$ et $j(Y \cup A) = Y$; j est donc une bijection et par suite l'application $j \circ b'$ est une bijection de $\mathfrak{P}(E)/S$ sur $\mathfrak{P}(E - A)$.

1.5 Soit f une application d'un ensemble A non vide, dans un ensemble B. Montrer que les propositions suivantes sont équivalentes :

a) f est injective,

b) pour tout ensemble C et tout couple (g, h) d'applications de C dans A, on a $[f \circ g = f \circ h \Rightarrow g = h]$.

Même question pour les propositions suivantes :

a') f est surjective,

b') pour tout ensemble D et tout couple (u, v) d'applications de B dans D, on a $[u \circ f = v \circ f \Rightarrow u = v]$.

Solution Supposons (*a*) satisfaite ; si C est un ensemble et g, h des applications de C dans A telles que $f \circ g = f \circ h$, alors pour tout élément c de C on a

$$f(g(c)) = f(h(c))$$

et comme f est injective, $g(c) = h(c)$; il en résulte que $g = h$ donc que (*a*) $\Rightarrow$ (*b*).

Supposons (*b*) vérifiée et soient a', a'' deux éléments de A tels que $f(a') = f(a'')$. Soit C un ensemble formé d'un seul élément c_0. Considérons les applications g et h de C dans A définies par $g(c_0) = a'$, $h(c_0) = a''$; alors on a

$$f(g(c_0)) = f(h(c_0)) \quad \text{donc} \quad f \circ g = f \circ h,$$

par suite $g = h$ donc $a' = g(c_0) = h(c_0) = a''$, ce qui montre que f est injective donc (*b*) $\Rightarrow$ (*a*) d'où (*a*) $\Leftrightarrow$ (*b*).

Supposons (*a'*) satisfaite et soient D un ensemble et u, v des applications de B dans D telles que $u \circ f = v \circ f$. Comme f est surjective, pour tout élément y de B il existe un élément x de A tel que $y = f(x)$ donc

$$u(y) = u(f(x)) = v(f(x)) = v(y),$$

par suite $u = v$ donc $(a') \Rightarrow (b')$. Pour montrer que $(b') \Rightarrow (a')$ nous raisonnerons par l'absurde. Supposons donc (b') satisfaite et f non surjective ; alors il existe un élément b_0 de B qui n'appartient pas à $f(A)$; soient z_0 un élément de $f(A)$ et u, v les applications de B dans lui-même définies comme suit :

$$u = \mathrm{Id}B \quad \text{et} \quad \begin{cases} v(x) = x & \text{si} \quad x \in f(A) \\ v(x) = z_0 & \text{si} \quad x \in B - f(A) \end{cases}$$

alors $u(x_0) = x_0$, $v(x_0) = z_0$ donc $u \neq v$, cependant, pour tout élément x de A, $f(x) \in f(A)$ donc $u(f(x)) = v(f(x)) = f(x)$, par suite $u \circ f = v \circ f$ ce qui contredit notre hypothèse. Par suite $(b') \Rightarrow (a')$ et $(a') \Leftrightarrow (b')$.

1.6 Soient A, B, C, D des ensembles, f une application de A dans B, g une application de B dans C et h une application de C dans D. Montrer que les applications $g \circ f$ et $h \circ g$ sont bijectives si et seulement si f, g et h le sont.

Solution Nous savons (*cf.* Q., Ch. 1, § IV, n° 15) que la composée de deux bijections est une bijection, donc si f, g et h sont bijectives, il en est de même de $g \circ f$ et $h \circ g$.

Réciproquement, supposons que $g \circ f$ et $h \circ g$ soient bijectives. Comme $g \circ f$ est surjective, g est surjective ; en effet, on a $g(f(A)) = C$ et $f(A) \subset B$ donc $C = g(f(A)) \subset g(B) \subset C$ par suite $g(B) = C$. D'autre part, $h \circ g$ étant injective, g est injective ; en effet si b', b'' sont deux éléments de B tels que $g(b') = g(b'')$ on a $h(g(b')) = h(g(b''))$ donc $b' = b''$. L'application g est donc bijective ; soit g^{-1} son application réciproque, alors $g^{-1} \circ g = \mathrm{Id}B$ et $g \circ g^{-1} = \mathrm{Id}C$ donc

$$f = (g^{-1} \circ g) \circ f = g^{-1} \circ (g \circ f) \quad \text{et} \quad h = h \circ (g \circ g^{-1}) = (h \circ g) \circ g^{-1}$$

par suite f et h sont bijectives comme composées de bijections.

1.7 Soient E, F deux ensembles non vides, munis respectivement des relations d'équivalence R et S. On désigne par u l'application canonique de E sur E/R et par v l'application canonique de F sur F/S.

On dit qu'une application f de E dans F est compatible avec R et S si l'application $v \circ f$ est compatible avec R (c'est-à-dire que

$$[x \in E,\ x' \in E \text{ et } x \equiv x' \pmod{R}] \Rightarrow [v(f(x)) = v(f(x'))]$$

Démontrer que dans ce cas :

a) Si x, x' sont deux éléments de E,

$$x \equiv x' \pmod{R} \Rightarrow f(x) \equiv f(x') \pmod{S},$$

b) il existe une application h de E/R dans F/S telle que $v \circ f = h \circ u$. Etudier la réciproque.

Solution *a*) Supposons f compatible avec R et S et soient x, x' deux éléments de E tels que $x \equiv x' \pmod{R}$; comme $v \circ f$ est compatible avec R, on a

$$v(f(x)) = v(f(x')),$$

ce qui signifie que $f(x) \equiv f(x') \pmod{S}$.

b) Nous cherchons à construire une application h de E/R dans F/S rendant commutatif le carré ci-contre :

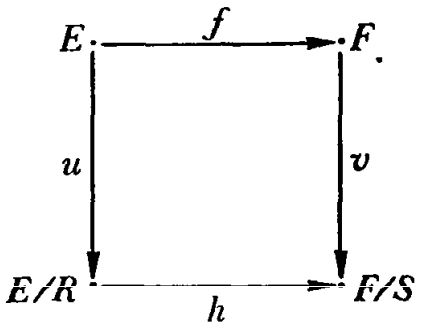


FIG. 1.1

c'est-à-dire telle que $h \circ u = v \circ f$.

Soit X un élément de E/R et x un représentant de X dans E ; alors on a par définition de u, $X = u(x)$. Posons $h(X) = v(f(x))$. Ceci définit bien une application h de E/R dans F/S ; en effet, si x' est un autre représentant de X dans E, on a $x \equiv x' \pmod{R}$ donc d'après (*a*), $v(f(x)) = v(f(x'))$ par suite $v(f(x))$ ne dépend que de X et non du choix de x.

L'application h que nous venons de définir répond bien à la question car on a pour tout élément x de E, $h(u(x)) = v(f(x))$ donc $h \circ u = v \circ f$.

Réciproquement, supposons qu'il existe une application h de E/R dans F/S telle que $h \circ u = v \circ f$; alors si x, x' sont deux éléments de E tels que

$$x \equiv x' \pmod{R}$$

on a par définition de u, $u(x) = u(x')$ donc

$$v \circ f(x) = h \circ u(x) = h \circ u(x') = v \circ f(x')$$

ce qui montre que $v \circ f(x) = v \circ f(x')$ donc que l'application f est compatible avec R et S.

1.8 Soit f une application d'un ensemble E dans lui-même. On désigne par $\mathscr{S}$ la famille des parties S de E telles que $f^{-1}(f(S)) = S$.

a) A étant une partie de E, démontrer que $f^{-1}(f(A))$ est un élément de $\mathscr{S}$.

b) Démontrer que toute intersection et toute réunion d'éléments de $\mathscr{S}$ est un élément de $\mathscr{S}$.

c) S étant un élément de $\mathscr{S}$ et A une partie de E telle que S et A soient disjointes, démontrer que S et $f^{-1}(f(A))$ sont disjointes.

d) S_1 et S_2 étant deux éléments de $\mathscr{S}$ tels que $S_1 \subset S_2$, démontrer que $S_2 - S_1$ est un élément de $\mathscr{S}$.

Solution Remarquons tout d'abord que pour toute partie X de E, on a $X \subset f^{-1}(f(X))$ (*cf.* Q., Ch. 1, § IV, n° 13).

a) Posons $B = f^{-1}(f(A))$. En vertu de la remarque précédente, pour montrer que B est un élément de $\mathscr{S}$, il suffit de montrer que $f^{-1}(f(B)) \subset B$. Soit x un élément de $f^{-1}(f(B))$, alors $f(x) \in f(B)$, il existe donc un élément y de B tel que $f(x) = f(y)$. Comme $y \in B$, $f(y) \in f(A)$ donc $f(x) \in f(A)$ et par suite $x \in f^{-1}(f(A))$; comme ceci est vrai pour tout élément x de $f^{-1}(f(B))$, on voit que $f^{-1}(f(B)) \subset B$ donc B est un élément de la famille $\mathscr{S}$.

b) Rappelons que si $(X_i)_{i \in I}$ est une famille de parties de E, on a

$$f\left(\bigcap_{i \in I} X_i\right) \subset \bigcap_{i \in I} f(X_i) \qquad \text{et} \qquad f^{-1}\left(\bigcap_{i \in I} X_i\right) = \bigcap_{i \in I} f^{-1}(X_i).$$

Soit $(S_i)_{i \in I}$ une famille d'éléments de $\mathscr{S}$; on a

$$f\left(\bigcap_{i \in I} S_i\right) \subset \bigcap_{i \in I} f(S_i)$$

d'où

$$f^{-1}\left(f\left(\bigcap_{i \in I} S_i\right)\right) \subset f^{-1}\left(\bigcap_{i \in I} f(S_i)\right)$$

or,

$$f^{-1}\left(\bigcap_{i \in I} f(S_i)\right) = \bigcap_{i \in I} f^{-1}(f(S_i)) = \bigcap_{i \in I} S_i,$$

par suite

$$f^{-1}\left(f\left(\bigcap_{i \in I} S_i\right)\right) \subset \bigcap_{i \in I} S_i$$

or on sait (remarque ci-dessus) que

$$\bigcap_{i \in I} S_i \subset f^{-1}\left(f\left(\bigcap_{i \in I} S_i\right)\right)$$

donc

$$f^{-1}\left(f\left(\bigcap_{i \in I} S_i\right)\right) = \bigcap_{i \in I} S_i$$

ce qui montre que $\bigcap_{i \in I} S_i$ est un élément de $\mathscr{S}$, donc toute intersection d'éléments de $\mathscr{S}$ est un élément de $\mathscr{S}$.

Rappelons à présent que si $(X_i)_{i \in I}$ est une famille de parties de E, on a

$$f\left(\bigcup_{i \in I} X_i\right) = \bigcup_{i \in I} f(X_i) \qquad \text{et} \qquad f^{-1}\left(\bigcup_{i \in I} X_i\right) = \bigcup_{i \in I} f^{-1}(X_i).$$

Soit $(S_i)_{i \in I}$ une famille d'éléments de $\mathscr{S}$, alors on a

$$f^{-1}\Big(f\Big(\bigcup_{i\in I} S_i\Big)\Big) = f^{-1}\Big(\bigcup_{i\in I} f(S_i)\Big) = \bigcup_{i\in I} f^{-1}\Big(f(S_i)\Big) = \bigcup_{i\in I} S_i ,$$

donc $\bigcup_{i\in I} S_i$ est un élément de $\mathscr{S}$ et toute réunion d'éléments de $\mathscr{S}$ est un élément de $\mathscr{S}$.

c) Nous raisonnerons par l'absurde ; si $S \cap f^{-1}(f(A)) \neq \varnothing$, soit x un élément de $S \cap f^{-1}(f(A))$, alors $f(x) \in f(A)$ donc il existe un élément y de A tel que $f(x) = f(y)$. Comme $x \in S, f(x) \in f(S)$ donc

$$f(y) \in f(S) \qquad \text{et} \qquad y \in f^{-1}(f(S)) ;$$

or, par hypothèse $f^{-1}(f(S)) = S$ donc y appartient à $S \cap A$. Mais nous avions supposé $S \cap A = \varnothing$ donc nécessairement $S \cap f^{-1}(f(A)) = \varnothing$.

d) Comme $S_2 - S_1 \subset S_2$ on a $f^{-1}(f(S_2 - S_1)) \subset f^{-1}(f(S_2)) = S_2$. Appliquant le résultat de *c*) aux parties disjointes $S_2 - S_1$ et S_2, on voit que $S_1 \cap f^{-1}(f(S_2 - S_1)) = \varnothing$ donc $f^{-1}(f(S_2 - S_1)) \subset S_2 - S_1$ et comme $S_2 - S_1 \subset f^{-1}(f(S_2 - S_1))$ (remarque ci-dessus), on a

$$f^{-1}(f(S_2 - S_1)) = S_2 - S_1$$

et $S_2 - S_1$ est un élément de $\mathscr{S}$.

1.9 On désigne par E un ensemble et par $\mathscr{R}$ l'ensemble des relations binaires entre éléments de E. Soient $R \in \mathscr{R}$ et $R' \in \mathscr{R}$; on dit que R est contenue dans R' et on note $R \subset R'$ si :

$$(\forall (x, y) \in E \times E) \quad [xRy \Rightarrow xR'y] .$$

1) Montrer que la relation d'inclusion ($\subset$) est une relation d'ordre dans $\mathscr{R}$.

2) Soit R un élément de $\mathscr{R}$. On désigne par $\bar{R}$ la relation binaire sur E définie par : $(\forall (a, b) \in E \times E)$ $a\bar{R}b$ si et seulement s'il existe un entier $n > 0$ et une suite finie $a_0, a_1, \ldots, a_{2n}$ d'éléments de E, tels que : $a_0 = a$, $a_{2n} = b$, ($a_{2i} R a_{2i+1}$ ou $a_{2i} = a_{2i+1}$) et ($a_{2i+2} R a_{2i+1}$ ou $a_{2i+2} = a_{2i+1}$) si $i = 0, 1, \ldots, n - 1$.

a) Montrer que $\bar{R}$ est une relation d'équivalence et que $R \subset \bar{R}$.

b) Montrer que si R' est une relation d'équivalence telle que $R \subset R'$, alors $\bar{R} \subset R'$.

c) En déduire que R est une relation d'équivalence, si et seulement si $R = \bar{R}$.

Solution 1) *Réflexivité* : $(\forall R \in \mathscr{R})\ (\forall (x, y) \in E \times E)\quad [xRy \Rightarrow xRy]$ donc $R \subset R$.

Antisymétrie : si $R \in \mathscr{R}$, $R' \in \mathscr{R}$, $R \subset R'$ et $R' \subset R$, alors on a :

$$(\forall (x, y) \in E \times E)\quad ([xRy \Rightarrow xR'y] \text{ et } [xR'y \Rightarrow xRy])$$

soit aussi :

$$(\forall (x, y) \in E \times E)\quad [xRy \Leftrightarrow xR'y]$$

donc $R = R'$.

Transitivité : si $R \in \mathscr{R}$, $R' \in \mathscr{R}$, $R'' \in \mathscr{R}$, $R \subset R'$ et $R' \subset R''$, alors :

$$(\forall (x, y) \in E \times E)\quad ([xRy \Rightarrow xR'y] \text{ et } [xR'y \Rightarrow xR''y])$$

donc en vertu de la transitivité de l'implication, on a :

$$(\forall (x, y) \in E \times E)\quad [xRy \Rightarrow xR''y]$$

c'est-à-dire $R \subset R''$.

2) a) *Réflexivité* : si $a \in E$, posons $a_0 = a_1 = a_2 = a$; on a : $a_2 = a_1$ et $a_0 = a_1$, donc $a\bar{R}a$.

Transitivité : soient $a \in E$, $b \in E$, $c \in E$ tels que $a\bar{R}b$ et $b\bar{R}c$; alors il existe deux entiers $n > 0$ et $m > 0$ et deux suites finies $a_0, \ldots, a_{2n}$ et $b_0, \ldots, b_{2m}$ d'éléments de E, tels que : $a_0 = a$, $a_{2n} = b_0 = b$, $b_{2m} = c$,

$$(a_{2i}\,Ra_{2i+1} \text{ ou } a_{2i} = a_{2i+1}) \text{ et } (a_{2i+2}\,Ra_{2i+1} \text{ ou } a_{2i+2} = a_{2i+1})$$

si $0 \leqslant i \leqslant n - 1$,

$$(b_{2j}\,Rb_{2j+1} \text{ ou } b_{2j} = b_{2j+1}) \text{ et } (b_{2j+2}\,Rb_{2j+1} \text{ ou } b_{2j+2} = b_{2j+1})$$

si $0 \leqslant j \leqslant m - 1$. Formons la suite $c_0, \ldots, c_{2(m+n)}$ définie en posant : $c = a_i$ si $0 \leqslant i \leqslant 2n$, et $c_j = b_{j-2n}$ si $2n + 1 \leqslant j \leqslant 2(m + n)$; alors on a :

$$m + n > 0\,,\ c_0 = a\,,\ c_{2(m+n)} = c\,,$$

$$(c_{2i}\,Rc_{2i+1} \text{ ou } c_{2i} = c_{2i+1}) \text{ et } (c_{2i+2}\,Rc_{2i+1} \text{ ou } c_{2i+2} = c_{2i+1})$$

si $0 \leqslant i \leqslant m + n - 1$, donc $a\bar{R}c$, ce qui montre que $\bar{R}$ est transitive.

Symétrie : soient $a \in E$, $b \in E$, tels que $a\bar{R}b$; alors il existe un entier $n > 0$ et une suite finie $a_0, \ldots, a_{2n}$ d'éléments de E tels que : $a_0 = a$, $a_{2n} = b$,

$$(a_{2i}\,Ra_{2i+1} \text{ ou } a_{2i} = a_{2i+1}) \text{ et } (a_{2i+2}\,Ra_{2i+1} \text{ ou } a_{2i+2} = a_{2i+1})$$

si $0 \leqslant i \leqslant n - 1$. Formons la suite $b_0, \ldots, b_{2n}$ définie en posant $b_j = a_{2n-j}$ si $0 \leqslant j \leqslant 2n$, et posons $k = n - i - 1$; on voit alors que si $0 \leqslant i \leqslant n - 1$, on a :

$$a_{2i} = b_{2(n-i)} = b_{2k+2}\,;$$

$$a_{2i+1} = b_{2(n-i)+1} = b_{2k+1} \quad \text{et} \quad a_{2i+2} = b_{2(n-i)-2} = b_{2k}\,;$$

lorsque i parcourt [0, 1, ..., $n-1$], k parcourt aussi [0, 1, ..., $n-1$], on a donc si $0 \leqslant k \leqslant n-1$:

$$(b_{2k+2}\, R b_{2k+1} \text{ ou } b_{2k+2} = b_{2k+1}) \quad \text{et} \quad (b_{2k}\, R b_{2k+1} \text{ ou } b_{2k} = b_{2k+1}),$$

par suite $b\bar{R}a$ et $\bar{R}$ est symétrique. Si $a \in E$, $b \in E$ et aRb, alors en prenant la suite : $a_0 = a$, $a_1 = a_2 = b$, on a $a_0\, R a_1$ et $a_2 = a_1$ donc $a\bar{R}b$, par suite $R \subset \bar{R}$.

b) Soit R' une relation d'équivalence telle que $R \subset R'$ et soient $a \in E$, $b \in E$ deux éléments tels que $a\bar{R}b$; alors il existe un entier $n > 0$ et une suite finie $a_0, \ldots, a_{2n}$ d'éléments de E, telle que : $a_0 = a$, $a_{2n} = b$,

$$(a_{2i}\, R a_{2i+1} \text{ ou } a_{2i} = a_{2i+1}) \quad \text{et} \quad (a_{2i+2}\, R a_{2i+1} \text{ ou } a_{2i+2} = a_{2i+1})$$

si $0 \leqslant i \leqslant n-1$; comme $R \subset R'$, on a alors :

$$(a_{2i}\, R' a_{2i+1} \text{ ou } a_{2i} = a_{2i+1}) \quad \text{et} \quad (a_{2i+2}\, R' a_{2i+1} \text{ ou } a_{2i+2} = a_{2i+1})$$

si $0 \leqslant i \leqslant n-1$, or R' est réflexive donc on a $(a_{2i}\, R' a_{2i+1})$ et $(a_{2i+2}\, R'\, a_{2i+1})$ si $0 \leqslant i \leqslant n-1$; de plus R' est symétrique, donc on a :

$$(a_{2i}\, R'\, a_{2i+1}) \quad \text{et} \quad (a_{2i+1}\, R'\, a_{2i+2})$$

si $0 \leqslant i \leqslant n-1$, par suite on a : $a_i\, R'\, a_{i+1}$ si $0 \leqslant i \leqslant n-1$ et comme R' est transitive, on a : $aR'\, b$ donc $\bar{R} \subset R'$.

c) Si R est une relation d'équivalence, en prenant $R' = R$ dans *b*), il vient : $\bar{R} \subset R$, or $R \subset \bar{R}$ d'après *a*) donc $R = \bar{R}$ (question 1). La réciproque est évidente.

1.10 On dit qu'une relation binaire sur un ensemble E est une relation de préordre si elle est réflexive et transitive ; soit P une telle relation. On considère la relation binaire R sur E définie par

$$(\forall (x, y) \in E \times E) \qquad [R(x, y) \Leftrightarrow (P(x, y) \quad \text{et} \quad P(y, x))]\,.$$

a) Montrer que R est une relation d'équivalence.

b) Montrer que P est compatible avec R (*cf.* Q., Ch. 1, § V, n° 19) ; en déduire que l'on peut définir sur l'ensemble quotient E/R de E par R, une relation binaire $\mathcal{O}$ par :

$$\mathcal{O}(\dot{x}, \dot{y}) \Leftrightarrow P(x, y)$$

($\dot{x}$ et $\dot{y}$ désignant respectivement la classe d'équivalence de x et y modulo R).

Démontrer que $\mathcal{O}$ est une relation d'ordre sur E/R (on l'appelle la *relation d'ordre sur E/R associée à la relation de préordre P*).

c) On considère les cas suivants :

α) $E = \mathbf{R} \times \mathbf{R}$ (où $\mathbf{R}$ désigne l'ensemble des nombres réels), la relation P entre $x = (x_1, x_2)$ et $y = (y_1, y_2)$ étant définie par $P(x, y) \Leftrightarrow x_1 \leqslant y_1$.

β) E est l'ensemble des parties finies de l'ensemble N des nombres entiers. Si $X \in E$, on désigne par $\delta(X)$ la somme des éléments de X. La relation P est définie par :

$$(\forall (X, Y) \in E \times E) \quad [P(X, Y) \Leftrightarrow \delta(X) \leqslant \delta(Y)] .$$

γ) E est l'ensemble des entiers rationnels non nuls. La relation P est définie par

$$(\forall (x, y) \in E \times E) \quad [P(x, y) \Leftrightarrow (x \text{ divise } y)] .$$

Montrer que dans chaque cas P est une relation de préordre sur E et étudier les relations d'ordre associées.

Solution a) *Réflexivité* : comme P est réflexive pour tout élément x de E on a $P(x, x)$ donc $R(x, x)$.

Symétrie : elle résulte immédiatement de la définition.

Transitivité : si x, y, z sont trois éléments de E tels que $R(x, y)$ et $R(y, z)$, on a : $P(x, y)$ et $P(y, x)$ et $P(y, z)$ et $P(z, y)$, or, P est transitive donc on a $P(x, z)$ et $P(z, x)$ soit $R(x, z)$ ce qui montre que R est transitive.

b) Pour montrer que P est compatible avec R, rappelons (*cf.* Q., Ch. 1, § V, n° 19) qu'il faut montrer que :

$$(\forall (x, y, x', y') \in E \times E \times E \times E) \; [(P(x, y) \text{ et } R(x, x') \text{ et } R(y, y')) \Rightarrow P(x', y')]$$

Soient donc x, y, x', y' des éléments de E tels que l'on ait :

$$(P(x, y) \text{ et } R(x, x') \text{ et } R(y, y')) .$$

Par définition de R, $R(x, x') \Rightarrow P(x', x)$ et $R(y, y') \Rightarrow P(y, y')$ donc on a $(P(x', x)$ et $P(x, y)$ et $P(y, y'))$ et comme P est transitive, on a $P(x', y')$, ce qui montre que P est compatible avec R.

La relation binaire $\mathcal{O}$ est bien définie car la démonstration précédente montre que $\mathcal{O}(\dot{x}, \dot{y})$ ne dépend pas du choix des représentants x, y des classes $\dot{x}$, $\dot{y}$. Cette relation est évidemment réflexive et transitive comme la relation P. Montrons qu'elle est antisymétrique. Soient $\dot{x}$, $\dot{y}$ deux éléments de E/R tels que $\mathcal{O}(\dot{x}, \dot{y})$ et $\mathcal{O}(\dot{y}, \dot{x})$, alors, par définition de $\mathcal{O}$, on a $P(x, y)$ et $P(y, x)$ si l'on désigne par x, y des représentants de $\dot{x}$ et $\dot{y}$; on a alors $R(x, y)$ c'est-à-dire que $\dot{x} = \dot{y}$.

La relation $\mathcal{O}$ est donc bien une relation d'ordre sur E/R.

c) α) La définition de la relation binaire P sur E ne fait intervenir que la première coordonnée. Elle est donc réflexive et transitive comme la relation d'ordre $\leqslant$ sur **R**. Elle n'est pas antisymétrique car si $x = (x_1, x_2)$ et $y = (y_1, y_2)$ sont deux éléments de E tels que $P(x, y)$ et $P(y, x)$, on a seulement $x_1 = y_1$. P est donc une relation de préordre. Soit R la relation binaire définie sur E par

$$(\forall (x, y) \in E \times E) \quad [R(x, y) \Leftrightarrow (P(x, y) \text{ et } P(y, x))] .$$

Si $x = (x_1, x_2)$ et $y = (y_1, y_2)$ sont deux éléments de E, on voit que :

$$R(x, y) \Leftrightarrow x_1 = y_1 .$$

Si on représente les points de E au moyen d'un graphe cartésien relatif à deux axes (Ox_1, Ox_2), on voit que la classe d'équivalence modulo R, d'un point $x = (x_1, x_2)$ est formée de tous les points situés sur la droite passant par x qui est parallèle à Ox_2. Un représentant particulier de la classe de x est $(x_1, 0)$.

E/R muni de l'ordre $\mathcal{O}$ est donc isomorphe à $\mathbf{R}$ (comme ensemble ordonné) par l'application qui associe à $\dot{x}$, le nombre réel x_1 tel que, pour tout représentant x de $\dot{x}$, x_1 soit la première coordonnée de x.

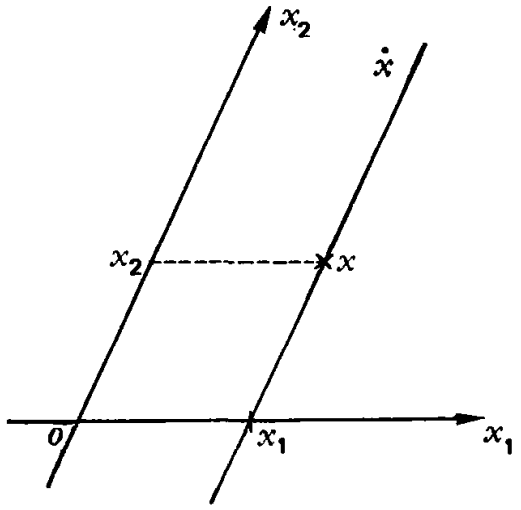


FIG. 1.2

β) Si $X \in E$ on a évidemment $\delta(X) \leqslant \delta(X)$ donc $P(X, X)$. Si X, Y, Z sont des éléments de E tels que l'on ait $P(X, Y)$ et $P(Y, Z)$, on a $\delta(X) \leqslant \delta(Y)$ et $\delta(Y) \leqslant \delta(Z)$, donc $\delta(X) \leqslant \delta(Z)$ par suite on a $P(X, Z)$. Ceci montre que P est une relation de préordre sur E. Soit R la relation binaire sur E définie par

$$(\forall (X, Y) \in E \times E) \quad [R(X, Y) \Leftrightarrow P(X, Y) \text{ et } P(Y, X)]$$

soit encore, compte tenu de la définition de P,

$$(\forall (X, Y) \in E \times E) \quad [R(X, Y) \Leftrightarrow \delta(X) = \delta(Y)] .$$

Observons que si X, Y sont deux éléments de E, $R(X, Y)$ n'implique pas $X = Y$ (exemple : $X = (1, 1, 1)$, $Y = (2, 1)$). On sait a) que R est une relation d'équivalence sur E. A chaque entier $n \in \mathbf{N}$ correspond dans E/R la classe $\dot{X}_n$ formée des parties X de $\mathbf{N}$ telles que $\delta(X) = n$; l'application φ de E/R dans $\mathbf{N}$ qui associe n à $\dot{X}_n$ est un isomorphisme d'ensembles ordonnés de E/R muni de l'ordre $\mathcal{O}$ associé à P, sur $\mathbf{N}$ muni de l'ordre habituel.

γ) On vérifie immédiatement que P est une relation de préordre sur E. Observons que P n'est pas antisymétrique, en effet, si x, y sont deux éléments de E tels que $P(x, y)$ et $P(y, x)$, alors, il existe deux éléments k, h de E tels que $x = ky$ et $y = hx$, donc $x = khx$ ce qui implique, soit $k = h = 1$, soit $k = h = -1$, donc on a soit $x = y$, soit $x = -y$. La relation R définie sur E par

$$(\forall (x, y) \in E \times E) \quad [R(x, y) \Leftrightarrow (P(x, y) \text{ et } P(y, x))]$$

est donc aussi définie par

$$(\forall (x, y) \in E \times E) \quad [R(x, y) \Leftrightarrow |x| = |y|] .$$

Chaque classe d'équivalence de E, modulo R, contient donc deux nombres rationnels non nuls, de même valeur absolue. On peut d'autre part remarquer que la relation P induit une relation d'ordre sur N*.

E/R muni de l'ordre $\mathcal{O}$ associé à P est donc isomorphe (comme ensemble ordonné) à N* muni de l'ordre induit par P, au moyen de l'application qui associe à toute classe X (modulo R) la valeur absolue de l'un quelconque de ses représentants.

1.11 Soit E un ensemble fini de cardinal n. Quel est le cardinal de $\mathfrak{P}(E)$?

Solution *Première méthode* (récurrence).

Si card $E = 0$, $E = \varnothing$, $\mathfrak{P}(E) = \{ \varnothing \}$ donc card $\mathfrak{P}(E) = 1$. Si card E = 1 alors $\mathfrak{P}(E) = \{ \varnothing, E \}$ donc card $\mathfrak{P}(E) = 2$. Supposons que si card $E = n - 1$, alors card $\mathfrak{P}(E) = 2^{n-1}$ et considérons un ensemble E de cardinal n. Soient x un élément de E et F le complémentaire de $\{ x \}$ dans E ; alors on a

$$E = F \cup \{ x \} \qquad \text{et} \qquad F \cap \{ x \} = \varnothing$$

Soit A une partie de E ; si A ne contient pas x, A est une partie de F ; si A contient x, $A - \{ x \}$ est une partie de F ; de plus, si A, A' sont deux parties contenant x telles que $A \neq A'$, alors $A - \{ x \} \neq A' - \{ x \}$. On en déduit que

$$\text{card } \mathfrak{P}(E) = 2.\text{card } \mathfrak{P}(F)$$

or, d'après l'hypothèse de récurrence card $\mathfrak{P}(E) = 2^{n-1}$, donc card $\mathfrak{P}(E) = 2^n$.

Deuxième méthode (fonctions caractéristiques).

Nous allons définir une bijection de $\mathfrak{P}(E)$ dans l'ensemble $\mathcal{F}(E, \{ 0, 1 \})$ des fonctions de E dans $\{ 0, 1 \}$.

A toute partie A de E, associons l'élément f_A de $\mathcal{F}(E, \{ 0, 1 \})$ (appelé la *fonction caractéristique* de A) défini par

$$\begin{cases} f_A(x) = 1 & \text{si} \quad x \in A \\ f_A(x) = 0 & \text{si} \quad x \notin A \,. \end{cases}$$

On voit facilement que la fonction f de $\mathfrak{P}(E)$ dans $\mathcal{F}(E, \{ 0, 1 \})$ définie en posant $f(A) = f_A$ pour tout élément A de $\mathfrak{P}(E)$, est une bijection dont la bijec-

tion réciproque est l'application g de $\mathscr{F}(E, \{0, 1\})$ dans $\mathfrak{P}(E)$ qui associe à tout élément f de $\mathscr{F}(E, \{0, 1\})$ la partie de E formée des éléments x tels que $f(x) = 1$.

On a donc card $\mathfrak{P}(E)$ = card $\mathscr{F}(E, \{0, 1\}) = 2^n$ (*cf.* Q., Ch. 2, § IV, n° 39).

1.12 Soit n un entier naturel ; calculer $\sum_{p=0}^{n} (C_n^p)^2$

Solution Soit E un ensemble ayant $2n$ éléments ; le nombre de parties X de E ayant n éléments est C_{2n}^n.

Soit A un sous-ensemble de E ayant n éléments. X_1 étant une partie fixée de A ayant p éléments ($p \leqslant n$), le nombre de parties X de E ayant n éléments telles que $X \cap A = X_1$ est C_n^{n-p} ; en effet, pour obtenir X on doit compléter X_1 par $n - p$ éléments de $E - A$.

Le nombre de parties de A ayant p éléments étant C_n^p, le nombre de parties X de E ayant n éléments telles que $X \cap A$ ait p éléments est $C_n^p . C_n^{n-p}$. Le nombre de parties X de E ayant n éléments est donc $\sum_{p=0}^{n} C_n^p . C_n^{n-p}$, or nous savons que $C_n^p = C_n^{n-p}$ donc

$$\sum_{p=0}^{n} (C_n^p)^2 = C_{2n}^n .$$

1.13 Démontrer que 1 000 ! est divisible par 2^{994} et n'est pas divisible par 2^{995}. Trouver le plus grand entier n tel que 3^n divise 1 000 !.

Solution Si 2^n divise 1 000 !, 2^n divise le produit de tous les facteurs pairs du produit 1 000 ! c'est-à-dire 2, 4, 6, ..., 1 000. Donc si 2^n divise 1 000 !, 2^n divise $2^{500}.(500\ !)$. De manière générale remarquons que si 2^n divise p !, 2^n divise $2^{Q(p/2)}.(Q(p/2)\ !)$, $Q(p/2)$ désignant le quotient de la division de p par 2 ; en effet, les facteurs pairs de p ! sont 2×1, 2×2, 2×3, ..., $2 \times Q(p/2)$. Appliquons ceci pour chercher le plus grand entier n tel que 2^n divise 1 000 !

$$Q\left(\frac{1\,000}{2}\right) = 500$$

$$Q\left(\frac{500}{2}\right) = 250$$

$$Q\left(\frac{250}{2}\right) = 125$$

$$Q\left(\frac{125}{2}\right) = 62$$

$$Q\left(\frac{62}{2}\right) = 31$$

$$Q\left(\frac{31}{2}\right) = 15$$

$$Q\left(\frac{15}{2}\right) = 7$$

$$Q\left(\frac{7}{2}\right) = 3$$

$$Q\left(\frac{3}{2}\right) = 1\,.$$

On applique 9 fois le résultat précédent. Donc si 2^n divise 1 000 !, 2^n divise $2^{500}.2^{250}.2^{125}.2^{62}.2^{31}.2^{15}.2^7.2^3.2^1.(1\ !)$, le plus grand entier n tel que 2^n divise 1 000 ! est donc,

$$n = 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 994\,.$$

Dans la suite des facteurs composant p !, les nombres divisibles par 3 sont placés de 3 en 3 et sont en nombre $Q(p/3)$, si $Q(p/3)$ désigne le quotient de la division de p par 3. Donc si 3^n divise p !, 3^n divise aussi $3^{Q(p/3)}.(Q(p/3)\ !)$.

Cherchons ainsi le plus grand entier n tel que 3^n divise 1 000!

$$Q\left(\frac{1\,000}{3}\right) = 333$$

$$Q\left(\frac{333}{3}\right) = 111$$

$$Q\left(\frac{111}{3}\right) = 37$$

$$Q\left(\frac{37}{3}\right) = 12$$

$$Q\left(\frac{12}{3}\right) = 4$$

$$Q\left(\frac{4}{3}\right) = 1\,.$$

Donc si 3^n divise 1 000 !, 3^n divise aussi $3^{333}.3^{111}.3^{37}.3^{12}.3^4.3^1.(1\ !)$. Le plus grand entier n tel que 3^n divise 1 000 ! est donc

$$n = 333 + 111 + 37 + 12 + 4 + 1 = 498 .$$

1.14 k, p, n désignant des nombres entiers tels que $0 \leqslant k \leqslant p \leqslant n$, démontrer les égalités suivantes :

a) $$C_n^k\, C_{n-k}^{p-k} = C_p^k\, C_n^p$$

b) $$C_n^0\, C_n^p + C_n^1\, C_{n-1}^{p-1} + \cdots + C_n^p\, C_{n-p}^0 = 2^p\, C_n^p .$$

Solution *a)* E étant un ensemble à n éléments, C_n^k représente le nombre de parties à k éléments de E. Le nombre de parties à p éléments de E contenant une partie à k éléments déterminée est $C_{n-k}^{p-k}.C_n^k$. Or C_{n-k}^{p-k} représente le nombre de façons de compléter une partie à k éléments pour en faire une partie à p éléments. Ce nombre est aussi égal au nombre de façons de choisir une partie à k éléments dans une partie quelconque à p éléments. Le nombre de parties à p éléments de E est C_n^p ; une partie à p éléments étant déterminée, le nombre de parties à k éléments de cette partie est C_p^k ; on en déduit

$$C_n^k.C_{n-k}^{p-k} = C_n^p.C_p^k .$$

b) En appliquant l'égalité précédente p fois on obtient

$$C_n^0\, C_n^p + C_n^1\, C_{n-1}^{p-1} + \cdots + C_n^p\, C_{n-p}^0 = (C_p^0 + C_p^1 + \cdots + C_p^p)\, C_n^p .$$

Or $C_p^0 + C_p^1 + \cdots + C_p^p$ est le nombre de parties d'un ensemble à p éléments, soit 2^p (*cf.* exercice 1.11), donc

$$C_n^0\, C_n^p + C_n^1\, C_{n-1}^{p-1} + \cdots + C_n^p\, C_{n-p}^0 = 2^p.C_n^p .$$

1.15 Soit E un ensemble muni d'une loi de composition associative notée multiplicativement.

a) On suppose qu'il existe un élément a de E tel que la translation à gauche γ_a de E soit surjective et qu'il existe un élément u de E tel que $ua = a$. Démontrer que pour tout élément x de E on a $ux = x$.

b) On suppose qu'il existe un élément a de E tel que les translations à gauche et à droite γ_a et δ_a de E soient surjectives. Démontrer qu'il existe un élément neutre.

c) On suppose que pour tout élément a de E, γ_a et δ_a sont surjectives ; démontrer que tout élément de E est inversible.

Solution *a*) Soit x un élément quelconque de E ; comme la translation à gauche γ_a de E est surjective, il existe un élément y de E tel que $ay = x$ et on a $ux = u(ay)$; or la loi est associative donc $u(ay) = (ua)\,y = ay = x$. Pour tout élément x de E on a donc $ux = x$.

b) δ_a étant surjective, il existe un élément u de E tel que $ua = a$. D'après la question précédente, γ_a étant surjective, u est neutre à gauche pour la loi.

De même, il existe un élément v de E tel que $av = a$ et δ_a est surjective ; on montre comme précédemment que v est neutre à droite pour la loi.

Calculons uv ; comme u est neutre à gauche, $uv = v$; comme v neutre à droite, $uv = u$ donc $u = v$ et la loi admet un élément neutre.

c) γ_a et δ_a sont surjectives pour tout élément a de E. La question précédente nous permet de conclure que la loi admet un élément neutre que l'on notera e. Soit x un élément quelconque de E ; l'application γ_x étant surjective, il existe un élément x' de E tel que $xx' = e$. De même, l'application δ_x étant surjective on obtient un élément x'' de E tel que $x''\,x = e$. Calculons $x''\,xx'$ en utilisant l'associativité de la loi

$$x''\,xx' = (x''\,x)\,x' = ex' = x' \qquad \text{et} \qquad x''\,xx' = x''(xx') = x''\,e = x''$$

donc $x' = x''$ et tout élément de E est inversible.

1.16 Soit E un ensemble fini muni d'une loi associative notée multiplicativement et possédant un élément neutre e. Démontrer que tout élément régulier de E est symétrisable. A l'aide d'un contre-exemple, montrer que ce résultat est faux si E est infini.

Solution Soit a un élément régulier de E. La translation à gauche γ_a de E associée à a est alors injective (*cf.* Q., Ch. 3, § I, n° 47) ; comme l'ensemble E est fini, γ_a est surjective (*cf.* Q., Ch. 2, § II, n° 31) ; il existe donc un élément a_1 tel que $a.a_1 = e$; a étant régulier à droite, on montre de même que la translation à droite δ_a de E associée à a est injective donc surjective. Il existe donc un élément a_2 de E tel que $a_2\,a = e$. Alors a admet un inverse à droite a_1 et un inverse à gauche a_2, or la loi est associative donc $a_1 = (a_2\,a)\,a_1 = a_2(aa_1) = a_2$ donc a est symétrisable ce qui montre que tout élément régulier de E est symétrisable.

Considérons l'ensemble $\mathbf{Z}$ des entiers rationnels muni de la multiplication ; cette loi est associative et admet l'élément neutre + 1. Tous les éléments de $\mathbf{Z}^* = \mathbf{Z} - \{0\}$ sont réguliers et pourtant seuls + 1 et − 1 sont symétrisables.

1.17 Soit E un ensemble muni d'une loi $\top$. On dit qu'un élément a de $(E, \top)$ est idempotent si $a \top a = a$. Une loi $\top$ est dite idempotente si tout élément de $(E, \top)$ est idempotent.

a) Démontrer que si une loi $\top$ associative et commutative est idempotente, la relation binaire R sur E définie par

$$(\forall (x, y) \in E \times E) \quad [R(x, y) \Leftrightarrow x \top y = y]$$

est une relation d'ordre. Démontrer que si x, y sont deux éléments de E, $x \top y$ est la borne supérieure de $\{x, y\}$ dans l'ensemble E ordonné par R.

b) On dit qu'un ensemble ordonné T est un treillis, si et seulement si pour tout couple (x, y) d'éléments de T, $\{x, y\}$ possède une borne inférieure $\inf(x, y)$ est une borne supérieure $\sup(x, y)$ dans T.

Soit T un treillis ; pour tout élément (x, y) de $T \times T$ on pose

$$x \vee y = \sup(x, y) \qquad \text{et} \qquad x \wedge y = \inf(x, y).$$

Démontrer que $\vee$ et $\wedge$ sont des lois de composition de T associatives, commutatives et idempotentes.

c) Etudier les cas particuliers suivants :

α) L'ensemble $\mathfrak{P}(E)$ des parties d'un ensemble E, ordonné par l'inclusion.

β) $\mathbf{N}^*$ ordonné par la relation R définie par

$$(\forall (x, y) \in \mathbf{N}^* \times \mathbf{N}^*) \quad [R(x, y) \Leftrightarrow (x \text{ divise } y)].$$

γ) L'ensemble $\mathscr{R}$ des relations binaires entre éléments d'un ensemble E, ordonné par la relation d'inclusion ($\subset$) (*cf.* exercice 1.9).

Solution *a*) *Réflexivité* : comme la loi $\top$ est idempotente, on a pour tout élément x de E, $x \top x = x$ donc $R(x, x)$ ce qui montre que R est réflexive.

Transitivité : soient x, y, z des éléments de E tels que $R(x, y)$ et $R(y, z)$, alors on a $x \top y = y$ et $y \top z = z$, or la loi $\top$ étant associative on a

$$x \top z = x \top (y \top z) = (x \top y) \top z = y \top z = z$$

donc $R(x, z)$ ce qui montre que R est transitive.

Antisymétrie : si x, y sont deux éléments de E tels que $R(x, y)$ et $R(y, x)$ on a $x \top y = y$ et $y \top x = x$ or la loi $\top$ est commutative donc $x = y$.

Nous venons de montrer que R est une relation d'ordre dans E. A présent soient x, y deux éléments de E ; observons que

$$x \top (x \top y) = (x \top x) \top y = x \top y$$

donc $R(x, x \top y)$ et

$$y \top (x \top y) = y \top (y \top x) = (y \top y) \top x = y \top x = x \top y$$

donc $R(y, x \top y)$ par suite $x \top y$ est un majorant de $\{x, y\}$ pour l'ordre R Soit maintenant m un majorant de $\{x, y\}$ pour R, alors on a $R(x, m)$ et $R(y, m)$ soit $x \top m = m$ et $y \top m = m$, donc $(x \top y) \top m = x \top (y \top m) = x \top m = m$ par suite $R(x \top y, m)$; ceci montre que $x \top y$ est le plus petit des majorants du sous-ensemble $\{x, y\}$ de E c'est-à-dire que $x \top y = \sup(x, y)$.

b) Il est clair que $\vee$ et $\wedge$ sont des applications de $T \times T$ dans T donc des lois de composition de T. Notons $\leqslant$ la relation d'ordre du treillis T et considérons trois éléments x, y, z de T. Posons

$$a = (x \vee y) \vee z \qquad \text{et} \qquad a' = x \vee (y \vee z).$$

Par définition on a : $a \geqslant x \vee y$ et $a \geqslant z$ donc $a \geqslant x$, $a \geqslant y$ et $a \geqslant z$, or $(a \geqslant y$ et $a \geqslant z) \Rightarrow (a \geqslant y \vee z)$, et $(a \geqslant x$ et $a \geqslant y \vee z) \Rightarrow a \geqslant a'$. On montre de la même manière que $a' \geqslant a$ donc $a = a'$ et la loi $\vee$ est associative. On fait une démonstration analogue pour montrer l'associativité de la loi $\wedge$.

Les définitions de la borne supérieure et de la borne inférieure de l'ensemble (x, y) ne font pas intervenir l'ordre dans lequel on donne x et y ; les lois $\vee$ et $\wedge$ sont donc commutatives. Pour tout élément x de T, x est bien le plus petit des majorants et le plus grand des minorants de l'ensemble $\{x\}$, car $x \leqslant x$ (réflexivité de la relation d'ordre) : on a donc $x \vee x = x$ et $x \wedge x = x$ ce qui montre que les lois $\vee$ et $\wedge$ sont idempotentes.

c) α) $\mathfrak{P}(E)$ est un treillis ; en effet, pour tout couple (A, B) d'éléments de $\mathfrak{P}(E)$ on a $\sup(A, B) = A \cup B$ et $\inf(A, B) = A \cap B$, car $A \cup B \supset A$, $A \cup B \supset B$ et pour toute partie C de E contenant A et B, $C \supset A \cup B$; de même $A \cap B \subset A$, $A \cap B \subset B$ et toute partie D contenue dans A et B est contenue dans $A \cap B$. Par ailleurs, il est bien connu que les lois $\cap$ et $\cup$ sont associatives, commutatives et idempotentes.

β) $\mathbf{N}^*$ ordonné par la relation R est un treillis ; pour tout couple (x, y) d'entiers strictement positifs, $\sup(x, y)$ est le plus petit commun multiple de x et y, $\inf(x, y)$ est le plus grand commun diviseur de x et y. En effet, soit M le p. p. c. m. de x et y, x divise M et y divise M et M divise tout multiple commun à x et y ; de même, si m est le p. g. c. d. de x et y, m divise x, m divise y et tout diviseur commun à x et y divise m.

Les résultats d'arithmétique élémentaire montrent que les opérations $\vee$ et $\wedge$ associées à ce treillis sont associatives, commutatives et idempotentes.

γ) $\mathscr{R}$ muni de la relation d'inclusion $(\subset)$ est aussi un treillis. En effet, on montre facilement que si R, R' sont deux éléments de $\mathscr{R}$, $\sup(R, R')$ est la relation (R ou R') et $\inf(R, R')$ est la relation (R et R'). Les opérations $\vee$ et $\wedge$ sont aussi de manière évidente associatives, commutatives et idempotentes. L'exemple γ se ramène d'ailleurs à l'exemple α si l'on fait la remarque suivante : si l'on désigne par $\Gamma(R)$ le graphe d'une relation binaire R sur E, alors si $R \in \mathscr{R}$ et $R' \in \mathscr{R}$,

$$[R \subset R' \Leftrightarrow \Gamma(R) \subset \Gamma(R')].$$

Le graphe de la relation (R ou R') est $\Gamma(R) \cup \Gamma(R')$ et celui de la relation (R et R') est $\Gamma(R) \cap \Gamma(R')$.

1.18 Soit E un ensemble sur lequel on a défini deux lois de composition, l'une notée multiplicativement et l'autre notée $*$. On suppose que chaque loi possède un élément neutre ; on appelle e l'élément neutre de la première loi et f celui de la seconde. On suppose de plus que pour tous éléments x, y, u, v de E on a

$$(x * y)(u * v) = (xu) * (yv). \qquad \text{(I)}$$

Montrer que :

a) $e = f$.

b) $(\forall (x, y) \in E \times E) \quad [xy = x * y]$.

c) Les deux lois données sont associatives et commutatives.

Solution *a*) Appliquons l'égalité (I) pour $x = v = f$ et $y = u = e$; il vient

$$(f * e)(e * f) = (fe) * (ef).$$

f est neutre pour la seconde loi donc $f * e = e * f = e$ et $f * f = f$; e est neutre pour la première loi donc $fe = ef = f$ et $ee = e$; (I) s'écrit alors $e.e = f * f$ soit $e = f$.

b) Appliquons l'égalité (I) pour $y = u = e$; il vient

$$(x * e)(e * v) = (xe) * (ev).$$

D'après *a*), e est neutre pour les deux lois donc

$$x * e = xe = x \qquad \text{et} \qquad e * v = ev = v,$$

donc pour tout élément (x, v) de $E \times E$, $xv = x * v$. La loi $*$ est donc la même que la loi notée multiplicativement.

c) Notons la loi multiplicativement ; l'égalité (I) s'écrit :

$$(xy)(uv) = (xu)(yv)$$

Appliquons cette égalité pour $x = v = e$; on obtient : $yu = uy$ pour tout couple (y, u) d'éléments de E, la loi est donc commutative.

Appliquons maintenant l'égalité ci-dessus pour $u = e$; on obtient :

$$(xy)\, v = x(yv)$$

pour tout triplet (x, y, v) d'éléments de E, la loi est donc associative.

2

GROUPES

2.1 Soient G un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes de G.

a) Montrer que $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

b) On suppose que pour tout élément i de I et tout élément j de I, il existe un élément k de I tel que $H_i \subset H_k$ et $H_j \subset H_k$. Montrer que $\bigcup_{i \in I} H_i$ est un sous-groupe de G.

Solution *a*) Comme l'élément neutre e de G appartient à tous les sous-groupes de G, il appartient à $\bigcap_{i \in I} H_i$; il suffira donc de montrer que si x et y sont deux éléments de $\bigcap_{i \in I} H_i$, il en est de même de xy^{-1} (*cf.* Q., Ch. 4, § II, n° 72). Or chaque H_i $(i \in I)$ est un sous-groupe de G donc contient en même temps que x et y le produit xy^{-1} par suite $xy^{-1} \in \bigcap_{i \in I} H_i$.

b) Comme en *a*) on voit que $e \in \bigcup_{i \in I} H_i$ et il suffit de démontrer que si x et y sont deux éléments de $\bigcup_{i \in I} H_i$, il en est de même de xy^{-1}. Soient donc x et y deux éléments de $\bigcup_{i \in I} H_i$; il existe des éléments i et j de I tels que $x \in H_i$ et $y \in H_j$. D'après l'hypothèse, il existe alors un élément k de I tel que $H_i \subset H_k$ et $H_j \subset H_k$ donc x et y appartiennent à H_k qui est un sous-groupe de G, par suite $xy^{-1} \in H_k$ donc $xy^{-1} \in \bigcup_{i \in I} H_i$.

2.2 Démontrer que le centre d'un groupe G est un sous-groupe de G.

Solution Désignons par C le centre de G. Il suffira de démontrer que si x et y sont deux éléments de C il en est de même de xy et x^{-1} (*cf.* Q., Ch. 4, § II, n° 72). Soient donc x et y deux éléments de C ; alors on a quel que soit z dans G : $(xy)\,z = x(yz) = x(zy) = (xz)\,y = (zx)\,y = z(xy)$ donc $xy \in C$; d'autre part on a pour tout z de G, $xz = zx$ donc $z = x^{-1}zx$ et $zx^{-1} = x^{-1}z$, par suite $x^{-1} \in C$, d'où le résultat.

2.3 Soit G un groupe non commutatif de centre C. On désigne par Aut G l'ensemble de tous les automorphismes de G et par Int G l'ensemble $(f_a)_{a \in G}$ de tous les automorphismes intérieurs de G (f_a est défini en posant, pour tout élément x de G, $f_a(x) = axa^{-1}$).

a) Montrer que Aut G est un groupe pour la composition des applications et que Int G en est un sous-groupe.

b) Démontrer que l'application φ de G dans Int G, définie en posant pour chaque élément a de G, $\varphi(a) = f_a$ est un homomorphisme de G sur Int G.

c) Démontrer que Int G est isomorphe à G/C.

Solution *a*) On sait que le composé de deux automorphismes est un automorphisme et que la composition des applications est associative donc induit une loi de composition interne associative sur Aut G. L'application identique I de G est un automorphisme et pour tout élément f de Aut G, on a

$$f \circ I = I \circ f = f \qquad \text{et} \qquad f \circ f^{-1} = f^{-1} \circ f = I,$$

donc I est élément neutre de Aut G et tout élément de Aut G est inversible, ce qui prouve que Aut G est un groupe.

Observons maintenant que si a et b sont deux éléments de G, on a pour tout élément x de G, $f_a \circ f_b(x) = a(bxb^{-1})\,a^{-1} = abx(ab)^{-1} = f_{ab}(x)$ donc $f_a \circ f_b = f_{ab}$ ce qui montre que Int G est une partie stable de Aut G ; d'autre part, si e est l'élément neutre de G, on a pour tout x dans G, $f_e(x) = exe^{-1} = x$ donc $f_e = I$ et $I \in$ Int G ; de plus, si a est un élément de G et a^{-1} son inverse, on a

$$f_a \circ f_{a^{-1}} = f_{aa^{-1}} = f_e = I \qquad \text{et} \qquad f_{a^{-1}} \circ f_a = f_{a^{-1}.a} = f_e = I$$

donc $f_{a^{-1}} = f_a^{-1}$ et tout élément de Int G a son inverse dans Int G, par suite (*cf.* Q., Ch. 4, § II, n° 72) Int G est un sous-groupe de Aut G.

b) L'application φ est surjective par définition de Int G, de plus si a et b sont deux éléments de G on a $\varphi(a) \circ \varphi(b) = f_a \circ f_b = f_{ab} = \varphi(ab)$ donc (*cf.* Q., Ch. 4, § III, n° 77) φ est un homomorphisme surjectif de G sur Int G.

c) Le noyau de φ est l'ensemble des éléments a de G tels que $\varphi(a) = f_a = I$. Cette condition exprime que pour tout élément x de G, on a $f_a(x) = axa^{-1} = x$ soit $ax = xa$, autrement dit, que a est un élément central de G, par suite Ker $\varphi = C$. La décomposition canonique de φ (*cf.* Q., Ch. 4, § III, n° 78) se réduit donc à

$$G \xrightarrow{p} G/C \xrightarrow{s} \varphi(G) = \text{Int } G\,,$$

où p est l'homomorphisme canonique de G sur G/C et s un isomorphisme de G/C sur $\varphi(G) = \text{Int } G$, d'où le résultat.

2.4 Soit G un groupe. Montrer que la relation binaire R définie sur G par « xRx' si et seulement s'il existe un élément a de G tel que $x' = axa^{-1}$ » est une relation d'équivalence. Si x et x' sont congrus modulo R on dit qu'ils sont *conjugués* dans G. Montrer que si a est un élément de G et H un sous-groupe de G, $H' = aHa^{-1}$ est aussi un sous-groupe de G (on dit alors que H et H' sont des *sous-groupes conjugués* dans G).

Solution *Réflexivité* : si $x \in G$ et si e est l'élément neutre de G, on a $x = exe^{-1}$ donc xRx.

Symétrie : si $x \in G$, $x' \in G$ et xRx', il existe un élément a de G tel que $x' = axa^{-1}$ donc on a $x = a^{-1} x' a = (a^{-1}) x'(a^{-1})^{-1}$ et $x'Rx$.

Transitivité : si $x \in G$, $x' \in G$, $x'' \in G$, xRx' et $x'Rx''$, il existe deux éléments a et b de G tels que $x' = axa^{-1}$ et $x'' = bx' b^{-1}$, donc

$$x'' = baxa^{-1} b^{-1} = (ba)\, x(ba)^{-1} \qquad \text{et} \qquad xRx''\,.$$

Ceci montre que R est une relation d'équivalence.

Si $a \in G$, si H est un sous-groupe de G et $H' = aHa^{-1}$, alors $e \in H$ et $e = aea^{-1}$ donc $e \in H'$. Soient donc deux éléments x et y de H', alors il existe deux éléments h et g de H tels que :

$$x = aha^{-1} \qquad \text{et} \qquad y = aga^{-1}\,,$$

donc

$$xy^{-1} = (aha^{-1})(aga^{-1})^{-1} = (aha^{-1})(ag^{-1} a^{-1}) = ahg^{-1} a^{-1}\,,$$

or H est un sous-groupe de G donc (*cf.* Q., Ch. 4, § II, n° 72) $hg^{-1} \in H$, par suite $xy^{-1} \in H'$ donc (*loc. cit.*) H' est un sous-groupe de G.

2.5 A et B étant deux sous-groupes d'un groupe G, soit S le sous-groupe de G engendré par $A \cup B$.

a) Montrer que S est l'ensemble des éléments de G de la forme $x_1 . x_2 \ldots . x_{2n+1}$ où $n \in \mathbf{N}$, $(x_{2i})_{1 \leqslant i \leqslant n}$ sont des éléments de A et $(x_{2i+1})_{0 \leqslant i \leqslant n}$ des éléments de B.

b) Montrer que $S = A.B$ si et seulement si $A.B = B.A$.

Solution *a*) Soit S' l'ensemble des éléments de G de la forme $x_1 . x_2 \ldots . x_{2n+1}$ ($n \in \mathbf{N}$) tels que $x_{2i} \in A$ si $1 \leqslant i \leqslant n$ et $x_{2i+1} \in B$ si $0 \leqslant i \leqslant n$; alors $B \subset S'$ (prendre $n = 0$) et comme l'élément neutre e de G appartient à B, chaque élément a de A se met sous la forme $a = e.a.e$ ($e \in B$, $a \in A$) donc appartient à S', par suite $A \subset S'$ et $A \cup B \subset S'$. A présent je dis que S' est un sous-groupe de G ; en effet, $S' \neq \varnothing$ car $A \cup B \subset S'$ et A et B sont des sous-groupes de G, de plus si $x = x_1 . x_2 \ldots . x_{2n+1}$ et $y = y_1 . y_2 \ldots . y_{2p+1}$ sont deux éléments de S', alors on a

$$\begin{aligned} xy^{-1} &= (x_1 . x_2 \ldots . x_{2n+1})\,(y_1 . y_2 \ldots . y_{2p+1})^{-1} \\ &= (x_1 . x_2 \ldots . x_{2n+1})\,(y_{2p+1}^{-1}\, y_{2p}^{-1} \ldots . y_1^{-1}) \\ &= (x_1 \ldots . x_{2n})\,(x_{2n+1}\, y_{2p+1}^{-1})\,(y_{2p}^{-1} \ldots . y_1^{-1}) \end{aligned}$$

or $x_{2n+1} \in B$, $y_{2p+1} \in B$ et B est un sous-groupe de G, donc (*cf.* Q., Ch. 4, § II, n° 72) $x_{2n+1}\, y_{2p+1}^{-1} \in B$ de plus comme A et B sont des sous-groupes de G, on a $y_{2i}^{-1} \in A$ pour $1 \leqslant i \leqslant n$ et $y_{2i+1}^{-1} \in B$ pour $0 \leqslant i \leqslant n$, donc en posant $z_j = x_j$ si $1 \leqslant j \leqslant 2n$, $z_{2n+1} = x_{2n+1}\, y_{2p+1}^{-1}$, et lorsque $p > 0$, $z_{2n+k} = y_{2p+2-k}^{-1}$ si $2 \leqslant k \leqslant 2p + 1$, on a $xy^{-1} = z_1 . z_2 \ldots . z_{2(p+n)+1}$ avec $z_{2j} \in A$ si $1 \leqslant j \leqslant p + n$ et $z_{2j+1} \in B$ si $0 \leqslant j \leqslant n + p$, par suite $xy^{-1} \in S'$, donc (*cf.* Q., Ch. 4, § II, n° 71) S' est un sous-groupe de G.

Soit maintenant S'' un sous-groupe de G contenant $A \cup B$, alors S'' contient tous les éléments de A, tous ceux de B donc aussi tous les composés de tels éléments, donc $S' \subset S''$; il en résulte que S' est le plus petit sous-groupe de G qui contienne $A \cup B$ c'est-à-dire (*cf.* Q., Ch. 4, § II, n° 73) que $S' = S$.

b) Supposons que $S = A.B$ et soit $b.a$ un élément de $B.A$ ($a \in A$, $b \in B$) alors $b.a = (a^{-1}\, b^{-1})^{-1}$ ($a^{-1} \in A$, $b^{-1} \in B$) et $A.B$ est un sous-groupe de G donc $b.a \in A.B$ par suite $B.A \subset A.B$. Soit maintenant $a_1 . b_1$ un élément de $A.B$ ($a_1 \in A$, $b_1 \in B$) alors, comme $A.B$ est un sous-groupe de G, $a_1 . b_1$ est l'inverse d'un élément de $A.B$ soit $a_2 . b_2$ ($a_2 \in A$, $b_2 \in B$) donc

$$a_1 . b_1 = (a_2 . b_2)^{-1} = b_2^{-1} . a_2^{-1},$$

or $a_2^{-1} \in A$, $b_2^{-1} \in B$ donc $a_1 . b_1 \in B.A$ et $A.B \subset B.A$, si bien que $A.B = B.A$.

Réciproquement supposons que $A.B = B.A$; alors je dis que $A.B$ est un sous-groupe de G ; en effet, $e \in A.B$ et si $a_1 . b_1$ et $a_2 . b_2$ sont deux éléments de $A.B$ ($a_1 \in A$, $a_2 \in A$, $b_1 \in B$, $b_2 \in B$) on a $(a_1 . b_1)\,(a_2 . b_2)^{-1} = a_1\, b_1\, b_2^{-1}\, a_2^{-1}$,

or $b_1 b_2^{-1} a_2^{-1} \in B.A$ et $B.A = A.B$, donc il existe un élément a_3 de A et un élément b_3 de B tels que $b_1 b_2^{-1} a_2^{-1} = a_3.b_3$, alors $(a_1 b_1)(a_2 b_2)^{-1} = (a_1 a_3) b_3$ et $(a_1 a_3) b_3 \in A.B$ donc (*cf.* Q., Ch. 4, § II, n° 72) $A.B$ est un sous-groupe de G, de plus $A \cup B \subset A.B$ et si S' est un sous-groupe de G qui contient $A \cup B$, il contient tous les composés d'un élément de A et d'un élément de B donc contient $A.B$, par suite (*cf.* Q., Ch. 4, § II, n° 73) $S = A.B$.

2.6 Trouver tous les groupes d'ordre 4. On montrera qu'ils sont tous commutatifs.

Solution Soit G un groupe d'ordre 4 noté multiplicativement ; désignons par e, a_1, a_2, a_3 ses éléments, e étant l'élément neutre. On sait (*cf.* Q., Ch. 4, § V, n° 83) que l'ordre de a_1, a_2 ou a_3 divise 4 et n'est pas égal à 1 (le seul élément d'ordre 1 d'un groupe est l'élément neutre) ; deux cas peuvent donc se produire :

(i) *l'un des éléments* a_1, a_2, a_3 *est d'ordre* 4 ; supposons par exemple que ce soit a_1, alors a_1 engendre G donc G est cyclique et isomorphe au groupe additif $\mathbf{Z}/4\,\mathbf{Z}$ (*cf.* Q., Ch. 4, § V, n° 83).

(ii) *les trois éléments* a_1, a_2, a_3 *sont d'ordre* 2 ; alors $a_1^2 = a_2^2 = a_3^2 = e$ et sachant que la table de multiplication de G est un carré latin (*cf.* Q., Ch. 4, § I, n° 71) on voit que la seule table possible pour G est

	e	a_1	a_2	a_3
e	e	a_1	a_2	a_3
a_1	a_1	e	a_3	a_2
a_2	a_2	a_3	e	a_1
a_3	a_3	a_2	a_1	e

Le lecteur vérifiera que cette table définit bien une loi associative et que le groupe G est alors commutatif ; de plus si l'on désigne par $\bar{0}$ et $\bar{1}$ les éléments du groupe additif $\mathbf{Z}/2\,\mathbf{Z}$, en posant

$$\varphi(e) = (\bar{0}, \bar{0}), \quad \varphi(a_1) = (\bar{0}, \bar{1}), \quad \varphi(a_2) = (\bar{1}, \bar{0}), \quad \varphi(a_3) = (\bar{1}, \bar{1})$$

on définit une application bijective φ de G sur l'ensemble produit $\mathbf{Z}/2\,\mathbf{Z} \times \mathbf{Z}/2\,\mathbf{Z}$. Le lecteur vérifiera que φ est un homomorphisme de G sur le groupe additif produit $\mathbf{Z}/2\,\mathbf{Z} \times \mathbf{Z}/2\,\mathbf{Z}$ (*cf.* Q., Ch. 4, § IV, n° 79) donc un isomorphisme.

En résumé nous venons de démontrer que les groupes d'ordre 4 sont tous commutatifs et qu'ils sont de deux types :

— soit cycliques d'ordre 4, donc isomorphes au groupe additif $\mathbf{Z}/4\,\mathbf{Z}$,

— soit isomorphes au groupe additif produit $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ nommé *groupe de Klein.*

2.7 Soit G un groupe fini d'ordre $2\,n$ et d'élément neutre e. On suppose qu'il existe deux sous-groupes d'ordre n, H_1 et H_2 tels que $H_1 \cap H_2 = \{ e \}$. Montrer que $n = 2$, que la structure de G est entièrement déterminée et donner sa table. Combien G possède-t-il de sous-groupes d'ordre 2 ?

Solution Observons d'abord que $n \geqslant 2$ sinon $H_1 = H_2$; d'autre part $H_1 \cup H_2$ a $2\,n - 1$ éléments donc $G = H_1 \cup H_2 \cup \{ a_3 \}$ où $a_3 \in G$, $a_3 \notin H_1$, $a_3 \notin H_2$ et $a_3^{-1} = a_3$ (si on avait $a_3^{-1} \in H_i$ $(i = 1, 2)$ on aurait $a_3 \in H_i$, ce qui n'est pas). Supposons $n > 2$, alors il existe des éléments $a_1 \in H_1$, $a_1' \in H_1$, $a_2 \in H_2$ tels que $a_1 \neq e$, $a_1' \neq e$, $a_1' \neq a_1$, $a_2 \neq e$, mais alors on a $a_1 . a_2 = a_3$ car si on avait $a_1\, a_2 \in H_1$ on aurait $a_2 \in H_1$ et si on avait $a_1 . a_2 \in H_2$ on aurait $a_1 \in H_2$ ce qui n'est pas ; de même on voit que $a_1' . a_2 = a_3$ par suite $a_1 . a_2 = a_1' . a_2$ donc $a_1 = a_1'$ ce qui est contradictoire, donc $n = 2$.

Désignons par a_i l'élément de H_i $(i = 1, 2)$ qui n'est pas l'élément neutre ; alors $G = \{ e, a_1, a_2, a_3 \}$ et on a $a_1^2 = a_2^2 = a_3^2 = e$, par suite G est un groupe d'ordre 4 dont trois éléments sont d'ordre 2, et on sait (*cf.* corrigé de l'exercice 2.6) que dans ces conditions G est un groupe abélien isomorphe au groupe additif produit $\mathbf{Z}/2\,\mathbf{Z} \times \mathbf{Z}/2\,\mathbf{Z}$ et que sa table de multiplication est

	e	a_1	a_2	a_3
e	e	a_1	a_2	a_3
a_1	a_1	e	a_3	a_2
a_2	a_2	a_3	e	a_1
a_3	a_3	a_2	a_1	e

Il en résulte que les sous-groupes d'ordre 2 de G sont H_1, H_2 et $H_3 = \{ e, a_3 \}$.

2.8 Soient G un groupe cyclique, fini d'ordre n, noté multiplicativement, a un générateur de G et $e = a^n$ l'élément neutre de G.

1) Montrer que tout sous-groupe de G est cyclique.

2) Soit m un entier strictement positif, montrer que $a^m = e$ si et seulement si n divise m.

3) Soit $H = \langle a^p \rangle$ le sous-groupe de G engendré par a^p $(1 \leqslant p \leqslant n)$.

a) Montrer que H coïncide avec le sous-groupe $\langle a^q \rangle$ de G engendré par a^q où q est le p. g. c. d. de n et p.

b) En déduire que $H = G$ si et seulement si n et p sont premiers entre eux.

Solution 1) Soit G_0 un sous-groupe de G ; désignons par n_0 le plus petit entier strictement positif tel que $a^{n_0} \in G_0$, alors le sous-groupe $\langle a^{n_0} \rangle$ engendré par a^{n_0} est contenu dans G_0 et si $x \in G_0$, il existe un entier m tel que $x = a^m$ et $m \geqslant n_0$ donc en faisant la division euclidienne de m par n_0 on obtient $m = n_0.q + r$ avec soit $r = 0$, soit $0 < r < n_0$; alors on a $a^m = a^{n_0 q + r} = a^{n_0 q}.a = (a^{n_0})^q.a^r$ et $a^m \in G_0$, $(a^{n_0})^q \in G_0$ donc $a^r \in G_0$ et on ne peut avoir $0 < r < n_0$ par définition de n_0, donc $r = 0$, $m = n_0 q$ et $x \in \langle a^{n_0} \rangle$; comme ceci est vrai pour tout élément x de G_0, $G_0 \subset \langle a^{n_0} \rangle$ donc $G = \langle a^{n_0} \rangle$ ce qui montre que G_0 est cyclique.

2) Si n divise m il existe un entier q tel que $m = nq$ donc

$$a^m = a^{nq} = (a^n)^q = e^q = e$$

puisque a est d'ordre n. Réciproquement, si $a^m = e$, on a $m \geqslant n$ sinon a n'engendrerait pas G ; faisons la division euclidienne de m par n, on obtient $m = nq + r$, avec soit $r = 0$, soit $0 < r < n$, alors

$$a^m = a^{nq+r} = a^{nq}.a^r = (a^n)^q.a^r = a^r = e$$

or ceci est impossible si $0 < r < n$ car a est d'ordre n, donc $r = 0$, et $m = n.q$ d'où le résultat.

3) *a*) Si q est le p. g. c. d. de n et p, il existe un entier q' tel que $p = q.q'$, donc $a^p = (a^q)^{q'}$ et $a^p \in \langle a^q \rangle$ par suite $H \subset \langle a^q \rangle$. D'autre part, d'après le théorème de BEZOUT (*cf.* Q., Ch. 5, § III, n° 99, th. 4) il existe deux entiers r et s tels que $q = p.r + n.s$ donc $a^q = a^{pr+ns} = a^{pr}.a^{ns} = (a^p)^r.(a^n)^s = (a^p)^r$ puisque $a^n = e$, donc $a^q \in H$ et par suite $\langle a^q \rangle \subset H$ donc $H = \langle a^q \rangle$.

b) D'après *a*), $H = \langle a^q \rangle$ où q est le p. g. c. d. de n et p, donc si p et n sont premiers entre eux, $q = 1$ et $H = G$; si p et n ne sont pas premiers entre eux, $q > 1$ et $H \neq G$ d'où le résultat.

2.9

Soient G_1 et G_2 deux groupes, a_1 un élément d'ordre n_1 de G_1 et a_2 un élément d'ordre n_2 de G_2.

a) Montrer que l'ordre de l'élément (a_1, a_2) du groupe produit $G_1 \times G_2$ est le p. p. c. m. des ordres de a_1 et a_2.

b) En déduire que si G_1 est cyclique d'ordre n_1, G_2 cyclique d'ordre n_2 et si n_1 et n_2 sont premiers entre eux, alors $G_1 \times G_2$ est cyclique d'ordre $n_1.n_2$.

Solution *a*) Désignons par e_1 l'élément neutre de G_1 et par e_2 celui de G_2. Si q est un entier, on a $(a_1, a_2)^q = (e_1, e_2)$ si et seulement si $a_1^q = e_1$ et $a_2^q = e_2$, donc (*cf.* exercice 2.8) si et seulement si q est un multiple commun de n_1 et n_2, par suite l'ordre de (a_1, a_2) dans $G_1 \times G_2$ est le p. p. c. m. des ordres de a_1 et a_2.

b) Si n_1 et n_2 sont premiers entre eux, si l'on désigne par a_1 un générateur de G_1 et par a_2 un générateur de G_2, alors d'après la première partie, l'ordre de l'élément (a_1, a_2) dans $G_1 \times G_2$ est $n_1.n_2$; comme $G_1 \times G_2$ a $n_1.n_2$ éléments, (a_1, a_2) engendre $G_1 \times G_2$, d'où le résultat.

2.10

Un groupe *abélien* G est dit *simple* s'il n'est pas réduit à son élément neutre 0 et s'il ne possède aucun sous-groupe différent de $\{ 0 \}$ et de G. Montrer que les conditions suivantes sont équivalentes :

(*i*) G est un groupe cyclique d'ordre premier ;

(*ii*) G est un groupe abélien simple.

Solution (i) $\Rightarrow$ (ii). Soit G un groupe cyclique d'ordre premier p ; comme G est cyclique, il est abélien (*cf.* Q., Ch. 4, § V, n° 83) ; comme l'ordre de G est premier, G n'est pas réduit à son élément neutre. Si H est un sous-groupe de G, l'ordre de H divise p (*cf.* Q., Ch. 4, § II, n° 74) donc est égal à 1 ou à p ; dans le premier cas $H = \{ 0 \}$ et dans le second $H = G$, donc G est simple.

(ii) $\Rightarrow$ (i). Soit G un groupe abélien simple ; G n'étant pas réduit à son élément neutre 0, soit x un élément de G différent de 0 et soit $\langle x \rangle$ le sous-groupe de G engendré par x ; alors $\langle x \rangle$ n'est pas $\{ 0 \}$ et G est simple, donc $\langle x \rangle = G$, ce qui montre que G est monogène, par suite (*cf.* Q., Ch. 4, § V, n° 83) G est isomorphe à $\mathbf{Z}$ s'il est infini et à $\mathbf{Z}/n\mathbf{Z}$ s'il est fini d'ordre n.

Je dis que G n'est pas infini ; en effet, s'il l'était, l'application f de $\mathbf{Z}$ dans G définie en posant pour chaque entier rationnel m, $f(m) = mx$, serait un isomorphisme de $\mathbf{Z}$ sur G ; mais alors si q est un entier strictement positif, $q\mathbf{Z}$ est un sous-groupe propre de $\mathbf{Z}$ dont l'image par f est un sous-groupe de G différent de $\{ 0 \}$ et de G ce qui est impossible.

Donc G est cyclique fini ; soit n son ordre. Je dis que n est nécessairement premier ; en effet, s'il ne l'était pas on pourrait l'écrire sous la forme $n = p.q$ où p et q sont deux entiers $\geqslant 2$, par suite $p.x$ serait un élément d'ordre q et le sous-groupe $\langle p.x \rangle$ de G engendré par $p.x$ serait différent de $\{ 0 \}$ et de G ce qui est impossible puisque G est simple, donc G est cyclique d'ordre premier.

2.11

Soient a et b deux éléments d'un groupe fini G.

1) Montrer que si a, b et ab sont d'ordre 2, a et b commutent.

2) Montrer que a et a^{-1} ont même ordre.

3) Montrer que a et bab^{-1} ont même ordre.

4) Montrer que ab et ba ont même ordre.

5) On suppose qu'il existe des entiers rationnels m et n tels que $a^m b^n = ba$; montrer que $a^{m-2} b^n$, $a^m b^{n-2}$ et ab^{-1} ont même ordre.

Solution 1) Comme a, b et ab sont d'ordre 2, on a : $a^2 = b^2 = (ab)^2 = e$ (e étant l'élément neutre de G), donc on a : $a = a^{-1}$, $b = b^{-1}$ et $ab = (ab)^{-1}$ par suite $ab = b^{-1} a^{-1} = ba$.

2) Le sous-groupe de G engendré par a et le sous-groupe de G engendré par a^{-1} coïncident donc a et a^{-1} ont même ordre.

3) Soit H le sous-groupe de G engendré par a, alors (*cf.* exercice 2.4) bHb^{-1} est un sous-groupe de G. Je dis que bHb^{-1} est le sous-groupe de G engendré par bab^{-1} ; en effet, pour tout entier rationnel n on a

$$(bab^{-1})^n = ba^n b^{-1}$$

donc tout sous-groupe de G qui contient bab^{-1} contient bHb^{-1}. D'autre part bHb^{-1} et H ont même ordre, donc bab^{-1} et a ont même ordre.

4) Comme $ba = b(ab)\, b^{-1}$, il résulte de la question 3 que ba et ab ont même ordre.

5) Comme $a^m b^{n-2} = (a^m b^n)\, b^{-2} = (ba)\, b^{-2} = b(ab^{-1})\, b^{-1}$, il résulte de la question 3 que $a^m b^{n-2}$ et ab^{-1} ont même ordre. De même on a

$$a^{m-2} b^n = a^{-2}(a^m b^n) = a^{-2}(ba) = a^{-1}(a^{-1} b)\, a = a^{-1}(a^{-1} b)\,(a^{-1})^{-1}$$

donc $a^{m-2} b^n$ et $a^{-1} b$ ont même ordre, or $a^{-1} b$ et son inverse $b^{-1} a$ ont même ordre (question 2) et $b^{-1} a$ et ab^{-1} ont même ordre (question 4), finalement $a^m b^{n-2}$, $a^{m-2} b^n$ et ab^{-1} ont même ordre.

2.12

Soit σ une permutation de degré n et $\sigma = \sigma_1 . \sigma_2 ..... \sigma_r$ sa décomposition en cycles opérant sur des parties disjointes deux à deux, de $[1, n]$. Montrer que l'ordre de σ est le p. p. c. m. des ordres des cycles σ_i.

Solution Comme les cycles σ_i opèrent sur des parties disjointes deux à deux de $[1, n]$, ils commutent deux à deux (*cf.* Q., Ch. 4, § VI, n° 85), par suite pour tout entier positif q on a $\sigma^q = \sigma_1^q . \sigma_2^q ..... \sigma^q$ et $\sigma^q = I$ si et seulement si $\sigma_i^q = I$ ($1 \leqslant i \leqslant r$). Or on sait (*cf.* exercice 2.8) que σ_i^q est l'identité si et seulement si l'ordre de σ_i divise q, donc le plus petit entier positif q tel que σ^q soit l'identité est le p. p. c. m. des ordres des σ_i ($1 \leqslant i \leqslant r$).

2.13 Décomposer les permutations suivantes en produit de cycles et donner leurs ordres :

$$a = \begin{pmatrix}1234567\\5647321\end{pmatrix} \quad b = \begin{pmatrix}12345678\\14327865\end{pmatrix} \quad c = \begin{pmatrix}123456789\\378945216\end{pmatrix}.$$

Calculer a^{201}, b^{198} et $c^{1\,000}$ dans $\mathscr{S}_9$.

Solution Les décompositions sont

$$a = (15347)\,(26)\,, \quad b = (24)\,(5768) \quad \text{et} \quad c = (138)\,(27)\,(4965)\,.$$

En appliquant le résultat de l'exercice 2.12, sachant que l'ordre d'un cycle de longueur p est p, on voit que l'ordre de a est 10, celui de b est 4 et celui de c est 12. Par suite,

$$a^{201} = a^{10\times 20+1} = a\,;\; b^{198} = b^{4\times 49+2} = b^2 = (24)^2\,(5768)^2 = (56)\,(78),$$

et

$$c^{1\,000} = c^{12\times 93+4} = c^4 = (138)^4\,(27)^4\,(4965)^4 = (138)^4 = (138)\,.$$

2.14 Soient n un entier $\geqslant 2$ et $\mathscr{S}_n$ le groupe symétrique de degré n.

1) Démontrer que $\mathscr{S}_n$ est engendré par les transpositions (1, 2), (2, 3), ... $(n-1, n)$.

(On montrera d'abord que toute transposition (i, j), $i \neq j$, est décomposable en produit de transpositions de la forme $(k, k+1)$, $1 \leqslant k \leqslant n-1$.)

2) En déduire que $\mathscr{S}_n$ est engendré par les transpositions

$$(1, 2), (1, 3), ..., (1, n)\,.$$

3) On pose $t = (1, 2)$ et $c = (1, 2, ..., n)$; calculer c^k et $c^k\, tc^{-k}$ lorsque $1 \leqslant k \leqslant n-2$ et en déduire que t et c engendrent $\mathscr{S}_n$.

Solution 1) Comme on sait (*cf.* Q., Ch. 4, § VI, n° 86) que toute permutation de $[1, n]$ s'écrit sous la forme d'un produit de transpositions, il suffira de montrer que toute transposition (i, j) $i \neq j$ s'écrit sous forme d'un produit de transpositions

$(k, k+1)$ avec $1 \leqslant k \leqslant n-1$; or $(i, j) = (j, i)$ donc on peut supposer $i < j$ et on a alors

$$(i,j) = (i,i+1)(i+1,i+2).....(j-2,j-1)(j-1,j)$$
$$(j-2,j-1).....(i+1,i+2)(i,i+1)$$

d'où le résultat.

2) Compte tenu du résultat de la question précédente, il suffira de montrer que toute transposition de la forme $(k, k+1)$ $(1 \leqslant k \leqslant n-1)$ s'exprime comme produit de transpositions de la forme $(1, p)$ $(2 \leqslant p \leqslant n)$, or on a pour tout entier k compris entre 1 et $n-1$,

$$(k, k+1) = (1, k)(1, k+1)(1, k)$$

d'où le résultat.

3) Si $n = 2$, $c = t$ et t engendre $\mathscr{S}_2$. Supposons donc $n \geqslant 3$ et soit k un entier tel que $1 \leqslant k \leqslant n-2$; comme

$$c = \begin{pmatrix} 1, 2, ..., n-1, & n \\ 2, 3, ..., & n, & 1 \end{pmatrix}$$

on a

$$c^k = \begin{pmatrix} 1, & 2, & ..., n-k, & n-k+1, & ..., n \\ k+1, & k+2, & ..., & n, & 1, & ..., k \end{pmatrix}$$

et

$$c^{-k} = \begin{pmatrix} 1, & 2, & ..., k, & k+1, & ..., & n \\ n-k+1, & n-k+2, & ..., n, & 1, & ..., & n-k \end{pmatrix}$$

d'où il vient que $c^k t c^{-k} = (k+1, k+2)$. Il en résulte que toute transposition de la forme $(k, k+1)$ avec $1 \leqslant k \leqslant n-1$, s'exprime comme produit de c, t et c^{-1}, or on sait (question 1) que les transpositions (1, 2), (2, 3), ..., $(n-1, n)$ engendrent $\mathscr{S}_n$, donc c et t engendrent $\mathscr{S}_n$.

2.15

Pour $n > 3$ on désigne par $\mathscr{A}'_n$ le sous-groupe de $\mathscr{S}_n$ engendré par les cycles

$$(1, 2, 3), (1, 2, 4), ..., (1, 2, n).$$

1) Montrer que $\mathscr{A}'_n$ est un sous-groupe du groupe alterné $\mathscr{A}_n$.

2) Démontrer que si i et j sont deux entiers distincts $(1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n)$ les permutations $(1, 2)(i, j)$ et $(i, j)(1, 2)$ appartiennent à $\mathscr{A}'_n$.

3) Montrer que $\mathscr{A}'_n = \mathscr{A}_n$. (On remarquera que toute permutation p de $\mathscr{A}_n$ peut s'écrire sous la forme

$$p = t_1 . t_2 ..... t_{2p-1} . t_{2p} = t_1 . t_0 . t_0 . t_2 . t_3 . t_0 ..... t_{2p-1} . t_0 . t_0 . t_{2p},$$

où $t_0, t_1, ..., t_{2p}$ sont des transpositions et $t_0 = (1, 2)$.)

Solution 1) Comme $\mathscr{A}_n$ est un sous-groupe de $\mathscr{S}_n$ il suffira de montrer que la famille génératrice $(1, 2, k)$, $(3 \leqslant k \leqslant n)$ de $\mathscr{A}'_n$ appartient à $\mathscr{A}_n$ ce qui est clair puisque les permutations $(1, 2, k)$, $(3 \leqslant k \leqslant n)$ sont des cycles d'ordre 3 donc des permutations paires.

2) Comme i et j sont distincts nous supposerons $i < j$ et distinguerons trois cas :

a) $i = 1$ et $j = 2$; alors $(i,j) = (1, 2)$ et $(i,j)(1, 2) = (1, 2)(i,j) = e$ où e est l'élément neutre de $\mathscr{S}_n$ donc $(i, j)(1, 2) \in \mathscr{A}'_n$ et $(1, 2)(i, j) \in \mathscr{A}'_n$.

b) $i = 1$ et $j > 2$; alors $(1, 2)(1, j) = (1, j, 2) = (1, 2, j)^2$ donc

$$(1, 2)(1, j) \in \mathscr{A}'_n$$

et $(1, j)(1, 2) = (1, 2, j)$ donc

$$(1, j)(1, 2) \in \mathscr{A}'_n .$$

c) $i > 1$; alors $j > 2$ donc (i, j) et $(1, 2)$ opèrent sur des parties disjointes de $[1, n]$ par suite ces transpositions commutent (*cf.* Q., Ch. 4, § VI, n° 85) or on a $(1, 2)(i, j) = (i, j)(1, 2) = (1, 2, i)(1, 2, j)^2 (1, 2, i)$ donc

$$(1, 2)(i, j) \in \mathscr{A}'_n \qquad \text{et} \qquad (i, j)(1, 2) \in \mathscr{A}'_n .$$

3) Soit p un élément de $\mathscr{A}_n$; comme p est une permutation paire elle s'exprime comme produit d'un nombre pair de transpositions (*cf.* Q., Ch. 4, § VI, n° 87) ; posons $p = t_1 . t_2 \ldots . t_{2p}$ où $t_1, t_2, \ldots, t_{2p}$ sont des transpositions et notons t_0 la transposition $(1, 2)$, alors $t_0^2 = e$ donc on a

$$\begin{aligned} p &= t_1\, t_0\, t_0\, t_2\, t_3\, t_0\, t_0\, t_4 \ldots . t_{2p-1}\, t_0\, t_0\, t_{2p} \\ &= (t_1\, t_0)(t_0\, t_2)(t_3\, t_0) \ldots . (t_{2p-1}\, t_0)(t_0\, t_{2p}) ; \end{aligned}$$

or d'après la question précédente les permutations $t_{2i-1}\, t_0$ et $t_0\, t_{2i}$ $(1 \leqslant i \leqslant p)$ appartiennent à $\mathscr{A}'_n$ donc $p \in \mathscr{A}'_n$ et $\mathscr{A}_n = \mathscr{A}'_n$.

2.16 Soient G_1 et G_2 deux groupes, $G_1 \times G_2$ le groupe produit de G_1 et G_2, π_1 et π_2 ses projections sur G_1 et G_2 respectivement. On se donne deux homomorphismes de groupes u_1 et u_2 définis tous deux sur un groupe G, à valeurs dans G_1 et G_2 respectivement ; montrer qu'il existe un homomorphisme h défini sur G à valeurs dans $G_1 \times G_2$, et un seul, tel que l'on ait $\pi_1 \circ h = u_1$ et $\pi_2 \circ h = u_2$.

Solution Nous noterons tous les groupes multiplicativement. Nous avons à prouver l'existence et l'unicité de h.

Unicité. Si h est un homomorphisme tel que $\pi_1 \circ h = u_1$ et $\pi_2 \circ h = u_2$, on a pour tout élément x de G, $\pi_1(h(x)) = u_1(x)$ et $\pi_2(h(x)) = u_2(x)$ donc $h(x) = (u_1(x), u_2(x))$ par conséquent h est uniquement déterminé.

Existence. Soit h l'application de G dans $G_1 \times G_2$ définie en posant pour chaque élément x de G, $h(x) = (u_1(x), u_2(x))$; alors on a bien $\pi_1 \circ h = u_1$ et $\pi_2 \circ h = u_2$ et il reste à vérifier que h est un homomorphisme de groupes ; or u_1 et u_2 sont des homomorphismes et, par définition de la loi produit dans $G_1 \times G_2$, on a pour tout couple (x, x') d'éléments de G,

$$\begin{aligned} h(x,x') &= (u_1(x,x'), u_2(x,x')) = (u_1(x)\,u_1(x'), u_2(x)\,u_2(x')) \\ &= (u_1(x), u_2(x)).(u_1(x'), u_2(x')) = h(x).h(x'), \end{aligned}$$

d'où le résultat.

2.17 On considère deux groupes G et G', deux homomorphismes de groupes f et g définis sur G à valeurs dans G' et on appelle H l'ensemble des éléments x de G tels que $f(x) = g(x)$.

1) Montrer que H est un sous-groupe de G.

2) On désigne par h l'injection canonique de H dans G.

a) Montrer que $f \circ h = g \circ h$.

b) Montrer que si G'' est un groupe et h' un homomorphisme défini sur G'' à valeurs dans G, tel que $f \circ h' = g \circ h'$, alors il existe un homomorphisme θ défini sur G'' à valeurs dans H, et un seul, tel que $h' = h \circ \theta$.

Solution 1) Soient e l'élément neutre de G et e' celui de G'. Comme f et g sont des homomorphismes, on a $f(e) = g(e) = e'$, donc $e \in H$, par suite (*cf.* Q., Ch. 4, § II, n° 72) il nous suffira de démontrer que si x et y sont deux éléments de H, $xy^{-1} \in H$. Si $x \in H$ et $y \in H$ on a $f(x) = g(x)$ et $f(y) = g(y)$ donc

$$f(y^{-1}) = (f(y))^{-1} = (g(y))^{-1} = g(y^{-1})$$

et

$$f(xy^{-1}) = f(x).f(y^{-1}) = g(x).g(y^{-1}) = g(xy^{-1})$$

donc $xy^{-1} \in H$ et H est un sous-groupe de G.

2) *a*) Si $x \in H$, $h(x) \in H$ donc $f(h(x)) = g(h(x))$ par suite $f \circ h = g \circ h$.

b) Si $f \circ h' = g \circ h'$, pour tout élément x'' de G'' on a $f(h'(x'')) = g(h'(x''))$ donc $h'(x'') \in H$. Soit donc θ l'application définie sur G'' à valeurs dans H que

l'on obtient en posant pour chaque élément x'' de G'', $\theta(x'') = h'(x'')$, alors θ est induite par h' donc est un homomorphisme de groupes, de plus on a pour tout élément x'' de G'' : $h(\theta(x'')) = \theta(x'') = h'(x'')$ donc $h \circ \theta = h'$ et si θ' est un homomorphisme défini sur G'' à valeurs dans H tel que $h \circ \theta' = h'$, on a pour tout élément x'' de G'',

$$h(\theta'(x'')) = h(\theta(x'')) = h'(x'')$$

donc $\theta(x'') = \theta'(x'')$ car h est injective, par suite $\theta = \theta'$ d'où le résultat.

2.18 Soient G_0, G_1, G_2 trois groupes, f_1 un homomorphisme de G_1 dans G_0 et f_2 un homomorphisme de G_2 dans G_0. On forme le groupe produit $G_1 \times G_2$ de G_1 et G_2, et on désigne par π_1 et π_2 ses projections sur G_1 et G_2 respectivement ; on appelle H l'ensemble des éléments (x_1, x_2) de $G_1 \times G_2$ tels que $f_1(x_1) = f_2(x_2)$, h l'injection canonique de H dans $G_1 \times G_2$ et on pose $g_1 = \pi_1 \circ h$ et $g_2 = \pi_2 \circ h$.

1) Montrer que H est un sous-groupe de $G_1 \times G_2$ et que $f_1 \circ g_1 = f_2 \circ g_2$.

2) Soient H' un groupe, g_1' et g_2' deux homomorphismes définis sur H' à valeurs dans G_1 et G_2 respectivement, tels que $f_1 \circ g_1' = f_2 \circ g_2'$. Montrer qu'il existe un homomorphisme θ défini sur H' à valeurs dans H, et un seul, tel que

$$g_1' = g_1 \circ \theta \qquad \text{et} \qquad g_2' = g_2 \circ \theta .$$

Solution 1) Pour chaque élément $x = (x_1, x_2)$ de $G_1 \times G_2$ on a $f_1 \circ \pi_1(x) = f_1(x_1)$ et $f_2 \circ \pi_2(x) = f_2(x_2)$ donc en posant $f_1 \circ \pi_1 = u_1, f_2 \circ \pi_2 = u_2, G = G_1 \times G_2$, $G' = G_0$, on se trouve dans la situation de l'exercice 2.17, donc H est un sous-groupe de $G_1 \times G_2$ et $f_1 \circ \pi_1 \circ h = f_2 \circ \pi_2 \circ h$ soit $f_1 \circ g_1 = f_2 \circ g_2$.

2) Si g_1' et g_2' sont deux homomorphismes définis sur H' à valeurs dans G_1 et G_2 respectivement, on sait (exercice 2.16) qu'il existe un homomorphisme h' défini sur H' à valeurs dans $G_1 \times G_2$, et un seul, tel que $g_1' = \pi_1 \circ h'$ et $g_2' = \pi_2 \circ h'$, alors l'égalité $f_1 \circ g_1' = f_2 \circ g_2'$ devient

$$f_1 \circ \pi_1 \circ h' = f_2 \circ \pi_2 \circ h'$$

soit, avec les notations introduites ci-dessus, $u_1 \circ h' = u_2 \circ h'$, par suite (exercice 2.17) il existe un homomorphisme θ défini sur H' à valeurs dans H, et un seul, tel que $h' = h \circ \theta$; alors on a $g_1' = \pi_1 \circ h' = \pi_1 \circ h \circ \theta = g_1 \circ \theta$ et $g_2' = \pi_2 \circ h' = \pi_2 \circ h \circ \theta = g_2 \circ \theta$. Il reste à prouver l'unicité de θ ; soit donc θ' un homomorphisme de H' dans H tel que $g_1' = g_1 \circ \theta'$ et $g_2' = g_2 \circ \theta'$;

on a $g'_1 = \pi_1 \circ (h \circ \theta')$ et $g'_2 = \pi_2 \circ (h \circ \theta')$ donc en vertu de l'assertion d'unicité de l'exercice 2.16, on a $h \circ \theta' = h' = h \circ \theta$, or h est injectif donc pour tout élément x' de H' on a $h(\theta'(x')) = h(\theta(x'))$ donc $\theta'(x') = \theta(x')$ et $\theta = \theta'$ d'où le résultat.

Le groupe H construit dans cet exercice s'appelle le *produit fibré de G_1 et G_2 au-dessus de G_0, relativement aux homomorphismes f_1 et f_2*.

2.19

Soient G_0 un groupe abélien, G_1 et G_2 deux sous-groupes de G_0 tels que $G_1 \subset G_2$ et π_1 et π_2 les homomorphismes canoniques de G_0 sur G_0/G_1 et G_0/G_2 respectivement.

1) Montrer qu'il existe un homomorphisme ρ défini sur G_0/G_1 à valeurs dans G_0/G_2, et un seul, tel que $\rho \circ \pi_1 = \pi_2$.

2) Montrer que ρ est surjectif et que son noyau est G_2/G_1.

Solution

1) Soit $\bar{x}$ un élément de G_0/G_1 ; comme π_1 est surjectif il existe un élément x de G_0 tel que $\bar{x} = \pi_1(x)$, de plus si x' est un élément de G_0 tel que $\pi_1(x') = \pi_1(x)$, alors $x - x' \in G_1$ donc $x - x' \in G_2$ et $\pi_2(x) = \pi_2(x')$, donc l'élément $\pi_2(x)$ de G_0/G_2 ne dépend que de $\bar{x}$ (et non du choix de x) ; posons $\rho(\bar{x}) = \pi_2(x)$. Nous avons ainsi défini une application ρ de G_0/G_1 dans G_0/G_2 telle que $\rho \circ \pi_1 = \pi_2$; de plus ρ est un homomorphisme, en effet, si $\bar{x}$ et $\bar{y}$ sont deux éléments de G_0/G_1, il existe deux éléments x et y de G_0 tels que $\bar{x} = \pi_1(x)$ et $\bar{y} = \pi_1(y)$ et par définition des lois de composition de G_0/G_1 et G_0/G_2 (*cf.* Q., Ch. 4, § II, n° 75) on a :

$$\bar{x} + \bar{y} = \pi_1(x + y)$$

donc

$$\rho(\bar{x} + \bar{y}) = \rho\big(\pi_1(x + y)\big) = \pi_2(x + y) = \pi_2(x) + \pi_2(y) = \rho(\bar{x}) + \rho(\bar{y}) .$$

A présent démontrons l'unicité de ρ ; si ρ' est un homomorphisme de G_0/G_1 dans G_0/G_2 tel que $\pi_2 = \rho' \circ \pi_1$, on a $\rho \circ \pi_1 = \rho' \circ \pi_1$, or, pour tout élément $\bar{x}$ de G_0/G_1 il existe un élément x de G_0 tel que $\bar{x} = \pi_1(x)$, donc

$$\rho(\bar{x}) = \rho(\pi_1(x)) = \rho'(\pi_1(x)) = \rho'(\bar{x})$$

par suite $\rho = \rho'$.

2) Comme π_1 et π_2 sont surjectifs on a $\pi_1(G_0) = G_0/G_1$ et $\pi_2(G_0) = G_0/G_2$ or $\pi_2(G_0) = \rho(\pi_1(G_0))$ donc $G_0/G_2 = \rho(G_0/G_1)$ ce qui prouve que ρ est surjectif. D'autre part, un élément $\bar{x} = \pi_1(x)$ de G_0/G_1 est dans le noyau de ρ si et seulement si on a $\rho(\bar{x}) = \pi_2(x) = G_2$ c'est-à-dire $x \in G_2$ ou encore $\bar{x} \in G_2/G_1$, donc $\operatorname{Ker} \rho = G_2/G_1$.

2.20 Soient G_0, G_1, G_2 des groupes, f_1 un homomorphisme surjectif de G_0 sur G_1 et f_2 un homomorphisme de G_0 dans G_2 tels que $\operatorname{Ker} f_1 \subset \operatorname{Ker} f_2$.

1) Montrer qu'il existe un homomorphisme g défini sur G_1 à valeurs dans G_2, et un seul, tel que $f_2 = g \circ f_1$.

2) Montrer que $\operatorname{Ker} g = f_1(\operatorname{Ker} f_2)$.

Solution Nous noterons tous les groupes multiplicativement et désignerons par e_i l'élément neutre de G_i $(0 \leqslant i \leqslant 2)$.

1) Soit y un élément de G_1 ; comme f_1 est surjectif, il existe un élément x de G_0 tel que $y = f_1(x)$, de plus si x' est un élément de G_0 tel que $y = f_1(x')$, on a $f_2(x) = f_2(x')$, en effet, la condition $f_1(x) = f_1(x')$ équivaut à

$$f_1(x^{-1}.x') = e_1 \quad \text{ou à} \quad x^{-1}.x' \in \operatorname{Ker} f_1 ,$$

or $\operatorname{Ker} f_1 \subset \operatorname{Ker} f_2$ donc $x^{-1}.x' \in \operatorname{Ker} f_2$ et $f_2(x^{-1}.x') = e_2$ d'où

$$f_2(x) = f_2(x') ;$$

il résulte de ceci que $f_2(x)$ ne dépend que de y (et non du choix de x) ; posons $g(y) = f_2(x)$. Nous avons ainsi défini une application g de G_1 dans G_2 telle que $g \circ f_1 = f_2$; de plus g est un homomorphisme, en effet, si y et y' sont deux éléments de G_1 et x et x' deux éléments de G_0 tels que $y = f_1(x)$ et $y' = f_1(x')$, on a $yy' = f_1(x.x')$ donc

$$g(yy') = g(f_1(xx')) = f_2(xx') = f_2(x).f_2(x') = g(y).g(y') .$$

Pour démontrer l'unicité de g supposons qu'il existe un homomorphisme g' de G_1 dans G_2 tel que $f_2 = g' \circ f_1$ alors pour tout élément y de G_1 il existe un élément x de G_0 tel que $y = f_1(x)$ donc

$$g'(y) = g'(f_1(x)) = f_2(x) = g(f_1(x)) = g(y)$$

par suite $g = g'$.

2) Soient y un élément de G_1 et x un élément de G_0 tels que $y = f_1(x)$; alors y est dans le noyau de g si et seulement si $g(y) = f_2(x) = e_2$, c'est-à-dire si et seulement si $x \in \operatorname{Ker} f_2$, autrement dit $y \in f_1(\operatorname{Ker} f_2)$ donc $\operatorname{Ker} g = f_1(\operatorname{Ker} f_2)$.

2.21 Soient G un groupe abélien d'élément neutre 0 et $(G_i)_{i \in I}$ une famille de sous-groupes de G telle que $\bigcap_{i \in I} G_i = \{ 0 \}$. Montrer que G est isomorphe à un sous-groupe G' du groupe produit $\prod_{i \in I} (G/G_i)$ et décrire G'.

Solution Notons G additivement. Pour chaque élément i de I, désignons par π_i l'homomorphisme canonique de G sur G/G_i et soit π l'application de G dans $\prod_{i \in I} (G/G_i)$ définie en posant pour chaque élément x de G, $\pi(x) = (\pi_i(x))_{i \in I}$. Alors π est un homomorphisme ; en effet, les π_i $(i \in I)$ étant des homomorphismes, par définition de la loi produit dans $\prod_{i \in I} (G/G_i)$, on a pour tout couple (x, y) d'éléments de G :

$$\begin{aligned}\pi(x + y) &= (\pi_i(x + y))_{i \in I} = (\pi_i(x) + \pi_i(y))_{i \in I} \\ &= (\pi_i(x))_{i \in I} + (\pi_i(y))_{i \in I} = \pi(x) + \pi(y) .\end{aligned}$$

De plus, le noyau de π se compose des éléments x de G tels que pour tout élément i de I, on ait $\pi_i(x) = G_i$ c'est-à-dire $x \in G_i$, donc

$$\operatorname{Ker} \pi = \bigcap_{i \in I} G_i = \{ 0 \}$$

si bien que π est injectif. Désignons par G' l'image de π ; alors π induit un isomorphisme de G sur G' et G' est le sous-groupe de $\prod_{i \in I} (G/G_i)$ formé des éléments $(y_i)_{i \in I}$ de $\prod_{i \in I} (G/G_i)$ pour lesquels il existe un élément x de G tel que $y_i = \pi_i(x)$ pour chaque élément i de I.

2.22 Si G est un groupe abélien, nous désignerons par Hom $(\mathbf{Z}, G)$ l'ensemble des homomorphismes de $\mathbf{Z}$ dans G.

1) Montrer que tout homomorphisme f de $\mathbf{Z}$ dans G est complètement déterminé par la donnée de $f(1)$.

2) On munit Hom $(\mathbf{Z}, G)$ de la loi de composition suivante : si f et g sont deux éléments de Hom $(\mathbf{Z}, G)$, $f + g$ est l'application de $\mathbf{Z}$ dans G définie en posant pour chaque entier rationnel n, $(f + g)(n) = f(n) + g(n)$. Montrer que Hom $(\mathbf{Z}, G)$ devient ainsi un groupe abélien.

3) Soient G_1, G_2, G_3 trois groupes abéliens, f_1 un homomorphisme de G_1 dans G_2 et f_2 un homomorphisme de G_2 dans G_3. On note f_1^* l'application de Hom $(\mathbf{Z}, G_1)$ dans Hom $(\mathbf{Z}, G_2)$ définie en posant pour chaque élément g de Hom $(\mathbf{Z}, G_1)$, $f_1^*(g) = f_1 \circ g$, et on définit de manière analogue f_2^*.

a) Montrer que f_1^* et f_2^* sont des homomorphismes.

b) Montrer que si $G_1 = G_2$ et si f_1 est l'identité de G_1, alors f_1^* est l'identité de Hom $(\mathbf{Z}, G_1)$.

c) Montrer que $(f_2 \circ f_1)^* = f_2^* \circ f_1^*$.

d) Montrer que si f_1 est injectif, f_1^* est injectif.

e) Montrer que si f_1 est surjectif, f_1^* est surjectif.

Solution 1) Soit x un élément de G ; je dis qu'il existe un seul homomorphisme f de $\mathbf{Z}$ dans G tel que $f(1) = x$. En effet, on a nécessairement $f(0) = 0$; si n est un entier $\geqslant 1$, $f(n) = f(1) + f(1) + \cdots + f(1)$ (n termes) donc $f(n) = n.x$ et si m est un entier < 0, on a $f(m) = -f(-m)$.

2) Observons d'abord que si f et g sont des homomorphismes de $\mathbf{Z}$ dans G, il en est de même de $f + g$; en effet, si m et n sont deux entiers rationnels, on a

$$(f + g)(m + n) = f(m + n) + g(m + n) = f(m) + f(n) + g(m) + g(n) = \\ = (f(m) + g(m)) + (f(n) + g(n)) = (f + g)(m) + (f + g)(n),$$

donc on a bien défini une loi de composition *interne* sur Hom $(\mathbf{Z}, G)$.

Cette loi est associative car si f, g, h sont des éléments de Hom $(\mathbf{Z}, G)$, en vertu de l'associativité de la loi de G, on a pour tout entier rationnel n,

$$((f + g) + h)(n) = ((f + g)(n) + h(n)) = (f(n) + g(n)) + h(n) = \\ = f(n) + (g(n) + h(n)) = f(n) + (g + h)(n) = (f + (g + h))(n),$$

donc

$$(f + g) + h = f + (g + h).$$

Cette loi est commutative, car on a pour tout couple (f, g) d'éléments de Hom $(\mathbf{Z}, G)$ et tout entier rationnel n,

$$(f + g)(n) = f(n) + g(n) = g(n) + f(n) = (g + f)(n),$$

donc

$$f + g = g + f.$$

La fonction constante définie sur $\mathbf{Z}$ qui prend pour valeur l'élément neutre 0 de G, est l'élément neutre de Hom $(\mathbf{Z}, G)$. Enfin si f est un élément de Hom $(\mathbf{Z}, G)$, l'application $(-f)$ de $\mathbf{Z}$ dans G, définie en posant pour tout entier rationnel n, $(-f)(n) = -f(n)$, est l'opposé dans Hom $(\mathbf{Z}, G)$ de f.

Par suite Hom $(\mathbf{Z}, G)$ est ainsi muni d'une structure de groupe abélien.

3) *a*) Montrons par exemple que f_1^* est un homomorphisme. Si g et h sont deux éléments de Hom $(\mathbf{Z}, G_1)$, pour tout entier rationnel n, on a

$$f_1((g + h)(n)) = f_1(g(n) + h(n)) = f_1(g(n)) + f_1(h(n))$$

donc $f_1 \circ (g + h) = f_1 \circ g + f_1 \circ h$ par suite

$$f_1^*(g + h) = f_1^*(g) + f_1^*(h).$$

d'où le résultat.

b) Si $f_1 = \mathrm{Id}\, G_1$, pour tout élément g de Hom $(\mathbf{Z}, G_1)$ on a

$$f_1^*(g) = \mathrm{Id}\, G_1 \circ g = g \qquad \text{donc} \qquad f_1^* = \mathrm{Id}\, \mathrm{Hom}\,(\mathbf{Z}, G_1).$$

c) Si g est un élément de Hom $(\mathbf{Z}, G_1)$, on a :

$$(f_2 \circ f_1)^*(g) = f_2 \circ f_1 \circ g \text{ et } (f_2^* \circ f_1^*)(g) = \\ = f_2^*(f_1^*(g)) = f_2^*(f_1 \circ g) = f_2 \circ f_1 \circ g$$

donc

$$f_2^* \circ f_1^* = (f_2 \circ f_1)^*$$

d) Si f_1 est injectif et si g et g' sont deux éléments de Hom $(\mathbf{Z}, G_1)$ tels que

$$f_1^*(g) = f_1^*(g'),$$

on a $f_1 \circ g = f_1 \circ g'$ donc pour tout entier rationnel n, on a $f_1(g(n)) = f_1(g'(n))$ donc $g(n) = g'(n)$ et $g = g'$, par suite f_1^* est injectif.

e) Supposons f_1 surjectif, soient h un élément de Hom $(\mathbf{Z}, G_2)$ et x un élément de G_1 tel que $f_1(x) = h(1)$. Alors (question 1) il existe un homomorphisme $\tilde{h}$ de $\mathbf{Z}$ dans G_1, et un seul, tel que $\tilde{h}(1) = x$ et on a $f_1 \circ \tilde{h}(1) = h(1)$ donc

$$f_1 \circ \tilde{h} = h = f_1^*(\tilde{h}) \qquad \text{et} \qquad f_1^* \text{ est surjectif}.$$

3

ANNEAUX ET CORPS

3.1 Soient E un ensemble et $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ l'ensemble des applications de E dans l'anneau $\mathbf{Z}/2\,\mathbf{Z}$. On désigne par 0 et 1 les éléments de $\mathbf{Z}/2\,\mathbf{Z}$.

1) On munit $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ de l'addition et de la multiplication définies comme suit : si f et g sont deux éléments de $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ alors $f + g$ et $f.g$ sont les applications de E dans $\mathbf{Z}/2\,\mathbf{Z}$ telles que l'on ait pour tout élément x de E :

$$(f + g)(x) = f(x) + g(x) \quad \text{et} \quad (f.g)(x) = f(x).g(x).$$

Démontrer que l'ensemble $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ muni de ces deux lois est un anneau commutatif et unitaire.

2) A toute partie A de E on associe l'application Φ_A de E dans $\mathbf{Z}/2\,\mathbf{Z}$ définie par :

$$\begin{cases} \Phi_A(x) = 1 & \text{si} \quad x \in A \\ \Phi_A(x) = 0 & \text{si} \quad x \notin A \end{cases}$$

a) Démontrer que, quelles que soient les parties A et B de E, la relation $A = B$ est équivalente à $\Phi_A = \Phi_B$.

b) Calculer Φ_{E-A} en fonction de Φ_A ; calculer Φ_{A-B} en fonction de Φ_A et Φ_B si $B \subset A$; calculer $\Phi_{A \cap B}$ et $\Phi_{A \cup B}$ en fonction de Φ_A et Φ_B.

c) Quelles que soient les parties A et B de E, on pose :

$$A \triangle B = (A \cup B) - (A \cap B).$$

Calculer $\Phi_{A \triangle B}$ en fonction de Φ_A et Φ_B.

3) Soit Φ l'application de l'ensemble $\mathfrak{P}(E)$ des parties de E dans $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$, définie par

$$\Phi(A) = \Phi_A \quad \text{pour tout } A \in \mathfrak{P}(E).$$

Montrer que Φ est une bijection de $\mathfrak{P}(E)$ sur $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$. En déduire, au moyen des résultats précédents, que $(\mathfrak{P}(E), \triangle, \cap)$ est un anneau commutatif et unitaire.

Solution 1) L'addition de $\mathbf{Z}/2\,\mathbf{Z}$ étant associative et commutative, il en est de même de l'addition définie ici sur $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ (*cf.* Q., Ch. 3, § II, n° 54), de plus la fonction constante n définie sur E et de valeur 0 est élément neutre de $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ (*loc. cit.*).

Si f est un élément de $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$, en posant $(-f)(x) = -f(x)$ pour tout $x \in E$ on voit que, $[f + (-f)](x) = f(x) + (-f(x)) = 0 = n(x)$ donc $f + (-f) = n$ ce qui montre que $(-f)$ est l'opposé de f pour l'addition. $(\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z}), +)$ est donc un groupe abélien. La multiplication de $\mathbf{Z}/2\,\mathbf{Z}$ est associative et commutative ; il en est donc de même de celle de $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ (*loc. cit.*) de plus, l'application constante u sur E de valeur 1 est l'élément neutre de $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ pour la multiplication. Par ailleurs, si f, g, h sont des éléments de $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ et x un élément de E, on a

$$[(f + g).h](x) = (f + g)(x).h(x) = (f(x) + g(x)).h(x)$$

d'où en vertu de la distributivité de la multiplication par rapport à l'addition dans $\mathbf{Z}/2\,\mathbf{Z}$:

$$\begin{aligned}[(f + g).h](x) &= f(x).h(x) + g(x).h(x) \\ &= (f.h)(x) + (g.h)(x) = [f.h + g.h](x) ;\end{aligned}$$

par suite $(f + g).h = f.h + g.h$ donc la multiplication de $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ est distributive à gauche, donc distributive par rapport à l'addition. Ceci montre que $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ muni de l'addition et de la multiplication ci-dessus, est un anneau commutatif et unitaire.

2) *a*) Il est clair que si $A = B$, $\Phi_A = \Phi_B$. Réciproquement, supposons que $\Phi_A = \Phi_B$, alors un élément x de E appartient à A si et seulement si

$$\Phi_A(x) = 1 = \Phi_B(x)$$

donc si et seulement s'il appartient à B, par suite $A = B$.

b) Si $x \in A$, $\Phi_{E-A}(x) = 0 = 1 - \Phi_A(x)$; si $x \notin A$, $\Phi_{E-A}(x) = 1 = 1 - \Phi_A(x)$; or, pour tout élément x de E, $\Phi_E(x) = 1$ donc $\Phi_{E-A} = \Phi_E - \Phi_A$. Comme, dans $\mathbf{Z}/2\,\mathbf{Z}$ chaque élément est égal à son opposé, il en est de même dans $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ et on a aussi $\Phi_{E-A} = \Phi_E + \Phi_A$.

Soient A et B deux parties de E telles que $B \subset A$; si x est un élément de E et si $x \notin A$, alors $x \notin B$ et $\Phi_{A-B}(x) = 0 = \Phi_A(x) - \Phi_B(x)$; si $x \in A$ et $x \notin B$ alors $x \in A - B$ donc $\Phi_{A-B}(x) = 1 = \Phi_A(x) - \Phi_B(x)$; enfin si $x \in B$, alors $x \in A$ et $\Phi_{A-B}(x) = 0 = \Phi_A(x) - \Phi_B(x)$. Ceci prouve que $\Phi_{A-B} = \Phi_A - \Phi_B$ soit aussi (*cf.* remarque ci-dessus) que $\Phi_{A-B} = \Phi_A + \Phi_B$.

Soient A et B deux parties de E et x un élément de E ; si $x \in A \cap B$ on a $\Phi_{A \cap B}(x) = \Phi_A(x).\Phi_B(x)$; si $x \notin A \cap B$, on a $\Phi_{A \cap B}(x) = 0 = \Phi_A(x).\Phi_B(x)$ car alors $\Phi_A(x) = 0$ ou $\Phi_B(x) = 0$; donc $\Phi_{A \cap B} = \Phi_A.\Phi_B$.

Nous allons déduire le calcul de $\Phi_{A \cup B}$ de celui de $\Phi_{A \cap B}$; on sait que $\Phi_{E-(A \cup B)} = \Phi_E + \Phi_{A \cup B}$ donc $\Phi_{A \cup B} = \Phi_{E-(A \cup B)} - \Phi_E$. Or

$$E - (A \cup B) = (E - A) \cap (E - B)$$

donc

$$\Phi_{E-(A \cup B)} = \Phi_{E-A}.\Phi_{E-B} = (\Phi_E - \Phi_A).(\Phi_E - \Phi_B) ;$$

comme $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ est un anneau, on a :

$$\Phi_{E-(A \cup B)} = \Phi_E.\Phi_E - \Phi_E.\Phi_B - \Phi_A.\Phi_E + \Phi_A.\Phi_B$$

soit

$$\Phi_{E-(A \cup B)} = \Phi_{E \cap E} - \Phi_{E \cap B} - \Phi_{A \cap E} + \Phi_{A \cap B} = \Phi_E - \Phi_B - \Phi_A + \Phi_{A \cap B}$$

d'où $\Phi_{A \cup B} = \Phi_A + \Phi_B - \Phi_{A \cap B}$ soit aussi $\Phi_{A \cup B} = \Phi_A + \Phi_B + \Phi_{A \cap B}$.

c) On a

$$\Phi_{A \Delta B} = \Phi_{A \cup B} - \Phi_{A \cap B} = \Phi_A + \Phi_B + \Phi_{A \cap B} - \Phi_{A \cap B} = \Phi_A + \Phi_B .$$

3) La question 2) *a*) montre que Φ est une injection ; si φ est un élément de $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ et $A(\varphi)$ l'ensemble des éléments x de E tels que $\varphi(x) = 1$, alors on a $\varphi = \Phi_{A(\varphi)}$ ce qui montre que Φ est surjective donc bijective. Comme, pour tout couple A, B de parties de E, on a

$$\Phi_{A \Delta B} = \Phi_A + \Phi_B \quad \text{et} \quad \Phi_{A \cap B} = \Phi_A.\Phi_B$$

soit

$$\Phi(A \triangle B) = \Phi(A) + \Phi(B) \quad \text{et} \quad \Phi(A \cap B) = \Phi(A).\Phi(B),$$

on voit que Φ est un homomorphisme de la loi $\triangle$ dans l'addition de $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ et un homomorphisme de la loi $\cap$ dans la multiplication de $\mathscr{F}(E, \mathbf{Z}/2\,\mathbf{Z})$ par suite $(\mathfrak{P}(E), \triangle, \cap)$ est un anneau commutatif et unitaire.

3.2 Soit C le centre d'un anneau A (c'est-à-dire, l'ensemble des éléments c de A tels que pour tout élément x de A, on ait : $c.x = x.c$). Montrer que C est un sous-anneau de A.

Solution Remarquons d'abord que l'élément nul 0 de A appartient à C puisque pour tout élément x de A, on a $0.x = x.0 = 0$. Il suffira donc de montrer que si a et b sont deux éléments de C, il en est de même de $a - b$ et de $a.b$ (*cf.* Q., Ch. 5, § I, n° 93) ; or pour tout élément x de A, on a $x.(a - b) = x.a - x.b$ et a et b appartiennent à C donc $x.a = a.x$ et $x.b = b.x$, par suite

$$x.(a - b) = a.x - b.x = (a - b).x$$

ce qui montre que $(a - b) \in C$. Calculons maintenant $x.(a.b)$, x désignant toujours un élément quelconque de A ; nous pouvons écrire $x.(a.b) = (x.a).b$ (associativité de la multiplication de A), or $x.a = a.x$, car $a \in C$, donc $(x.a).b = (a.x).b$ mais $(a.x).b = a.(x.b)$ et $x.b = b.x$ car $b \in C$, donc $(a.x).b = a.(b.x) = (a.b).x$ d'où $x.(a.b) = (a.b).x$, par suite $a.b \in C$ et C est un sous-anneau de A.

3.3 Soient A un anneau commutatif et I un idéal de A. On appelle *radical de I* et on note $\sqrt{I}$, l'ensemble des éléments x de A pour lesquels il existe un entier n tel que x^n appartienne à I.

1) Démontrer que $\sqrt{I}$ contient I et que $\sqrt{I}$ est un idéal de A.

2) Soient I et J deux idéaux de A tels que $I \subset J$; démontrer que $\sqrt{I} \subset \sqrt{J}$. Démontrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.

3) Soient I et J deux idéaux de A ; démontrer que $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Solution 1) Remarquons d'abord que $\sqrt{I}$ est non vide car il contient l'idéal I ; en effet, si x est un élément de I, $x^1 = x$ appartient à I donc x est élément de $\sqrt{I}$. Soient x et y deux éléments de $\sqrt{I}$; il existe alors deux entiers m et n tels que x^n et y^m appartiennent à I. Calculons $(x - y)^{m+n}$; puisque l'anneau A est commutatif nous pouvons utiliser la formule du binôme ; on obtient

$$(x - y)^{m+n} = \sum_{p=0}^{p=m+n} (-1)^{m+n-p} C_{m+n}^{p} x^p y^{m+n-p}$$

$$= \sum_{p=0}^{p=n} (-1)^{m+n-p} C_{m+n}^{p} x^p y^{m+n-p} + \sum_{p=n+1}^{p=m+n} (-1)^{m+n-p} C_{m+n}^{p} x^p y^{m+n-p}$$

si $0 \leqslant p \leqslant n$, $m + n - p \geqslant m$ donc

$$x^p y^{m+n-p} = y^m (x^p y^{n-p})$$

si $n + 1 \leqslant p \leqslant m + n$,

$$x^p y^{m+n-p} = x^n (x^{p-n} y^{m+n-p}),$$

donc

$$(x - y)^{m+n} = y^m \left(\sum_{p=0}^{p=n} (-1)^{m+n-p} C_{m+n}^{p} x^p y^{n-p} \right) + x^n \left(\sum_{p=n+1}^{p=m+n} (-1)^{m+n-p} C_{m+n}^{p} x^{p-n} y^{m+n-p} \right)$$

mais y^m appartient à l'idéal I donc

$$y^m\left(\sum_{p=0}^{p=n}(-1)^{m+n-p}\,C_{m+n}^{p}\,x^p\,y^{n-p}\right)$$

est élément de I, de même x^n appartient à I, donc

$$x^n\left(\sum_{p=n+1}^{p=m+n}(-1)^{m+n-p}\,C_{m+n}^{p}\,x^{p-n}\,y^{m+n-p}\right)$$

est élément de I, par suite $(x-y)^{m+n}$ appartient à I donc $x-y$ est élément de $\sqrt{I}$.

Soit a un élément de A, alors $(ax)^n = a^n x^n$ car l'anneau A est commutatif, mais x^n appartient à I donc $a^n x^n$ est élément de I, par suite ax appartient à $\sqrt{I}$ ce qui montre que $\sqrt{I}$ est un idéal de A.

2) Soit x un élément de $\sqrt{I}$, alors il existe un entier n tel que x^n appartienne à I ; comme $I \subset J$, x^n appartient à J donc x est élément de $\sqrt{J}$ ce qui montre que $\sqrt{I} \subset \sqrt{J}$. Nous avons vu que $I \subset \sqrt{I}$, donc $\sqrt{I} \subset \sqrt{\sqrt{I}}$. Soit y un élément de $\sqrt{\sqrt{I}}$ alors il existe un entier p tel que y^p appartienne à $\sqrt{I}$, mais comme y^p est un élément de $\sqrt{I}$, il existe un entier q tel que $(y^p)^q$ appartienne à I, donc y^{pq} est élément de I c'est-à-dire que y appartient à $\sqrt{I}$ donc $\sqrt{\sqrt{I}} \subset \sqrt{I}$ d'où $\sqrt{\sqrt{I}} = \sqrt{I}$.

3) On a $I \cap J \subset I$ et $I \cap J \subset J$ donc $\sqrt{I \cap J} \subset \sqrt{I}$ et $\sqrt{I \cap J} \subset \sqrt{J}$ soit $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$. A présent soit x un élément de $\sqrt{I} \cap \sqrt{J}$; alors il existe deux entiers m et n tels que x^n appartienne à I et x^m à J. Puisque x^n appartient à I, il en est de même de $x^m.x^n$; puisque x^m appartient à J, il en est de même de $x^m.x^n$, par suite x^{m+n} appartient à $I \cap J$ donc x est élément de $\sqrt{I \cap J}$, donc $\sqrt{I} \cap \sqrt{J} \subset \sqrt{I \cap J}$ d'où $\sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J}$.

3.4 Soit A un anneau. Un élément x de A est dit *nilpotent* s'il existe un entier n tel que x^n soit nul. Soient x et y deux éléments nilpotents de A qui commutent ; démontrer que xy, $x+y$ et $x-y$ sont des éléments nilpotents de A.

Solution Puisque x et y sont nilpotents, il existe deux entiers m et n tels que $x^n = y^m = 0$; comme x et y commutent, on a pour tout entier p, $(xy)^p = x^p y^p$, en particulier $(xy)^n = x^n y^n = 0$ donc xy est nilpotent.

Démontrons maintenant que $x + \varepsilon y$ ($\varepsilon = +1$ ou -1) est nilpotent.

Puisque x et y commutent, il en est de même de x et εy et on a pour tout entier p,

$$(x + \varepsilon y)^p = \sum_{k=0}^{k=p} C_p^k x^k \varepsilon^{p-k} y^{p-k}$$

en particulier on a

$$(x + \varepsilon y)^{m+n} = y^m \left(\sum_{k=0}^{k=n} C_{m+n}^k x^k \varepsilon^{m+n-k} y^{n-k} \right) + \\ + x^n \left(\sum_{k=n+1}^{k=m+n} C_{m+n}^k x^{k-n} \varepsilon^{m+n-k} y^{m+n-k} \right)$$

or $x^n = y^m = 0$ donc $(x + \varepsilon y)^{m+n} = 0$ ce qui montre que $x + y$ et $x - y$ sont nilpotents.

3.5 Soient A un anneau et X une partie non vide de A. Désignons par $N(X)$ l'ensemble des éléments u de A tels que $u.x = 0$ pour tout élément x de X.

1) Démontrer que $N(X)$ est un idéal à gauche de A.

2) Démontrer que si I est un idéal à gauche de A, alors $N(I)$ est un idéal bilatère.

Solution 1) Soient u et u' deux éléments de $N(X)$ et x un élément de X ; alors

$$(u - u').x = u.x - u'.x ,$$

mais $u.x = 0$ et $u'.x = 0$ donc $(u - u').x = 0$ et $u - u'$ appartient à $N(X)$. Soient a un élément de A et u un élément de $N(X)$; alors pour tout élément x de X on a : $(a.u).x = a.(u.x) = a.0 = 0$ donc $a.u$ appartient à $N(X)$. Ceci montre que $N(X)$ est un idéal à gauche de A (*cf.* Q., Ch. 5, § II, n° 94).

2) On sait déjà (question précédente) que $N(I)$ est un idéal à gauche de A ; il suffira donc de montrer que $N(I)$ est un idéal à droite. Soient donc a un élément de A et u un élément de $N(X)$; alors, pour tout élément x de I on a $(u.a).x = u.(a.x)$; comme I est un idéal à gauche, $a.x$ appartient à I donc $u.(a.x) = 0 = (u.a).x$, par suite $u.a$ appartient à $N(I)$ donc $N(I)$ est un idéal bilatère de A.

3.6 Soit A un anneau commutatif et unitaire. Nous désignerons par 0 (respectivement 1) l'élément neutre de l'addition (resp. la multiplication) de A. Soit d un élément fixé de A. On désigne par $A[\sqrt{d}]$ l'ensemble $A \times A$ muni des deux opérations

$$(a, a') + (b, b') = (a + b, a' + b')$$
$$(a, a').(b, b') = (ab + da'b', ab' + a'b) .$$

a) Démontrer que $A[\sqrt{d}]$ muni de ces deux opérations est un anneau commutatif unitaire.

b) Soit A' le sous-ensemble des éléments de $A[\sqrt{d}]$ de la forme $(a, 0)$. Démontrer que A' est un sous-anneau de $A[\sqrt{d}]$ isomorphe à A. Dans toute la suite on identifiera A et A' (autrement dit, $(x, 0)$ est identifié à x).

c) Démontrer que tout élément de $A[\sqrt{d}]$ s'écrit d'une manière unique sous la forme $a + a'.(0, 1)$. Démontrer que dans $A[\sqrt{d}]$, d admet une racine carrée (c'est-à-dire qu'il existe un élément (x, y) de $A[\sqrt{d}]$ tel que $(x, y)^2 = (d, 0) = d$). Cette racine carrée est-elle unique ?

d) Notons α l'élément $(0, 1)$ de A. Nous savons (*cf. c*) que tout élément z de $A[\sqrt{d}]$ s'écrit de manière unique sous la forme $z = x + \alpha y$. Nous appellerons *conjugué* de z l'élément $\bar{z} = x - \alpha y$ et nous poserons $N(z) = z.\bar{z}$. Démontrer que $\bar{\bar{z}} = z$; $\overline{z + z'} = \bar{z} + \bar{z}'$, $\overline{z.z'} = \bar{z}.\bar{z}'$ et $N(z.z') = N(z).N(z')$, si z et z' sont deux éléments de $A[\sqrt{d}]$.

e) Démontrer que $A[\sqrt{d}]$ est intègre si et seulement si A est intègre et si $N(z) = 0$ implique $z = 0$. Démontrer que z est inversible dans $A[\sqrt{d}]$ si et seulement si $N(z)$ est inversible dans A et calculer alors l'inverse de z.

Solution *a*) L'addition définie ici munit $A \times A$ d'une structure de groupe abélien (*cf.* Q., Ch. 4, § IV, n° 79).

Soient (a, a'), (b, b'), (c, c') trois éléments de $A[\sqrt{d}]$; on a

$$[(a, a').(b, b')].(c, c') = (ab + da'b', ab' + ba').(c, c') =$$
$$= (abc + da'b'c + dab'c' + da'bc', abc' + da'b'c' + ab'c + a'bc) =$$
$$= (a, a')\,[bc + db'c', bc' + cb'] = (a, a').[(b, b').(c, c')]$$

ce qui montre que la multiplication de $A[\sqrt{d}]$ est associative. Par ailleurs, on voit directement sur la formule de définition que cette multiplication est commutative. Si (a, a'), (b, b'), (c, c') sont toujours des éléments de $A[\sqrt{d}]$, on a aussi

$$(a, a').[(b, b') + (c, c')] = (a, a').(b + c, b' + c')$$
$$= (ab + ac + da'b' + da'c', ab' + ac' + a'b + a'c)$$
$$= (ab + da'b', ab' + ba') + (ac + da'c', ac' + ca')$$
$$= (a, a').(b, b') + (a, a').(c, c'),$$

ce qui montre que la multiplication de $A[\sqrt{d}]$ est distributive à droite sur l'addition ; comme cette multiplication est commutative, elle est distributive sur l'addition. Ainsi, nous venons de démontrer que $A[\sqrt{d}]$ est un anneau commutatif. Observons maintenant que pour tout élément (a, a') de $A[\sqrt{d}]$, on a :

$$(a, a').(1, 0) = (a.1 + da'.0, a.0 + a'.1) = (a, a')$$

donc $(a, a').(1, 0) = (1, 0).(a, a') = (a, a')$ et $(1, 0)$ est élément unité de $A[\sqrt{d}]$.

b) Soit φ l'application de A dans A' définie en posant $\varphi(a) = (a, 0)$ pour tout élément a de A. Si a, a' sont deux éléments de A tels que $\varphi(a) = \varphi(a')$, on a $(a, 0) = (a', 0)$ donc $a = a'$, ce qui montre que φ est injective. Tout élément de A' est de la forme $(a, 0) = \varphi(a)$ donc φ est surjective. De plus φ est un homomorphisme d'anneaux car si a et b sont deux éléments de A, on a :

$$\varphi(a + b) = (a + b, 0) = (a, 0) + (b, 0) = \varphi(a) + \varphi(b),$$

et

$$\varphi(a.b) = (a.b, 0) = (a, 0).(b, 0) = \varphi(a).\varphi(b);$$

A' est donc un sous-anneau de $A[\sqrt{d}]$ isomorphe à A.

c) Soit (a, a') un élément de $A[\sqrt{d}]$; on a

$$(a, a') = (a, 0).(1, 0) + (a', 0).(0, 1) = (a, 0) + (a', 0).(0, 1),$$

mais dans $A[\sqrt{d}]$, un élément de la forme $(x, 0)$ est identifié avec x, donc $(a, a') = a + a'.(0, 1)$; supposons qu'il existe deux éléments a_1 et a_1' de A tels que $(a, a') = a_1 + a_1'.(0, 1)$; alors on aurait

$$(a, a') = (a_1, 0) + (a_1', 0).(0, 1) \quad \text{soit} \quad (a, a') = (a_1, 0) + (0, a_1') = (a_1, a_1')$$

d'où $a = a_1$ et $a' = a_1'$. On peut donc décomposer d'une manière et d'une seule, un élément z de A sous la forme $z = x + \alpha.y$ avec x et y dans A et $\alpha = (0, 1)$. Cherchons un élément (a, a') de $A[\sqrt{d}]$ tel que $(a, a')^2 = (d, 0)$, soit $(a^2 + da'^2, 2aa') = (d, 0)$; il faut résoudre le système

$$\begin{cases} a^2 + da'^2 = d \\ 2aa' = 0. \end{cases}$$

Ce système admet la solution $a = 0$, $a' = 1$ (soit $\alpha^2 = d$). Cette solution n'est pas unique en général (exemple : si $A = \mathbf{Z}/4\,\mathbf{Z}$ et $d = \bar{2}$, les éléments $(\bar{0}, \bar{1})$ et $(\bar{2}, \bar{1})$ sont des racines carrées de d).

d) Soit $z = x + \alpha.y$ un élément de $A[\sqrt{d}]$; alors $\bar{z} = x - \alpha y$ et $\bar{\bar{z}} = x + \alpha y = z$. Soient maintenant $z' = x' + \alpha.y'$ un autre élément de $A[\sqrt{d}]$, alors

$$z + z' = x + x' + \alpha.(y + y') \quad \text{donc} \quad \overline{z + z'} = x + x' - \alpha(y + y'),$$

mais

$$\bar{z} + \bar{z}' = x - \alpha y + x' - \alpha y' = x + x' - \alpha(y + y') \quad \text{d'où} \quad \overline{z + z'} = \bar{z} + \bar{z}'.$$

Calculons $z.z'$:

$$z.z' = (x + \alpha y)(x' + \alpha y') = xx' + \alpha(xy' + yx') + \alpha^2 yy',$$

mais $\alpha^2 = d$, donc $z.z' = xx' + dyy' + \alpha(xy' + yx')$ d'où

$$\overline{zz'} = xx' + dyy' - \alpha(xy' + yx').$$

Calculons maintenant $\bar{z}.\bar{z}'$:

$$\bar{z}.\bar{z}' = (x - \alpha y)(x' - \alpha y') = xx' - \alpha(xy' + yx') + \alpha^2 yy'$$
$$= xx' + dyy' - \alpha(xy' + yx')$$

d'où $\overline{z.z'} = \bar{z}.\bar{z}'$. On en déduit que

$$N(z.z') = z.z'.\overline{z.z'} = z.z'.\bar{z}.\bar{z}' = z.\bar{z}.z'.\bar{z}' = N(z).N(z').$$

e) Supposons $A[\sqrt{d}]$ intègre ; puisque A est considéré comme sous-anneau de $A[\sqrt{d}]$, A est intègre, de plus si z est un élément de $A[\sqrt{d}]$ tel que $N(z) = 0$, alors $z.z = 0$; comme $A[\sqrt{d}]$ est intègre on a $z = 0$ ou $z = 0$, si $\bar{z} = 0$ alors $\bar{\bar{z}} = \bar{0} = 0 = z$ donc $z = 0$.

Démontrons la réciproque. Soient z et z' deux éléments de $A[\sqrt{d}]$ tels que $z.z' = 0$ et $z \neq 0$; nous avons $N(z.z') = N(z).N(z') = N(0) = 0$. Or, $N(z)$ et $N(z')$ sont des éléments de A qui est intègre donc $N(z)$ ou $N(z')$ est nul ; mais $z \neq 0$ donc $N(z) \neq 0$ par suite $N(z') = 0$ donc $z' = 0$ ce qui achève de montrer que $A[\sqrt{d}]$ est un anneau sans diviseur de 0. Nous avons vu que $A[\sqrt{d}]$ est commutatif, donc c'est un anneau intègre.

Soit z un élément inversible de $A[\sqrt{d}]$ et z^{-1} son inverse ; nous avons

$$N(z.z^{-1}) = N(z).N(z^{-1}) = N(1) = 1$$

donc $N(z)$ est inversible dans A. Réciproquement, soit $z = x + \alpha.y$ un élément de $A[\sqrt{d}]$ tel que $N(z) = x^2 - \alpha^2 y^2$ soit inversible ; désignons par u l'inverse de $N(z)$ dans A, alors on a : $N(z).u = 1 = z.\bar{z}.u$ donc z est inversible, d'inverse

$$\bar{z}.u = (x - \alpha y).(x^2 - \alpha^2 y^2)^{-1}.$$

3.7 Soient A un anneau d'intégrité unitaire et $A^* = A - \{0\}$. Nous dirons que A est un *anneau euclidien* s'il existe une application f de A^* dans N telle que :

E.1. Pour tout couple (x, y) d'éléments de A^*, $f(x.y) \geqslant f(y)$.

E.2. Pour tout couple (a, b) d'éléments de A^*, il existe des éléments q et r de A tels que : $a = bq + r$ et $(r = 0$ ou $f(r) < f(b))$.

1) Démontrer que si l'application f vérifie la condition :

$$(\forall (x, y) \in A^* \times A^*) \quad [x \neq y \Rightarrow f(x - y) \leqslant \mathrm{Sup}\,(f(x), f(y))]$$

alors, pour tout couple (a, b) d'éléments de A^*, le couple (q, r) défini en *E*.2 est unique.

2) Soit I un idéal de A différent de $\{0\}$.

a) Démontrer qu'il existe un élément a de I tel que pour tout élément x de $I - \{0\}$ on ait $f(a) \leqslant f(x)$.

b) Démontrer que l'idéal I est engendré par l'élément a.

Solution 1) Soient a, b deux éléments de A^* et (q, r) et (q', r') deux couples tels que

$$a = bq + r \quad \text{et} \quad (r = 0 \quad \text{ou} \quad f(r) < f(b)) \tag{1}$$

$$a = bq' + r' \quad \text{et} \quad (r' = 0 \quad \text{ou} \quad f(r') < f(b)). \tag{2}$$

En faisant la différence membre à membre des égalités (1) et (2) on obtient $0 = b(q - q') + r - r'$ soit $b(q - q') = r' - r$. Si $q = q'$ alors $r = r'$; si $r = r'$, comme A est un anneau intègre et b est non nul, $q = q'$. Supposons donc $q \neq q'$ et $r \neq r'$ et distinguons deux cas :

α) Si $r = 0$ ou $r' = 0$. Si $r = 0$, $r' \neq 0$ et on a $b(q - q') = r'$ d'où

$$f(b(q - q')) = f(r')$$

et par hypothèse $f(r') < f(b)$ mais d'après $E.1$, $f(b(q - q')) \geqslant f(b)$ ce qui est impossible. Le raisonnement est le même si $r' = 0$.

β) Si $r \neq 0$ et $r' \neq 0$. On a $b(q - q') = r' - r$ donc $f(b(q - q')) = f(r' - r)$ de plus, d'après $E.1$, on a $f(b(q - q')) \geqslant f(b)$. D'autre part, d'après l'hypothèse, on a $f(r' - r) \leqslant \operatorname{Sup}[f(r), f(r')]$ or $f(r') < f(b)$ et $f(r) < f(b)$ donc $f(r' - r) < f(b)$ ce qui est encore impossible. Par conséquent, pour tout couple (a, b) d'éléments de A^*, le couple (q, r) défini en $E.2$ est unique.

2) *a*) Soit X le sous-ensemble de N formé des éléments $f(x)$ pour tous les x appartenant à $I - \{0\}$; X est non vide car $I \neq \{0\}$, X admet donc un plus petit élément, par suite il existe un élément a de I tel que $f(a)$ soit le plus petit élément de X et pour tout élément x de I on a $f(a) \leqslant f(x)$.

b) Soient x un élément de I et a l'élément de I défini ci-dessus ; alors, il existe un couple (q, r) tel que

$$x = aq + r \quad \text{et} \quad (r = 0 \quad \text{ou} \quad f(r) < f(a)).$$

Comme I est un idéal, les éléments aq et $r = x - aq$ lui appartiennent, par suite $f(r) \geqslant f(a)$ et on ne peut avoir $f(r) < f(a)$, donc $r = 0$ et $x = aq$. Ceci démontre que tout élément de I est le produit d'un élément de A par a donc a engendre I.

3.8 Soient A un anneau commutatif et I un idéal de A. Soient A/I l'anneau quotient de A par l'idéal I et π la surjection canonique de A sur A/I. Si x est un élément de A, nous désignerons par $\dot{x}$ sa classe dans A/I.

1) Soit J un idéal de A contenant I. Démontrer que $\pi(J)$ est un idéal de A/I. Soit $\tilde{J}$ un idéal de A/I. Démontrer que $\pi^{-1}(\tilde{J})$ est un idéal de A contenant I.

2) Désignons par $\mathscr{I}(A, I)$ l'ensemble des idéaux de A contenant l'idéal I et par $\mathscr{I}(A/I)$ l'ensemble de tous les idéaux de A/I et ordonnons ces ensembles par l'inclusion. Démontrer que l'application θ de $\mathscr{I}(A, I)$ dans $\mathscr{I}(A/I)$ définie par $\theta(J) = \pi(J)$ pour tout élément J de $\mathscr{I}(A, I)$, est une bijection croissante, et que θ^{-1} est aussi une application croissante.

3) Démontrer qu'un anneau commutatif et unitaire B est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et B.

4) Déduire de ce qui précède qu'un idéal I de A est maximal si et seulement si A/I est un corps.

Solution 1) Soient $\bar{x}$ et $\bar{y}$ deux éléments de $\pi(J)$; il existe deux éléments x et y de J tels que $\pi(x) = \bar{x}$, $\pi(y) = \bar{y}$ et comme π est un homomorphisme d'anneaux, $\bar{x} - \bar{y} = \pi(x) - \pi(y) = \pi(x - y)$, or J est un idéal donc

$$x - y \in J \qquad \text{et} \qquad \bar{x} - \bar{y} \in \pi(J)\,.$$

Soient $\bar{x}$ un élément de $\pi(J)$ et a un élément de A/I ; il existe un élément x de J tel que $\pi(x) = \bar{x}$ et, comme π est une application surjective, il existe un élément a de A tel que $\pi(a) = \bar{a}$; nous avons $\bar{a}.\bar{x} = \pi(a)\,\pi(x) = \pi(ax)$ mais ax appartient à J donc $\bar{a}\bar{x}$ est un élément de $\pi(J)$ et $\pi(J)$ est un idéal de A/I.

Soit $\tilde{J}$ un idéal de A/I et soient x et y deux éléments de $\pi^{-1}(\tilde{J})$, alors $\pi(x)$ et $\pi(y)$ appartiennent à $\tilde{J}$; nous avons $\pi(x - y) = \pi(x) - \pi(y)$ et comme $\tilde{J}$ est un idéal, $\pi(x - y)$ appartient à $\tilde{J}$ si bien que $x - y \in \pi^{-1}(\tilde{J})$.

Soient x un élément de $\pi^{-1}(\tilde{J})$ et a un élément de A ; nous avons

$$\pi(ax) = \pi(a).\pi(x)$$

et $\pi(x)$ appartient à l'idéal $\tilde{J}$ donc $\pi(ax) \in \tilde{J}$ et $ax \in \pi^{-1}(\tilde{J})$ donc $\pi^{-1}(\tilde{J})$ est un idéal de A. Soit x un élément de I, alors $\pi(x) = \bar{0}$ donc $\pi(x) \in \tilde{J}$ par suite $x \in \pi^{-1}(\tilde{J})$ ce qui montre que $\pi^{-1}(\tilde{J})$ contient I.

2) Démontrons que l'application θ est surjective ; soit $\tilde{J}$ un idéal de A/I, alors $\pi^{-1}(\tilde{J})$ est un idéal de A contenant I et $\theta(\pi^{-1}(\tilde{J})) = \pi(\pi^{-1}(\tilde{J})) = \tilde{J}$ car π est une application surjective (*cf.* exercice 1.2). Démontrons maintenant que θ est injective ; soient J et J' deux idéaux de A contenant I tels que

$$\theta(J) = \theta(J')\,;$$

alors on a $\pi(J) = \pi(J')$; soit x un élément de J, alors $\pi(x) \in \pi(J)$ donc $\pi(x) \in \pi(J')$ par suite il existe un élément y de J' tel que $\pi(x) = \pi(y)$ donc $\pi(x - y) = \bar{0}$ c'est-à-dire que $x - y \in I$ et comme $I \subset J'$, $x - y$ appartient à J', mais $y \in J'$ donc $x \in J'$ d'où $J \subset J'$. Nous démontrerions de même

que $J' \subset J$. θ est donc une bijection de $\mathscr{I}(A, I)$ sur $\mathscr{I}(A/I)$. La bijection réciproque θ^{-1} est définie par $\theta^{-1}(\tilde{J}) = \pi^{-1}(\tilde{J})$ pour tout élément $\tilde{J}$ de $\mathscr{I}(A/I)$.

Soient J et J' deux idéaux de A contenant I et tels que $J \subset J'$; alors

$$\theta(J) = \pi(J) \subset \pi(J') = \theta(J')$$

donc θ est une application croissante. Soient $\tilde{J}$ et $\tilde{J}'$ deux idéaux de A/I tels que $\tilde{J} \subset \tilde{J}'$, alors $\theta^{-1}(\tilde{J}) = \pi^{-1}(\tilde{J}) \subset \pi^{-1}(\tilde{J}') = \theta^{-1}(\tilde{J}')$, donc θ^{-1} est aussi croissante.

3) Soit I un idéal d'un corps B ; si $I \neq \{0\}$ il existe un élément non nul x dans I, donc x est inversible et $x^{-1}.x = 1_B$ appartient à I ; soit alors b un élément de B, comme I est un idéal, $b = b.1_B$ appartient à B, par suite $I = B$ et nous venons de démontrer que les seuls idéaux d'un corps B sont $\{0\}$ et B. Supposons maintenant que les seuls idéaux de B soient $\{0\}$ et B. Soit x un élément non nul de B ; alors, l'ensemble des éléments de la forme $b.x$ où $b \in B$ est un idéal, soit $B.x$, de B ; en effet si $b.x$ et $b'.x$ sont deux éléments de $B.x$, alors $b.x - b'.x = (b - b').x$ donc $b.x - b'x$ appartient à $B.x$, d'autre part, si $b.x$ est un élément de $B.x$ et b' un élément de B, alors

$$b'.(b.x) = (b'.b).x$$

donc $b'.(b.x)$ appartient à $B.x$. L'idéal $B.x$ n'est pas réduit à $\{0\}$ car il contient l'élément non nul $x = 1_B.x$, donc $B.x = B$ et $1_B \in B.x$ par suite il existe un élément x' de B tel que $1_B = x'.x$. Comme l'anneau B est commutatif, x' est l'inverse de x ; tout élément non nul de B admet donc un inverse, par suite B est un corps.

4) Soit I un idéal de A ; si I est maximal, les seuls idéaux de A contenant I sont I et A, donc A/I n'a que deux idéaux $\{0\}$ et A/I donc A/I est un corps. Réciproquement supposons que A/I soit un corps ; si J est un idéal de A tel que $I \subset J$ et $J \neq A$, alors (θ étant injective) $\theta(J) \neq \theta(A)$ or $\theta(A) = A/I$ donc $\theta(J) = \{\bar{0}\}$ d'où $J = I$, ce qui prouve que I est un idéal maximal.

3.9

Cet exercice fournit une autre démonstration du résultat obtenu à l'exercice 3.8.

Soient A un anneau commutatif et unitaire et I un idéal de A ; on désigne par A/I l'anneau quotient de A par I, et pour tout élément x de A, la classe de x dans A/I sera notée $\dot{x}$.

1) Supposons que A/I soit un corps et soit J un idéal de A tel que $I \subset J$ et $I \neq J$. Démontrer que l'élément unité 1 de A appartient à J et en déduire que l'idéal J est maximal.

2) Supposons I maximal ; soit x un élément de A qui n'appartient pas à I. Démontrer que l'ensemble $I + Ax$ des éléments de la forme $u + ax$ avec $u \in I$ et $a \in A$ est un idéal de A contenant strictement I. En déduire que A/I est un corps.

Solution 1) Puisque J contient strictement I, il existe un élément x de J qui n'appartient pas à I ; alors $\dot{x} \neq \dot{0}$ donc $\dot{x}$ est inversible dans A/I par suite il existe un élément y de A tel que $\dot{x}\dot{y} = \dot{1}$ soit $\widehat{xy} = \dot{1}$, ce qui signifie que $xy - 1 \in I$, or $I \subset J$ donc l'élément $g = xy - 1$ appartient à J ; par ailleurs $x \in J$ et J est un idéal donc $xy \in J$ par suite $1 = xy - g$ appartient à J. Puisque $1 \in J$, J est l'anneau A tout entier donc tout idéal contenant strictement I est l'anneau A si bien que I est un idéal maximal.

2) Soient $z = u + a.x$ et $z' = u' + a'.x$ deux éléments de $I + Ax$ et a'' un élément de A, alors $z - z' = u - u' + (a - a').x$ donc $z - z' \in I + A.x$ et $a''.z = a''u + (a''a).x$, or I est un idéal donc $a''.u \in I$ et $a''.z \in I + Ax$; il en résulte (*cf.* Q., Ch. 5, § II, n° 94), que $I + Ax$ est un idéal de A. Il est clair que $I \subset I + Ax$ de plus, x n'appartient pas à I et appartient à $I + A.x$ ($x = 0 + 1.x$) donc $I + Ax$ contient I strictement. Nous savons que A/I est un anneau commutatif et unitaire ; pour démontrer que A/I est un corps il suffit donc de montrer que tout élément non nul de A/I est inversible ; soit donc $\dot{x}$ un élément non nul de A/I, alors si x est un représentant de $\dot{x}$ nous savons que $I + Ax$ est un idéal de A contenant strictement I, or I est maximal donc $I + Ax = A$ et $1 \in I + Ax$ donc il existe un élément u de I et un élément a de A tels que $1 = u + ax$; alors $\dot{1} = \dot{u} + \widehat{ax} = \dot{u} + \dot{a}\dot{x}$, mais $u \in I$ donc $\dot{u} = 0$ par suite $\dot{1} = \dot{a}.\dot{x}$. Comme A/I est commutatif, ceci prouve que $\dot{x}$ est inversible dans A/I ; A/I est donc un corps.

3.10 1) Soient p un nombre premier et q un entier tels que $0 < q < p$. Démontrer que C_p^q est divisible par p.

2) Démontrer que dans un anneau commutatif A de caractéristique p, pour toute suite finie $a_1, a_2, \ldots, a_k$ d'éléments de A, on a

$$(a_1 + a_2 + \cdots + a_k)^p = a_1^p + a_2^p + \cdots + a_k^p .$$

En déduire que pour tout entier positif k, on a $k^p \equiv k \pmod{p}$.

Solution 1) Nous avons

$$C_p^q = \frac{p(p-1)\ldots(p-q+1)}{q(q-1)\ldots 2.1} ;$$

$q(q-1)\ldots 2.1$ divise $p(p-1)\ldots(p-q+1)$ et est premier avec p (car q est différent de 0 et de p) donc $q(q-1)\ldots 2.1$ divise $(p-1)(p-2)\ldots(p-q+1)$ d'où

$$C_p^q = p.m$$

avec

$$m = \frac{(p-1)(p-2)\dots(p-q+1)}{q(q-1)\dots 2.1} \quad \text{et} \quad m \in \mathbf{N}$$

2) Nous démontrerons le résultat par récurrence sur la longueur k de la suite ; la formule est évidente si $k = 1$; démontrons-la pour $k = 2$: si a_1, a_2 sont deux éléments de A, on a d'après la formule du binôme

$$(a_1 + a_2)^p = a_1^p + \left(\sum_{q=1}^{p-1} C_p^q a_1^q a_2^{p-q}\right) + a_2^p ,$$

or A est de caractéristique p donc, pour tout entier q compris entre 1 et $p - 1$,

$$C_p^q a_1^q a_2^{q-q} = 0$$

si bien que

$$(a_1 + a_2)^p = a_1^p + a_2^p .$$

Supposons maintenant la formule vraie lorsque la longueur de la suite est $k - 1$ (avec $k > 1$) et soit $a_1, a_2, \dots, a_k$ une suite de longueur k d'éléments de A ; alors on a

$$(a_1 + a_2 + \cdots + a_k)^p = [(a_1 + a_2 + \cdots + a_{k-1}) + a_k]^p$$

d'où en appliquant la formule précédente pour les suites de longueur 2 :

$$(a_1 + a_2 + \cdots + a_k)^p = (a_1 + a_2 + \cdots + a_{k-1})^p + a_k^p ;$$

or par hypothèse de récurrence, on a :

$$(a_1 + a_2 + \cdots + a_{k-1})^p = a_1^p + a_2^p + \cdots + a_{k-1}^p$$

donc

$$(a_1 + a_2 + \cdots + a_k)^p = a_1^p + a_2^p + \cdots + a_k^p .$$

Considérons l'anneau $\mathbf{Z}/p\mathbf{Z}$; il est de caractéristique p. Si $k \in \mathbf{N}$, nous avons $\dot{k} = \dot{1} + \dot{1} + \cdots + \dot{1}$ (k termes) donc en appliquant le résultat ci-dessus,

$$\dot{k}^p = (\dot{1} + \dot{1} + \cdots + \dot{1})^p = \dot{1}^p + \dot{1}^p + \cdots + \dot{1}^p = \dot{1} + \dot{1} + \cdots + \dot{1} = \dot{k}$$

soit $\dot{k}^p = \dot{k}$ ou $k^p \equiv k \pmod{p}$.

3.11 Démontrer que l'anneau $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est un nombre premier.

Solution Supposons n non premier ; alors il existe deux entiers p et q distincts de 1 et de n tels que $n = p.q$, d'où en passant aux classes modulo n, $\dot{n} = \dot{p}.\dot{q}$, or $\dot{n} = \dot{0}$, $\dot{p} \neq \dot{0}$ et $\dot{q} \neq \dot{0}$, ce qui prouve que $\mathbf{Z}/n\mathbf{Z}$ a des diviseurs de $\dot{0}$ donc n'est pas un corps, par suite, si $\mathbf{Z}/n\mathbf{Z}$ est un corps, n est premier.

Réciproquement, supposons n premier. $\mathbf{Z}/n\mathbf{Z}$ est un anneau commutatif et unitaire, pour montrer que c'est un corps il suffit donc de montrer que chacun de ses éléments non nuls est inversible. Soit donc $\dot{m}$ un élément non nul de $\mathbf{Z}/n\mathbf{Z}$, alors m n'est pas un multiple de n et comme n est un nombre premier, m et n sont premiers entre eux ; il existe donc deux entiers u et v tels que $um + nv = 1$ (Théorème de BEZOUT, *cf.* Q., Ch. 5, § III, n° 99), d'où en passant aux classes modulo n, $\dot{u}\dot{m} + \dot{n}\dot{v} = \dot{1}$, mais $\dot{n} = \dot{0}$ donc $\dot{u}.\dot{m} = \dot{1}$ si bien que m est inversible. $\mathbf{Z}/n\mathbf{Z}$ est donc un corps.

3.12 Soit A un anneau fini, sans diviseur de zéro, non réduit à $\{0\}$. Montrer que A est un corps. (On utilisera les résultats et les méthodes de l'exercice 1.15.)

Solution Soit a un élément non nul de A ; désignons par γ_a et δ_a la translation à gauche et la translation à droite dans A, relatives à a. L'application γ_a est injective car si x, x' sont deux éléments de A tels que $\gamma_a(x) = \gamma_a(x')$, on a $ax = ax'$ donc $a(x - x') = 0$ et comme $a \neq 0$ et A n'a pas de diviseur de zéro, $x - x' = 0$ donc $x = x'$. Comme A est fini, γ_a est aussi surjective donc bijective (*cf.* Q., Ch 2, § II, n° 31). On démontre de la même manière que δ_a est bijective. γ_a et δ_a étant des bijections, d'après le résultat b de l'exercice 1.15 (appliqué à l'ensemble $E = A - \{0\}$, muni de la multiplication induite par celle de A) A est unitaire ; en appliquant alors le résultat c de l'exercice 1.15 à E, on voit que tout élément non nul de A est inversible, donc A est un corps.

3.13 Tous les corps considérés dans cet exercice sont commutatifs. Soient A un anneau commutatif intègre, Q_A son corps des fractions et π l'injection canonique de A dans Q_A. Soit K un corps et soit f un homomorphisme d'anneaux injectif de A dans K.

1) Soit (x, y) un représentant d'un élément q de Q_A ($x \in A$, $y \in A$ et $y \neq 0$). Démontrer que l'élément $f(y)$ est inversible dans K et que $f(x).[f(y)]^{-1}$ ne dépend que de q et non du choix de (x, y).

2) Montrer qu'il existe un homomorphisme de corps φ de Q_A dans K, et un seul, tel que $f = \varphi \circ \pi$.

3) Soient Q un corps et σ un homomorphisme d'anneaux injectif de A dans Q. Supposons que pour tout corps K et tout homomorphisme injectif g de A dans K, il existe un homomorphisme de corps ψ de Q dans K, et un seul, tel que $g = \psi \circ \sigma$.

En utilisant les propriétés des corps Q_A et Q démontrer qu'il existe un homomorphisme de corps θ de Q_A dans Q et un homomorphisme de corps θ' de Q dans Q_A tels que $\theta' \circ \theta = \mathrm{Id}\, Q_A$ et $\theta \circ \theta' = \mathrm{Id}\, Q$. En déduire que les corps Q et Q_A sont isomorphes.

Solution 1) Puisque f est injective et y non nul, $f(y)$ est un élément non nul de K donc est inversible. Soient (x, y) et (x', y') deux représentants d'un élément q de Q_A ; alors on a $xy' = yx'$; or f est un homomorphisme d'anneaux donc $f(x)f(y') = f(y)f(x')$ mais $f(y)$ et $f(y')$ sont inversibles donc

$$f(x)\,[f(y)]^{-1} = f(x')\,[f(y')]^{-1}\,.$$

2) Soit q un élément de Q_A ; si (x, y) est un représentant de q, nous avons vu que $f(x)\,[f(y)]^{-1}$ ne dépend que de q ; posons $\varphi(q) = f(x)\,[f(y)]^{-1}$, ceci définit une application φ de Q_A dans K. Soient q et q' deux éléments de Q_A et (x, y) et (x', y') des représentants de q et q' respectivement ; alors $(xy' + yx', yy')$ et (xx', yy') sont des représentants de $q + q'$ et qq' respectivement. Nous avons donc $\varphi(q + q') = f(xy' + yx')\,[f(yy')]^{-1}$; or f est un homomorphisme d'anneaux donc

$$\begin{aligned}(xy' + yx')\,[f(yy')]^{-1} &= (f(x)f(y') + f(y)f(x'))\,[f(yy')]^{-1} = \\ &= f(x)f(y')\,[f(y')]^{-1}.[f(y)]^{-1} + f(y).f(x')\,[f(y')]^{-1}\,[f(y)]^{-1} \\ &= f(x)\,[f(y)]^{-1} + f(x').[f(y')]^{-1} = \varphi(q) + \varphi(q')\,;\end{aligned}$$

par ailleurs,

$$\begin{aligned}\varphi(qq') = f(xx')\,[f(yy')]^{-1} &= f(x).f(x')\,[f(y')]^{-1}\,[f(y)]^{-1} = \\ &= (f(x).[f(y)]^{-1}).(f(x').[f(y')]^{-1}) = \varphi(q)\,\varphi(q')\end{aligned}$$

φ est donc un homomorphisme de corps de Q_A dans K ; de plus si x est un élément de A alors $\pi(x)$ admet $(x, 1)$ pour représentant donc

$$\varphi(\pi(x)) = f(x)\,[f(1)]^{-1} = f(x)$$

et comme ceci est vrai pour tout élément x de A, $f = \varphi \circ \pi$. Soit maintenant φ' un homomorphisme de Q_A dans K tel que $\varphi' \circ \pi = f$; soit q un élément de Q_A et soit (x, y) un représentant de q ; $(x, 1)$ est un représentant de l'élément $\pi(x)$ et $(1, y)$ est un représentant de l'élément $[\pi(y)]^{-1}$, nous avons donc $q = \pi(x)\,[\pi(y)]^{-1}$, donc

$$\begin{aligned}\varphi'(q) = \varphi'(\pi(x)\,[\pi(y)]^{-1}) &= \varphi'(\pi(x))\,\varphi'([\pi(y)]^{-1}) = \\ &= \varphi'(\pi(x))\,[\varphi'(\pi(y))]^{-1} = f(x)\,[f(y)]^{-1} = \varphi(q)\,;\end{aligned}$$

comme $\varphi(q) = \varphi'(q)$ pour chaque élément q de Q_A, $\varphi' = \varphi$ ce qui démontre l'unicité de φ.

3) La propriété du corps des fractions Q_A de A nous montre l'existence d'un homomorphisme θ de Q_A dans Q, et d'un seul, tel que $\sigma = \theta \circ \pi$. De même la propriété du corps Q nous montre l'existence d'un homomorphisme θ' de Q dans Q_A et d'un seul, tel que $\pi = \theta' \circ \sigma$. Appliquons la propriété du corps Q_A en prenant comme corps K le corps Q_A lui-même et comme application f, l'application π ; alors il existe un homomorphisme de corps φ de Q_A dans Q_A et un seul tel que $\pi = \varphi \circ \pi$; comme Id Q_A vérifie cette relation le seul homomorphisme φ tel que $\pi = \varphi \circ \pi$ est Id Q_A ; nous avons $\pi = \theta' \circ \sigma = (\theta' \circ \theta) \circ \pi$ donc $\theta' \circ \theta = \text{Id } Q_A$. En faisant le même raisonnement avec le corps Q on démontre que $\theta \circ \theta' = \text{Id } Q$. Par suite θ est un isomorphisme du corps Q_A sur le corps Q.

3.14 Soient a et b deux nombres premiers entre eux et u et v deux entiers tels que $au + bv = 1$.

1) Démontrer que si u' et v' sont deux entiers tels que $au' + bv' = 1$, il existe un entier k tel que $u' = u - kb$ et $v' = v + ka$.

2) Démontrer que si $a > 2$ et $b > 2$, il existe un couple unique (u_0, v_0) tel que $au_0 + bv_0 = 1$ et $|u_0| < b/2$ et $|v_0| < a/2$. Etudier le cas où $a = 2$ ou $b = 2$.

Solution 1) Nous avons $au + bv = 1$ et $au' + bv' = 1$ d'où par différence

$$a(u - u') + b(v - v') = 0$$

soit $a(u - u') = b(v' - v)$. Le nombre a divise $b(v' - v)$ et est premier à b donc a divise $v' - v$ et il existe un entier k tel que $v' - v = ka$, d'où

$$a(u - u') = bka$$

soit $u - u' = bk$ par suite $u' = u - kb$ et $v' = v + ka$.

2) Puisque a et b sont positifs, u ou v est positif sinon $au + bv$ serait négatif, ce qui est impossible. Supposons donc u positif. Nous allons chercher u_0 et v_0 sous la forme $u_0 = u - kb$, $v_0 = v + ka$.

Considérons l'ensemble A des entiers n tels que $nb \geqslant u$; cet ensemble n'est pas vide, en effet, b étant supérieur à 2, $ub \geqslant u$ donc u appartient à A. Mais tout sous-ensemble A non vide de N admet un plus petit élément k' et nous avons $(k' - 1)\, b < u \leqslant k'\, b$; par ailleurs on a

$$u - (k' - 1)\, b \leqslant \frac{b}{2} \quad \text{ou} \quad k'\, b - u \leqslant \frac{b}{2},$$

en effet si $u - (k' - 1)\, b > \frac{b}{2}$ et $k'\, b - u > \frac{b}{2}$ alors, en ajoutant membre à membre ces deux inégalités, on obtient $b > b$ ce qui est impossible. D'autre part, on ne peut avoir $u - (k' - 1)\, b = \frac{b}{2}$ ou $k'\, b - u = \frac{b}{2}$; supposons en effet que u soit de la forme $u = \frac{b}{2} + \lambda b$, alors $a\left(\frac{b}{2} + \lambda b\right) + bv = 1$ soit

$$\frac{ab}{2} + \lambda ab + bv = 1 \qquad \text{ou} \qquad ab(1 + 2\lambda) + 2\, bv = 2$$

ce qui est impossible car b diviserait 2. De tout ceci il résulte que l'une des inégalités $u - (k' - 1)\, b < \frac{b}{2}$ ou $k'\, b - u < \frac{b}{2}$ est satisfaite, donc il existe un entier k tel que $| u - kb | < \frac{b}{2}$. Posons $u_0 = u - kb$ et $v_0 = v + ka$; alors $| u_0 | < \frac{b}{2}$ et nous allons montrer que le couple (u_0, v_0) satisfait aux conditions de l'énoncé.

Nous avons $au_0 + bv_0 = 1$ donc $1 - bv_0 = au_0$ d'où $| 1 - bv_0 | < \frac{ab}{2}$ soit

$$1 - \frac{ab}{2} < bv_0 < \frac{ab}{2} + 1\,, \qquad \text{d'où} \qquad -\frac{ab}{2} < bv_0 < \frac{ab}{2} + 1$$

Considérons l'inégalité $bv_0 < \frac{ab}{2} + 1$, elle donne $v_0 < \frac{a}{2} + \frac{1}{b}$ et comme $b > 2$, $v_0 < \frac{a}{2} + \frac{1}{3}$;

— si a est impair et $a = 2a' + 1$, on a $v_0 < a' + \frac{1}{2} + \frac{1}{3}$ soit $v_0 < a' + \frac{5}{6}$; v_0 et a' étant des nombres entiers, on en déduit $v_0 \leqslant a'$ mais $a' < \frac{a}{2}$ donc $v_0 < \frac{a}{2}$;

— si a est pair et $a = 2a'$, on a $v_0 < a' + \frac{1}{3}$ soit $v_0 \leqslant a'$ mais nous ne pouvons avoir $v_0 = a'$ car on aurait $au_0 + bv_0 = 2a'\, u_0 + ba' = 1$ or $a > 2$ donc $a' > 1$ soit $a' \geqslant 2$ et comme a' divise le premier membre, a' devrait diviser 1 ce qui est impossible.

Nous venons donc de démontrer que, dans tous les cas $v_0 < \frac{a}{2}$; comme $-\frac{ab}{2} < bv_0$, nous avons $| v_0 | < \frac{a}{2}$. Il reste à démontrer l'unicité du couple (u_0, v_0) tel que $au_0 + bv_0 = 1$, $| u_0 | < \frac{b}{2}$ et $| v_0 | < \frac{a}{2}$. Soit donc un couple (u_1, v_1) tel que $au_1 + bv_1 = 1$; d'après le résultat de la question 1, il existe un entier λ tel que $u_1 = u_0 - \lambda b$ et $v_1 = v_0 + \lambda a$; il nous suffira donc de

montrer que si $\lambda \neq 0$, l'une des inégalités $|u_1| < \frac{b}{2}$ ou $|v_1| < \frac{a}{2}$ n'est pas satisfaite ; or, si $\lambda \neq 0$, $|\lambda| \geqslant 1$ et on a $|u_0 - u_1| = |\lambda| b$ donc $|u_0 - u_1| \geqslant b$ par suite on ne peut avoir $|u_1| < \frac{b}{2}$ sinon on aurait

$$|u_0 - u_1| \leqslant |u_0| + |u_1| < b$$

ce qui n'est pas. Le couple (u_0, v_0) trouvé précédemment est donc unique.

Examinons maintenant le cas où $a = 2$ ou $b = 2$. Par exemple, si $a = 2$ alors b est un nombre impair car a et b sont premiers entre eux donc $b = 2b' + 1$, ceci n'est autre que l'égalité de BEZOUT $2(-b') + (1)\, b = 1$ avec $u_0 = -b'$ et $v_0 = 1$, nous avons donc $|u_0| < \frac{b}{2}$ et $|v_0| = \frac{a}{2}$. Le cas où $b = 2$ se traite de manière analogue.

3.15 Le but de cet exercice est de déterminer tous les triplets (x, y, z) d'entiers rationnels vérifiant l'équation :

$$x^2 + y^2 = z^2 . \qquad \text{(E)}$$

1) Soit (x', y', z') une solution de l'équation (E). Démontrer qu'il existe un entier d tel que $x' = dx$, $y' = dy$, $z' = dz$ et (x, y, z) premiers deux à deux, (x, y, z) étant une solution de l'équation (E).

2) Soit (x, y, z) une solution de (E) telle que (x, y, z) soient premiers deux à deux. Démontrer que x et y sont de parités différentes.

3) Supposons x pair et y impair. Démontrer qu'il existe deux entiers u et v tels que $y = u - v$, $z = u + v$ et u et v sont premiers entre eux.

4) Démontrer que u et v sont les carrés de deux entiers premiers entre eux. Donner la forme de la solution (x, y, z). En déduire toutes les solutions de l'équation (E).

Solution 1) Soit (x', y', z') une solution de (E) avec $x' \neq 0$, $y' \neq 0$, $z' \neq 0$ et soit d le p. g. c. d. de x', y', z'. Alors $x' = dx$, $y' = dy$, $z' = dz$ et (x, y, z) sont premiers entre eux dans leur ensemble. On a $d^2x^2 + d^2y^2 = d^2z^2$ donc $x^2 + y^2 = z^2$; de plus, si deux des nombres x, y, z admettent un diviseur commun δ différent de $+1$ et -1, alors δ^2 divise le carré du troisième donc δ divise le troisième nombre et δ est un diviseur commun à x, y, z ce qui est impossible. Il en résulte que x, y et z sont premiers deux à deux.

2) Soit (x, y, z) une solution de (E) telle que x, y, z soient premiers deux à deux. On a $x^2 + y^2 = z^2$; il est impossible que x et y soient pairs car 2 serait

diviseur commun à x et y. Supposons que x et y soient impairs et posons $x = 2p + 1$, $y = 2q + 1$, alors $(2p + 1)^2 + (2q + 1)^2 = z^2$ soit

$$2[2(p^2 + q^2 + p + q) + 1] = z^2$$

par suite z^2 est pair donc z est pair, mais si l'on pose $z = 2r$ on obtient

$$2[2(p^2 + q^2 + p + q) + 1] = 4r^2 \quad \text{donc} \quad 2(p^2 + q^2 + p + q) + 1 = 2r^2$$

ce qui est impossible, donc x et y sont de parités différentes.

3) Les notations étant comme à la question précédente, supposons x pair et y impair. Nous avons $x^2 = z^2 - y^2$. Puisque x est pair et y impair, y^2 est impair donc z^2 et z sont impairs, or $x^2 = (z - y)(z + y)$ et $z - y$ et $z + y$ sont pairs donc si l'on pose $z - y = 2u$ et $z + y = 2v$, on obtient $y = u + v$, $z = u - v$ et les entiers u et v sont premiers entre eux car s'ils avaient un diviseur commun l différent de $+ 1$ et $- 1$, ce diviseur diviserait à la fois y et z ce qui est impossible.

4) Nous avons $x^2 = 4uv$; posons $x = 2x'$, il vient $x'^2 = uv$; soit p un diviseur premier de x', alors p^2 divise uv et comme u et v sont premiers entre eux, p^2 divise soit u, soit v. Ceci démontre que les décompositions en facteurs premiers de u et v ne comportent que des exposants pairs donc u et v sont des carrés. Posons $u = a^2$ et $v = b^2$; a et b sont premiers entre eux car si λ était un diviseur commun à a et b différent de $+ 1$ et $- 1$, λ^2 diviserait u et v ce qui est impossible. Nous avons donc $x = 2ab$, $y = a^2 - b^2$ et $z = a^2 + b^2$. Compte tenu du résultat de la question 1 on voit que les seuls triplets d'entiers rationnels tels que (x, y, z) soit solution de l'équation (E) et x soit pair, sont les triplets de la forme

$$x = 2dab\,, \quad y = d(a^2 - b^2)\,, \quad z = d(a^2 + b^2)$$

où d, a, b sont des entiers rationnels, a et b étant premiers entre eux.

3.16

Soient p et q deux nombres entiers premiers entre eux.

1) Montrer que, quels que soient les entiers y, z, il existe un entier x tel que

$$x \equiv y \pmod{p} \qquad \text{et} \qquad x \equiv z \pmod{q}\,.$$

Démontrer que toutes les solutions sont congrues modulo $n = p.q$.

2) Soit $(\dot{y}, \dot{z})$ un élément de $(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})$. Démontrer qu'il existe un élément unique $\dot{x}$ de $\mathbf{Z}/n\mathbf{Z}$ tel que, si x (resp. y, z) est un représentant de $\dot{x}$ (resp. $\dot{y}$, $\dot{z}$) alors

$$x \equiv y \pmod{p} \qquad \text{et} \qquad x \equiv z \pmod{q}\,.$$

3) Démontrer que l'application f de $(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})$ dans $\mathbf{Z}/n\mathbf{Z}$, qui à $(\dot{y}, \dot{z})$ fait correspondre l'élément $\dot{x}$ défini ci-dessus, est un isomorphisme de l'anneau produit $(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})$ sur l'anneau $\mathbf{Z}/n\mathbf{Z}$.

4) Soit x un entier ; démontrer que la classe de x modulo p (resp. q) ne dépend que de la classe de x modulo n. En déduire l'isomorphisme réciproque de f.

Solution 1) Puisque les nombres p et q sont premiers entre eux, il existe des entiers u et v tels que :

$$pu + qv = 1. \tag{1}$$

x doit vérifier $y - x = kp$, $z - x = k'q$ où k et k' sont des entiers, soit $y - z = kp - k'q$, mais d'après (1) nous avons

$$y - z = (y - z)\,pu + (y - z)\,qv$$

donc $k = (y - z)\,u$ et $k' = (y - z)\,v$, d'où

$$x = y - (y - z)\,up = z - (z - y)\,vq$$

donc $x \equiv y \pmod{p}$ et $x \equiv z \pmod{q}$.

Soit x' une autre solution, on a : $y - x' = k_1 p$ et $z - x' = k_1' q$ où k_1 et k_1' sont des entiers rationnels, alors

$$x - x' = (k_1 - k)\,p \qquad \text{et} \qquad x - x' = (k_1' - k')\,q$$

donc $x - x'$ est divisible par p et par q. Comme p et q sont premiers entre eux, $x - x'$ est divisible par $p.q = n$ donc $x \equiv x' \pmod{n}$.

2) Soit y (resp. z) un représentant de $\dot{y}$ (resp. $\dot{z}$). Nous savons qu'il existe un élément x de $\mathbf{Z}$ tel que $x \equiv y \pmod{p}$ et $x \equiv z \pmod{q}$ et toute autre solution est congrue à x modulo n ; donc $\dot{y}$ et $\dot{z}$ nous donnent un élément $\dot{x}$ de $\mathbf{Z}/n\mathbf{Z}$ et un seul, vérifiant la condition de l'énoncé ; en effet, si y', z' sont d'autres représentants de $\dot{y}$ et $\dot{z}$, on a $y' \equiv y \pmod{p}$, $z' \equiv z \pmod{q}$ donc $x \equiv y' \pmod{p}$ et $x \equiv z' \pmod{q}$, nous retrouvons donc les mêmes solutions.

3) Démontrons d'abord que f est un homomorphisme d'anneaux. Soient $(\dot{y}, \dot{z})$ et $(\dot{y}', \dot{z}')$ deux éléments de $(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})$ et soient y, z, y', z' des représentants de $\dot{y}, \dot{z}, \dot{y}', \dot{z}'$ respectivement. Soit x (resp. x') un entier tel que $x \equiv y \pmod{p}$ et $x \equiv z \pmod{q}$ (resp. $x' \equiv y' \pmod{p}$ et $x' \equiv z' \pmod{q}$) ; alors on a

$$f[(\dot{y}, \dot{z}) + (\dot{y}', \dot{z}')] = f[\dot{y} + \dot{y}', \dot{z} + \dot{z}'],$$

or les quatre congruences précédentes nous montrent que

$$x + x' \equiv y + y' \pmod{p}, \quad x + x' \equiv z + z' \pmod{q}$$

donc

$$f[\dot{y} + \dot{y}', \dot{z} + \dot{z}'] = \dot{\widehat{x + x'}} = \dot{x} + \dot{x}'$$

d'où

$$f[(\dot{y}, \dot{z}) + (\dot{y}', \dot{z}')] = f(\dot{y}, \dot{z}) + f(\dot{y}', \dot{z}').$$

Nous avons de même $xx' \equiv yy' (\text{mod } p)$ et $xx' \equiv zz' (\text{mod } q)$ donc

$$f[(\dot{y}, \dot{z}).(\dot{y}', \dot{z}')] = f[\dot{y}\dot{y}', \dot{z}\dot{z}'] = \dot{\widehat{xx'}} = \dot{x}\dot{x}' = f(\dot{y}, \dot{z}) f(\dot{y}', \dot{z}')$$

et f est bien un homomorphisme d'anneaux. Cet isomorphisme est injectif car si $(\dot{y}, \dot{z})$ et $(\dot{y}', \dot{z}')$ sont deux éléments de $(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})$ tels que

$$f(\dot{y}, \dot{z}) = f(\dot{y}', \dot{z}')$$

alors en posant $\dot{x} = f(\dot{y}, \dot{z})$ et en choisissant des représentants x, y, z, y', z' de $\dot{x}, \dot{y}, \dot{z}, \dot{y}', \dot{z}'$ respectivement, on a $x \equiv y (\text{mod } p)$, $x \equiv z (\text{mod } q)$, $x \equiv y' (\text{mod } p)$ et $x \equiv z' (\text{mod } q)$ donc $y \equiv y' (\text{mod } p)$ et $z \equiv z' (\text{mod } q)$ soit $\dot{y} = \dot{y}'$ et $\dot{z} = \dot{z}'$. Par ailleurs, nous avons $\text{card } (\mathbf{Z}/n\mathbf{Z}) = n = \text{card } [(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})]$ donc (*cf.* Q., Ch. 2, § II, n° 31) f est bijective, par suite f est un isomorphisme de $(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})$ sur $\mathbf{Z}/n\mathbf{Z}$.

4) Soient x et x' deux entiers congrus modulo n ; alors il existe un entier k tel que $x = x' + kn$, mais $n = p.q$ donc $x = x' + (kq)\, p$ d'où $x \equiv x' (\text{mod } p)$; de même $x = x' + (kp)\, q$ d'où $x \equiv x' (\text{mod } q)$. Soit $\dot{x}$ un élément de $\mathbf{Z}/n\mathbf{Z}$ et soit x un représentant de $\dot{x}$; désignons par $(\dot{x})_p$ (resp. $(\dot{x})_q$) la classe de x modulo p (resp. q). Nous venons de voir que ces classes ne dépendent que de $\dot{x}$ et non du représentant x de $\dot{x}$ choisi. Considérons l'application g de $\mathbf{Z}/n\mathbf{Z}$ dans $(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})$ définie en posant pour tout élément $\dot{x}$ de $\mathbf{Z}/n\mathbf{Z}$:

$$g(\dot{x}) = ((\dot{x})_p, (\dot{x})_q).$$

Calculons $f(g(\dot{x}))$ pour un élément $\dot{x}$ de $\mathbf{Z}/n\mathbf{Z}$; on a

$$f(g(\dot{x})) = f((\dot{x})_p, (\dot{x})) = \dot{x}$$

car si x est un représentant de $\dot{x}$, $x \equiv x (\text{mod } p)$ et $x \equiv x (\text{mod } q)$. Calculons $g[f(\dot{y}, \dot{z})]$ pour un élément $(\dot{y}, \dot{z})$ de $(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})$; soit x un entier tel que, si y et z sont des représentants de $\dot{y}$ et $\dot{z}$ on ait $x \equiv y (\text{mod } p)$ et $x \equiv z (\text{mod } q)$, alors $f(\dot{y}, \dot{z}) = \dot{x}$ et $g(f(\dot{y}, \dot{z})) = g(\dot{x})$ or $x \equiv y (\text{mod } p)$ donc $(\dot{x})_p = \dot{y}$, de même $x \equiv z (\text{mod } q)$ donc $(\dot{x})_q = \dot{z}$ par suite $g(f(\dot{x}, \dot{y})) = g(\dot{x}) = (\dot{y}, \dot{z})$. Ces deux résultats montrent que

$$g \circ f = \text{Id } [(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})] \quad \text{et} \quad f \circ g = \text{Id } \mathbf{Z}/n\mathbf{Z},$$

donc g est l'isomorphisme réciproque de f.

3.17 Soit A un anneau commutatif unitaire et $(I_n)_{n \in \mathbf{N}}$ une suite croissante (pour l'inclusion) d'idéaux de A.

1) Démontrer que $I = \bigcup_{n \in \mathbf{N}} I_n$ est un idéal de A.

2) Démontrer que dans un anneau principal A toute suite croissante d'idéaux est stationnaire. (Utiliser le fait que la réunion de cette famille est un idéal principal).

3) Démontrer que toute famille $\mathscr{I}$ non vide d'idéaux d'un anneau principal A possède un élément maximal.

Solution 1) Soient x et y deux éléments de I ; il existe alors deux entiers m et n tels que $x \in I_m$ et $y \in I_n$; supposons $n \geqslant m$, alors $I_m \subset I_n$ donc x et y appartiennent à I_n et comme I_n est un idéal, $x - y \in I_n$ par suite $x - y \in I$. Soient x un élément de I et a un élément de A, alors il existe un entier n tel que $x \in I_n$ et comme I_n est un idéal, $ax \in I_n$ d'où $ax \in I$. Ces deux résultats montrent (*cf.* Q., Ch. 5, § II, n° 94) que I est un idéal.

2) Soit $(I_n)_{n \in \mathbf{N}}$ une suite croissante d'idéaux de A ; alors $I = \bigcup_{n \in \mathbf{N}} I_n$ est un idéal de A donc il existe un élément a de A tel que $I = (a)$. Mais a appartient à I donc il existe un entier n tel que $a \in I_n$, alors $(a) \subset I_n$, mais $I_n \subset I$ donc $I_n = I$. Pour tout entier m tel que $m \geqslant n$ on a alors $I_n \subset I_m \subset I$ donc $I_n = I_m$ ce qui montre que la suite $(I_n)_{n \in \mathbf{N}}$ est stationnaire.

3) Soit $\mathscr{I}$ une famille non vide d'idéaux de A. Supposons que cette famille n'admette pas d'élément maximal ; soit I_0 un élément de $\mathscr{I}$; puisque I_0 n'est pas maximal, il existe un élément de $\mathscr{I}$ soit I_1 tel que $I_0 \subset I_1$ et $I_0 \neq I_1$. I_1 n'est pas maximal donc il existe un élément de $\mathscr{I}$ soit I_2 tel que $I_1 \subset I_2$ et $I_1 \neq I_2$. On construit ainsi une suite *strictement* croissante d'idéaux de A. Comme l'anneau A est principal, cette suite est stationnaire, ce qui est en contradiction avec le fait qu'elle est strictement croissante. La famille $\mathscr{I}$ admet donc un élément maximal.

4

NOMBRES COMPLEXES

4.1 Mettre sous la forme $x + iy$ les nombres complexes suivants :

1) $\dfrac{3 + 6\,i}{3 - 4\,i}$.

2) $\left(\dfrac{1 + i}{2 - i}\right)^2 + \dfrac{1 - 7\,i}{4 + 3\,i}$.

3) $\dfrac{2 + 5\,i}{1 - i} + \dfrac{2 - 5\,i}{1 + i}$.

Solution

1) $$\frac{3 + 6\,i}{3 - 4\,i} = \frac{(3 + 6\,i)(3 + 4\,i)}{25} = -\frac{3}{5} + \frac{6}{5}i.$$

2)
$$\left(\frac{1 + i}{2 - i}\right)^2 + \left(\frac{1 - 7\,i}{4 + 3\,i}\right) = \left[\frac{(1 + i)(2 + i)}{5}\right]^2 + \frac{(1 - 7\,i)(4 - 3\,i)}{25} = -1 - i.$$

3) Posons $z = \dfrac{2 + 5\,i}{1 - i}$, alors $\bar{z} = \dfrac{2 - 5\,i}{1 + i}$ donc

$$\frac{2 + 5\,i}{1 - i} + \frac{2 - 5\,i}{1 + i} = z + \bar{z} = 2\,R(z),$$

or $z = \dfrac{(2 + 5\,i)(1 + i)}{2} = -\dfrac{3}{2} + \dfrac{7}{2}i$ donc $\dfrac{2 + 5\,i}{1 - i} + \dfrac{2 - 5\,i}{1 + i} = -3$.

4.2 Trouver les racines carrées des nombres complexes suivants :

1) $7 + 24\,\mathrm{i}$.

2) $4\,ab + 2(a^2 - b^2)\,\mathrm{i} \quad (a \in \mathbf{R},\ b \in \mathbf{R})$.

Solution 1) Soit $z = x + \mathrm{i}y$ une racine carrée de $7 + 24\,\mathrm{i}$, alors on a

$$z^2 = x^2 - y^2 + 2\,xy\,\mathrm{i} = 7 + 24\,\mathrm{i}$$

donc

$$\begin{cases} x^2 - y^2 = 7 & (1) \\ xy = 12 & (2) \end{cases}$$

de l'équation (2) il résulte que x et y ne sont pas nuls et que $y = \dfrac{12}{x}$ d'où en portant dans l'équation (1),

$$x^2 - \frac{144}{x^2} = 7 \qquad \text{soit} \qquad x^4 - 7\,x^2 - 144 = 0\,.$$

L'équation $X^2 - 7\,X - 144 = 0$ a les racines 16 et -9 donc $x^2 = 16$ par suite $x = \varepsilon.4$ avec $\varepsilon^2 = 1$ et $y = \dfrac{12}{\varepsilon.4} = \varepsilon.3$ donc les racines carrées de $7 + 24\,\mathrm{i}$ sont

$$4 + 3\,\mathrm{i} \quad \text{et} \quad -4 - 3\,\mathrm{i}\,.$$

2) Soit $z = x + \mathrm{i}y$ une racine carrée de $4\,ab + 2(a^2 - b^2)\,\mathrm{i}$, alors

$$z^2 = x^2 - y^2 + 2\,xy\,\mathrm{i} = 4\,ab + 2(a^2 - b^2)\,\mathrm{i}$$

donc on a

$$\begin{cases} x^2 - y^2 = 4\,ab & (1) \\ xy = a^2 - b^2\,. & (2) \end{cases}$$

Il y a donc trois cas :

a) si $a = b$; alors, $z^2 = 4\,a^2$ donc z est réel et vaut $2\,a$ ou $-2\,a$;

b) si $a = -b$; alors, $z^2 = -4\,a^2$ donc z est imaginaire pur et vaut $2\,a\,\mathrm{i}$ ou $-2\,a\,\mathrm{i}$;

c) si $a \neq b$ et $a \neq -b$; alors, de l'équation (2) il résulte que x et y ne sont pas nuls et que $y = \dfrac{a^2 - b^2}{x}$ d'où en portant dans (1),

$$x^2 - \frac{(a^2 - b^2)^2}{x^2} = 4\,ab \qquad \text{soit} \qquad x^4 - 4\,abx^2 - (a^2 - b^2)^2 = 0\,,$$

or l'équation $X^2 - 4abX - (a^2 - b^2)^2 = 0$ admet les racines $(a + b)^2$ et $-(a - b)^2$ donc $x^2 = (a + b)^2$ et $x = \varepsilon(a + b)$ avec $\varepsilon^2 = 1$, d'où

$$y = \frac{a^2 - b^2}{\varepsilon(a + b)} = \varepsilon(a - b)$$

et les racines de $4ab + 2(a^2 - b^2)\,\mathrm{i}$ sont dans ce cas $a + b + (a - b)\,\mathrm{i}$ et $-(a + b) - (a - b)\,\mathrm{i}$.

4.3 Résoudre les équations suivantes :

1) $x^2 - (5 - 14\,\mathrm{i})\,x - 2(5\,\mathrm{i} + 12) = 0 \quad (x \in \mathbf{C})$

2) $x^2 - (3 + 4\,\mathrm{i})\,x - 1 + 5\,\mathrm{i} = 0 \quad (x \in \mathbf{C})$.

Solution 1) Le discriminant de cette équation est

$$\Delta = (5 - 14\,\mathrm{i})^2 + 8(5\,\mathrm{i} + 12) = -75 - 100\,\mathrm{i}\,.$$

Comme il n'est pas nul, l'équation 1) possède les racines $\dfrac{5 - 14\,\mathrm{i} + \varepsilon d}{2}$ où $\varepsilon = 1$ ou $\varepsilon = -1$ et d est une racine carrée de Δ.

Posons $d = u + \mathrm{i}v$, alors $d^2 = (u^2 - v^2) + 2uv\,\mathrm{i} = -75 - 100\,\mathrm{i}$ donc on a

$$\begin{cases} u^2 - v^2 = -75 & (1') \\ uv = -50\,. & (2') \end{cases}$$

De l'équation (2') on tire $v = -\dfrac{50}{u}$ et en portant dans (1') il vient

$$u^2 - \frac{2\,500}{u^2} = -75 \qquad \text{soit} \qquad u^4 + 75\,u^2 - 2\,500 = 0\,,$$

or l'équation $X^2 + 75\,X - 2\,500 = 0$ admet les racines -100 et $+25$ par suite $u^2 = 25$ et $u = \varepsilon'.5$ avec $\varepsilon'^2 = 1$; en portant dans (2') on obtient alors $v' = -\varepsilon'.10$ donc les racines carrées de Δ sont $5 - 10\,\mathrm{i}$ et $-5 + 10\,\mathrm{i}$ et les racines de l'équation 1) sont

$$\frac{(5 - 14\,\mathrm{i}) + (5 - 10\,\mathrm{i})}{2} = 5 - 12\,\mathrm{i} \quad \text{et} \quad \frac{(5 - 14\,\mathrm{i}) - (5 - 10\,\mathrm{i})}{2} = -2\,\mathrm{i}\,.$$

2) Le discriminant de l'équation 2) est

$$\Delta = (3 + 4\,\mathrm{i})^2 + 4(1 - 5\,\mathrm{i}) = -3 + 4\,\mathrm{i}\,.$$

Il n'est pas nul donc l'équation 2) possède les racines $\frac{3 + 4\,i + \varepsilon d}{2}$ où $\varepsilon = 1$ ou $\varepsilon = -1$ et d est une racine carrée de Δ. Le calcul des racines carrées de Δ se fait comme à la question précédente et on trouve $1 + 2\,i$ et $-1 - 2\,i$ d'où les racines de l'équation 2), $2 + 3\,i$ et $1 + i$.

4.4 a, b, c, d étant des nombres réels, résoudre les équations suivantes :

1) $|z| + z = a + b\,i \quad (z \in \mathbf{C})$

2) $|z| - z = c + d\,i \quad (z \in \mathbf{C})$.

Solution 1) Posons $z = x + iy$; alors on a $\sqrt{x^2 + y^2} + x + iy = a + bi$ d'où en égalant les parties réelles et imaginaires :

$$\begin{cases} \sqrt{x^2 + y^2} + x = a & (1) \\ y = b & (2) \end{cases}$$

il en résulte que

$$\sqrt{x^2 + b^2} + x = a \qquad (3)$$

soit $\sqrt{x^2 + b^2} = a - x$ et en élévant au carré

$$x^2 + b^2 = (a - x)^2 \qquad \text{et} \qquad a - x \geqslant 0$$

d'où

$$ax = \frac{a^2 - b^2}{2} \qquad \text{et} \qquad a - x \geqslant 0\,.$$

Il y a donc deux cas :

a) Si $a \neq 0$, alors $x = \frac{a^2 - b^2}{2a}$, et la condition $a - x \geqslant 0$ est satisfaite si et seulement si $a \geqslant 0$. Donc si $a > 0$, on a

$$z = \frac{a^2 - b^2}{2a} + bi$$

et si $a < 0$, il n'y a pas de solution.

b) Si $a = 0$, alors l'équation (3) devient $\sqrt{x^2 + b^2} + x = 0$, soit

$$x^2 + b^2 = x^2 \qquad \text{et} \qquad x \leqslant 0\,.$$

Si $b = 0$, z est réel ; l'équation (1) s'écrit alors $|z| + z = 0$ soit $|z| = -z$ et ses solutions sont tous les nombres réels négatifs. Si $b \neq 0$ l'équation (1) ne possède aucune solution.

2) Posons $z = x + iy$; alors on a $\sqrt{x^2 + y^2} - x - iy = c + di$ d'où

$$\begin{cases} \sqrt{x^2 + y^2} - x = c \\ y = -d \end{cases}$$

et $\sqrt{x^2 + d^2} = c + x$; en élevant au carré on obtient

$$x^2 + d^2 = (c + x)^2 \quad \text{et} \quad c + x \geqslant 0$$

d'où

$$cx = \frac{d^2 - c^2}{2} \quad \text{et} \quad c + x \geqslant 0 ;$$

comme dans la résolution précédente on examine deux cas :

a) Si $c \neq 0$, alors $x = \dfrac{d^2 - c^2}{2c}$, et la condition $c + x \geqslant 0$ entraîne $c \geqslant 0$.

D'où si $c > 0$ on a

$$z = \frac{d^2 - c^2}{2c} - di$$

et si $c < 0$, il n'y a aucune solution.

b) Si $c = 0$, on obtient $\sqrt{x^2 + d^2} = x$, d'où $x^2 + d^2 = x^2$ et $x \geqslant 0$. Si $d = 0$, z est réel ; l'équation initiale s'écrit alors $|z| - z = 0$, soit $|z| = z$ et ses solutions sont tous les nombres réels positifs. Si $d \neq 0$, l'équation ne possède aucune solution.

4.5 Etablir les égalités suivantes :

1) $\left(\cos\frac{\pi}{7} + i\sin\frac{\pi}{7}\right)\left(\frac{1 - i\sqrt{3}}{2}\right)(1 + i) = \sqrt{2}\left(\cos\frac{5\pi}{84} + i\sin\frac{5\pi}{84}\right)$.

2) $(1 - i)\left(\cos\frac{\pi}{5} + i\sin\frac{\pi}{5}\right)(\sqrt{3} - i) = 2\sqrt{2}\left(\cos\frac{13\pi}{60} - i\sin\frac{13\pi}{60}\right)$.

3) $\dfrac{\sqrt{2}\left(\cos\frac{\pi}{12} + i\sin\frac{\pi}{12}\right)}{1 + i} = \dfrac{\sqrt{3} - i}{2}$.

Solution 1) On a

$$\frac{1}{2} - i\frac{\sqrt{3}}{2} = \cos\left(-\frac{\pi}{3}\right) + i\sin\left(-\frac{\pi}{3}\right) \quad \text{et} \quad 1 + i = \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)$$

donc en appliquant la formule de MOIVRE,

$$\left(\cos\frac{\pi}{7} + i\sin\frac{\pi}{7}\right)\left(\frac{1 - i\sqrt{3}}{2}\right)(1 + i) =$$

$$= \sqrt{2}\left(\cos\frac{\pi}{7} + i\sin\frac{\pi}{7}\right)\left(\cos\left(-\frac{\pi}{3}\right) + i\sin\left(-\frac{\pi}{3}\right)\right)\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)$$

$$= \sqrt{2}\left(\cos\left(\frac{\pi}{7} - \frac{\pi}{3} + \frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{7} - \frac{\pi}{3} + \frac{\pi}{4}\right)\right)$$

$$= \sqrt{2}\left(\cos\frac{5\pi}{84} + i\sin\frac{5\pi}{84}\right).$$

2) On a

$$1 - i = \sqrt{2}\left(\cos\left(-\frac{\pi}{4}\right) + i \sin\left(-\frac{\pi}{4}\right)\right)$$

et

$$\sqrt{3} - i = 2\left(\cos\left(-\frac{\pi}{6}\right) + i \sin\left(-\frac{\pi}{6}\right)\right)$$

donc

$$(1 - i)\left(\cos\frac{\pi}{5} + i \sin\frac{\pi}{5}\right)(\sqrt{3} - i) =$$

$$= 2\sqrt{2}\left(\cos\left(\frac{\pi}{5} - \frac{\pi}{4} - \frac{\pi}{6}\right) + i \sin\left(\frac{\pi}{5} - \frac{\pi}{4} - \frac{\pi}{6}\right)\right)$$

$$= 2\sqrt{2}\left(\cos\left(-\frac{13\,\pi}{60}\right) + i \sin\left(-\frac{13\,\pi}{60}\right)\right) = 2\sqrt{2}\left(\cos\frac{13\,\pi}{60} - i \sin\frac{13\,\pi}{60}\right)$$

3) On a

$$1 + i = \sqrt{2}\left(\cos\frac{\pi}{4} + i \sin\frac{\pi}{4}\right),$$

donc

$$\frac{\sqrt{2}\left(\cos\frac{\pi}{12} + i \sin\frac{\pi}{12}\right)}{1 + i} = \frac{\left(\cos\frac{\pi}{12} + i \sin\frac{\pi}{12}\right)}{\left(\cos\frac{\pi}{4} + i \sin\frac{\pi}{4}\right)}$$

$$= \cos\left(\frac{\pi}{12} - \frac{\pi}{4}\right) + i \sin\left(\frac{\pi}{12} - \frac{\pi}{4}\right)$$

$$= \cos\left(-\frac{\pi}{6}\right) + i \sin\left(-\frac{\pi}{6}\right) = \frac{\sqrt{3}}{2} - \frac{1}{2}i = \frac{\sqrt{3} - i}{2}$$

4.6 Résoudre les équations suivantes :

1) $$z^6 = \frac{1 + i\sqrt{3}}{1 - i\sqrt{3}}.$$

2) $$z^4 = \frac{1 - i}{1 + i\sqrt{3}}.$$

Solution 1) On a

$$\frac{1+i\sqrt{3}}{1-i\sqrt{3}} = \frac{2\left(\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}\right)}{2\left(\cos\left(-\frac{\pi}{3}\right)+i\sin\left(-\frac{\pi}{3}\right)\right)} = \cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}$$

l'équation 1) s'écrit donc

$$z^6 = \cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}$$

et ses six racines sont (*cf.* Q., Ch. 6, § II, n° 119)

$$z_k = \cos\frac{\frac{2\pi}{3}+2k\pi}{6}+i\sin\frac{\frac{2\pi}{3}+2k\pi}{6} \qquad (0 \leqslant k \leqslant 5)$$

soit aussi

$$z_k = \cos\left(\frac{\pi}{9}+\frac{k\pi}{3}\right)+i\sin\left(\frac{\pi}{9}+\frac{k\pi}{3}\right) \qquad (0 \leqslant k \leqslant 5).$$

2) On a

$$\frac{1-i}{1+i\sqrt{3}} = \frac{\sqrt{2}\left(\cos\left(-\frac{\pi}{4}\right)+i\sin\left(-\frac{\pi}{4}\right)\right)}{2\left(\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}\right)} = \frac{\sqrt{2}}{2}\left(\cos\frac{17\pi}{12}+i\sin\frac{17\pi}{12}\right)$$

l'équation 2) s'écrit donc

$$z^4 = 2^{-\frac{1}{2}}\left(\cos\frac{17\pi}{12}+i\sin\frac{17\pi}{12}\right)$$

et ses quatre racines sont (*cf.* Q., Ch. 6, § II, n° 119)

$$z_k = 2^{-\frac{1}{8}}\left(\cos\left(\frac{17\pi}{48}+\frac{k\pi}{2}\right)+i\sin\left(\frac{17\pi}{48}+\frac{k\pi}{2}\right)\right) \qquad (0 \leqslant k \leqslant 3).$$

4.7 α, β, ρ étant des nombres réels et n un entier positif, calculer :

$$A = \sum_{k=0}^{n-1} \rho^k \cos(\alpha + k\beta)$$

$$B = \sum_{k=0}^{n-1} \rho^k \sin(\alpha + k\beta).$$

Solution Posons $C = A + iB$ et calculons C.

$$C = \sum_{k=0}^{n-1} \rho^k(\cos(\alpha + k\beta) + i \sin(\alpha + k\beta)) = \sum_{k=0}^{n-1} \rho^k e^{i(\alpha+k\beta)}$$

donc

$$C = e^{i\alpha} \sum_{k=0}^{n-1} (\rho e^{i\beta})^k = e^{i\alpha} \frac{1 - \rho^n e^{in\beta}}{1 - \rho e^{i\beta}},$$

or on a

$$\frac{1 - \rho^n e^{in\beta}}{1 - \rho e^{i\beta}} = \frac{(1 - \rho^n e^{in\beta})(1 - \rho \cos\beta + i\rho \sin\beta)}{(1 - \rho\cos\beta)^2 + \rho^2 \sin^2\beta}$$

soit après calculs,

$$\frac{1 - \rho^n e^{in\beta}}{1 - \rho e^{i\beta}} = \frac{1 - \rho e^{-i\beta} - \rho^n e^{in\beta} + \rho^{n+1} e^{i(n-1)\beta}}{1 + \rho^2 - 2\rho\cos\beta}$$

d'où

$$C = \frac{e^{i\alpha} - \rho e^{i(\alpha-\beta)} - \rho^n e^{i(\alpha+n\beta)} + \rho^{n+1} e^{i(\alpha+(n-1)\beta)}}{1 + \rho^2 - 2\rho\cos\beta}$$

d'où en séparant partie réelle et partie imaginaire de C,

$$A = \frac{\cos\alpha - \rho\cos(\alpha - \beta) - \rho^n \cos(\alpha + n\beta) + \rho^{n+1}\cos(\alpha + (n-1)\beta)}{1 + \rho^2 - 2\rho\cos\beta}$$

$$B = \frac{\sin\alpha - \rho\sin(\alpha - \beta) - \rho^n \sin(\alpha + n\beta) + \rho^{n+1}\sin(\alpha + (n-1)\beta)}{1 + \rho^2 - 2\rho\cos\beta}.$$

4.8 Soit ε une racine n-ième de l'unité ; calculer

$$A = 1 + 2\varepsilon + 3\varepsilon^2 + \cdots + n\varepsilon^{n-1}.$$

Solution Si $\varepsilon = 1$, $A = \frac{n(n+1)}{2}$. Supposons $\varepsilon \neq 1$; nous allons donner trois méthodes pour le calcul de A.

Première méthode. Multiplions A par $(1 - \varepsilon)$; on obtient ;

$$(1 - \varepsilon)A = 1 + \varepsilon + \varepsilon^2 + \cdots + \varepsilon^{n-1} - n\varepsilon^n ;$$

comme ε est une racine n-ième de l'unité, différente de 1, on a

$$\varepsilon^n = 1 \quad \text{et} \quad 1 + \varepsilon + \varepsilon^2 + \cdots + \varepsilon^{n-1} = \frac{1 - \varepsilon^n}{1 - \varepsilon} = 0$$

donc

$$A(1-\varepsilon) = -n \qquad \text{et} \qquad A = \frac{n}{\varepsilon - 1}.$$

Seconde méthode. Remarquons que A est la somme des nombres écrits dans le triangle suivant :

$$\begin{array}{ccccccccc}
1 & \varepsilon & \varepsilon^2 & \varepsilon^3 & \cdots\cdots & \varepsilon^{n-2} & \varepsilon^{n-1} \\
 & \varepsilon & \varepsilon^2 & \varepsilon^3 & \cdots\cdots & \varepsilon^{n-2} & \varepsilon^{n-1} \\
 & & \varepsilon^2 & \varepsilon^3 & \cdots\cdots & \varepsilon^{n-2} & \varepsilon^{n-1} \\
 & & & \varepsilon^3 & \cdots\cdots & \varepsilon^{n-2} & \varepsilon^{n-1} \\
 & & & & \ddots & \vdots & \vdots \\
 & & & & & \varepsilon^{n-2} & \varepsilon^{n-1} \\
 & & & & & & \varepsilon^{n-1}
\end{array}$$

En sommant ligne par ligne, on obtient :

$$A = \sum_{k=0}^{n-1} (\varepsilon^k + \varepsilon^{k+1} + \cdots + \varepsilon^{n-1}) = \sum_{k=0}^{n-1} \frac{\varepsilon^k - \varepsilon^n}{1-\varepsilon} = \sum_{k=0}^{n-1} \frac{\varepsilon^k - 1}{1-\varepsilon}$$

donc

$$A = \frac{1}{1-\varepsilon} \sum_{k=0}^{n-1} (\varepsilon^k - 1) = \frac{1}{1-\varepsilon} (1 + \varepsilon + \varepsilon^2 + \cdots + \varepsilon^{n-1} - n),$$

or on a vu que

$$1 + \varepsilon + \varepsilon^2 + \cdots + \varepsilon^{n-1} = 0$$

donc

$$A = \frac{n}{\varepsilon - 1}.$$

Troisième méthode. Considérons le polynôme

$$P(X) = 1 + X + X^2 + \cdots + X^n ;$$

alors on a

$$P(X) = \frac{1 - X^{n+1}}{1 - X}$$

donc

$$P'(X) = \frac{nX^{n+1} - (n+1)X^n + 1}{(1-X)^2} = 1 + 2X + 3X^2 + \cdots + nX^{n-1}$$

par suite

$$A = P'(\varepsilon) = \frac{n\varepsilon^{n+1} - (n+1)\varepsilon^n + 1}{(1-\varepsilon)^2} = \frac{n\varepsilon - n}{(1-\varepsilon)^2} = \frac{n}{\varepsilon - 1}.$$

4.9 j désignant le nombre complexe $e^{2i\pi/3}$ et a, b, c trois nombres complexes donnés, on considère le système

$$(S)\begin{cases} x + y + z = a & (1) \\ x + jy + j^2 z = b & (2) \\ x + j^2 y + jz = c & (3) \end{cases}$$

1) Résoudre ce système.

2) Comment faut-il choisir a, b, c pour que x, y, z soient réels ?

Solution 1) Rappelons que

$$1 + j + j^2 = \frac{1 - j^3}{1 - j} = 0 .$$

En additionnant membre à membre les équations (1), (2) et (3), on obtient :

$$3x + (y + z)(1 + j + j^2) = a + b + c \quad \text{donc} \quad x = \frac{a + b + c}{3} .$$

Multiplions les deux membres de l'équation (2) par j^2, ceux de l'équation (3) par j et additionnons membre à membre les équations ainsi obtenues et l'équation (1) ; on obtient

$$(x + z)(1 + j + j^2) + 3y = a + bj^2 + cj \quad \text{d'où} \quad y = \frac{a + bj^2 + cj}{3} .$$

Enfin, multiplions les deux membres de l'équation (2) par j, ceux de l'équation (3) par j^2 et additionnons membre à membre l'équation (1) et les deux équations ainsi obtenues ; il vient

$$z = \frac{a + bj + c^2}{3} .$$

Le système (S) admet donc la solution :

$$x = \frac{a + b + c}{3}, \quad y = \frac{a + bj^2 + cj}{3}, \quad z = \frac{a + bj + cj^2}{3} .$$

2) Si x, y, z sont réels, l'équation (1) montre que a est réel et les équations (2) et (3) que b et c sont deux nombres complexes conjugués. Réciproquement si a est réel et si b et c sont conjugués, alors $b + c$ est réel donc x l'est, et on a $\overline{bj} = cj^2$ et $\overline{bj^2} = cj$ (car $j^2 = \bar{j}$) par suite $bj + cj^2$ et $bj^2 + cj$ sont réels et il en est de même de y et z. Par conséquent, une condition nécessaire et suffisante pour que x, y, z soient réels est que a soit réel et b et c conjugués.

4.10 Etablir l'identité suivante :

$$|z + z'|^2 + |z - z'|^2 = 2(|z|^2 + |z'|^2) \quad (z \in \mathbf{C},\ z' \in \mathbf{C})$$

et en donner une interprétation géométrique.

Solution On a, pour tout couple (z, z') de nombres complexes :

$$|z + z'|^2 = (z + z')(\bar{z} + \bar{z}') = (z + z')(\bar{z} + \bar{z}') = z\bar{z} + z\bar{z}' + z'\bar{z} + z'\bar{z}',$$

$$|z - z'|^2 = (z - z')(\overline{z - z'}) = (z - z')(\bar{z} - \bar{z}') = z\bar{z} - z\bar{z}' - z'\bar{z} + z'\bar{z}',$$

donc

$$|z + z'|^2 + |z - z'|^2 = 2z\bar{z} + 2z'\bar{z}' = 2(|z|^2 + |z'|^2)$$

Soient M, M' deux points d'un plan, d'affixes z et z' relativement à un système d'axes orthonormé Ox, Oy ; si N est le point d'affixe $z + z'$, on sait que le quadrilatère $OMNM'$ est un parallélogramme. $|z + z'|^2$ est le carré de la longueur de la diagonale ON de ce parallélogramme, $|z - z'|^2$ est le carré de la longueur de la diagonale MM', et $2(|z|^2 + |z'|^2)$ est la somme des carrés des longueurs des quatre côtés du parallélogramme $OMNM'$.

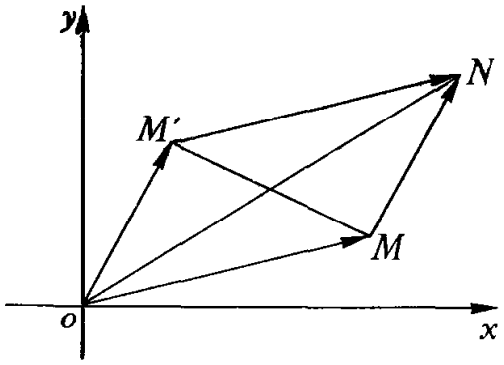


FIG. 4.1

L'identité

$$|z + z'|^2 + |z - z'|^2 = 2(|z|^2 + |z'|^2),$$

nous fournit donc le résultat géométrique : la somme des carrés des longueurs des diagonales d'un parallélogramme est égale à la somme des carrés des longueurs de ses quatre côtés.

4.11 Déterminer par le calcul et géométriquement les nombres complexes z tels que

a) $$\left|\frac{z - 3}{z - 5}\right| = 1 .$$

b) $$\left|\frac{z - 3}{z - 5}\right| = \frac{\sqrt{2}}{2}.$$

Solution a) *Solution par le calcul.* Posons $z = x + iy$, alors

$$|z - 3|^2 = (x - 3)^2 + y^2, \quad |z - 5|^2 = (x - 5)^2 + y^2$$

et la condition $\left|\frac{z-3}{z-5}\right| = 1$ équivaut à $|z - 3|^2 = |z - 5|^2$ soit aussi $x^2 - 6x + 9 + y^2 = x^2 - 10x + 25 + y^2$, soit $x = 4$. Les nombres complexes cherchés sont donc tous les nombres complexes dont la partie réelle est égale à 4.

Solution géométrique. Rapportons le plan à un système d'axes orthonormé $x'Ox$, $y'Oy$. Désignons par A, B, M les points d'affixes 3, 5, z par rapport à ce repère. Alors, la condition $\left|\frac{z-3}{z-5}\right| = 1$ équivaut à la condition

$$\| \overrightarrow{MA} \| = \| \overrightarrow{MB} \|$$

qui signifie que M est un point de la médiatrice du segment AB ; cette médiatrice est la droite d'équation $x = 4$, donc, un nombre complexe z vérifie la condition $\left|\frac{z-3}{z-5}\right| = 1$ si et seulement si sa partie réelle est égale à 4.

b) *Solution par le calcul.* Posons $z = x + iy$, alors la condition

$$\left|\frac{z-3}{z-5}\right| = \frac{\sqrt{2}}{2}$$

équivaut à $|z - 3|^2 = \frac{1}{2}|z - 5|^2$ soit $(x - 3)^2 + y^2 = \frac{1}{2}((x - 5)^2 + y^2)$ soit encore après calcul

$$(x - 1)^2 + y^2 = 8. \qquad (1)$$

Les nombres complexes cherchés sont donc les nombres $z = x + iy$ tels que x et y vérifient l'équation (1).

Solution géométrique. Rapportons le plan à un système d'axes orthonormé $x'Ox$, $y'Oy$; désignons par A, B, M les points d'affixes 3, 5, z ; alors la condition de l'énoncé est équivalente à la condition $\frac{\| \overrightarrow{MA} \|}{\| \overrightarrow{MB} \|} = \frac{\sqrt{2}}{2}$. Or on sait que l'ensemble des points M tels que $\frac{\| \overrightarrow{MA} \|}{\| \overrightarrow{MB} \|} = \frac{\sqrt{2}}{2}$ est le cercle de diamètre CD, les points C et D étant les points de $x'Ox$ qui divisent AB dans le rapport $\frac{\sqrt{2}}{2}$. La détermination des points C et D se fait comme suit : Le point C situé entre A et B tel que $\frac{\| \overrightarrow{CA} \|}{\| \overrightarrow{CB} \|} = \frac{\sqrt{2}}{2}$ vérifie $\| \overrightarrow{CA} \| + \| \overrightarrow{CB} \| = \| \overrightarrow{AB} \| = 2$ donc

$$\| \overrightarrow{CB} \| \left(1 + \frac{\sqrt{2}}{2}\right) = 2 \quad \text{et} \quad \| \overrightarrow{CB} \| = 4 - 2\sqrt{2},$$

par suite C est le point d'affixe $1 + 2\sqrt{2}$. Le point D extérieur au segment AB tel que $\dfrac{\| \overrightarrow{DA} \|}{\| \overrightarrow{DB} \|} = \dfrac{\sqrt{2}}{2}$ se trouve donc sur la demi-droite $x'A$ donc on a

$$\| \overrightarrow{DB} \| - \| \overrightarrow{DA} \| = \| \overrightarrow{AB} \| = 2 \qquad \text{et} \qquad \| \overrightarrow{DB} \| \left(1 - \frac{\sqrt{2}}{2} \right) = 2$$

d'où $\| \overrightarrow{DB} \| = 4 + 2\sqrt{2}$, par suite le point D est le point d'affixe $1 - 2\sqrt{2}$. Le cercle de diamètre CD est donc le cercle dont le centre E est le point d'affixe 1 et le rayon est $2\sqrt{2}$; son équation est $(x - 1)^2 + y^2 = (2\sqrt{2})^2 = 8$. Les nombres complexes z vérifiant la condition $\left| \dfrac{z - 3}{z - 5} \right| = \dfrac{\sqrt{2}}{2}$ sont donc les nombres $z = x + iy$ tels que $(x - 1)^2 + y^2 = 8$.

4.12 Quelles relations doivent exister entre les nombres complexes dont les images sont :

a) trois points alignés,

b) les sommets d'un triangle équilatéral,

c) les sommets d'un polygone régulier à n côtés.

Solution Rapportons le plan à un système d'axes orthonormé $x'Ox$, $y'Oy$.

a) Soient A, B, C trois points d'affixes a, b, c par rapport au repère choisi. Les trois points A, B, C sont alignés si et seulement si $(\overrightarrow{AB}, \overrightarrow{AC}) \equiv 0 \pmod{\pi}$ c'est-à-dire si et seulement si

$$\operatorname{Arg}(b - a) - \operatorname{Arg}(c - a) \equiv 0 \pmod{\pi},$$

d'où la condition nécessaire et suffisante pour que A, B, C soient alignés :

$$\operatorname{Arg}\left(\frac{b - a}{c - a} \right) \equiv 0 \pmod{\pi}.$$

b) Soient A, B, C trois points d'affixes a, b, c par rapport au repère précédent. Le triangle ABC est équilatéral si et seulement si

$$\| \overrightarrow{AB} \| = \| \overrightarrow{BC} \| \qquad \text{et} \qquad (\overrightarrow{AB}, \overrightarrow{BC}) = \frac{2\pi}{3} ;$$

le nombre complexe $\dfrac{c - b}{b - a}$ est de module 1 si et seulement si $\| \overrightarrow{AB} \| = \| \overrightarrow{BC} \|$,

il est d'argument $\frac{2\pi}{3}$ si et seulement si $(\overrightarrow{AB}, \overrightarrow{BC}) = \frac{2\pi}{3}$, donc la condition nécessaire et suffisante pour que le triangle ABC soit équilatéral est que

$$\frac{c-b}{\bar{b}-\bar{a}} = e^{\frac{2i\pi}{3}}.$$

c) Soient $A_0, A_1, A_2, \ldots, A_{n-1}$, n points d'affixes respectifs $a_0, a_1, a_2, \ldots, a_{n-1}$ par rapport au repère choisi. La condition nécessaire et suffisante pour que ces points soient les sommets d'un polygone régulier, est que l'on ait pour $1 \leqslant k \leqslant n-2$,

$$\| \overrightarrow{A_{k-1}A_k} \| = \| \overrightarrow{A_kA_{k+1}} \| \quad \text{et} \quad (\overrightarrow{A_{k-1}A_k}, \overrightarrow{A_kA_{k+1}}) = \frac{2\pi}{n},$$

donc $A_0, A_1, \ldots, A_{n-1}$ sont les sommets d'un polygone régulier si et seulement si on a

$$\frac{a_{k+1}-a_k}{a_k-a_{k-1}} = e^{\frac{2i\pi}{n}} \quad \text{pour} \quad 1 \leqslant k \leqslant n-$$

4.13 A chaque triplet A, B, C de points distincts du plan, d'affixes a, b, c relativement à un système d'axes orthonormé Ox, Oy, on associe les nombres complexes :

$$u(A, B, C) = a + bj + cj^2, \quad v(A, B, C) = a + bj^2 + cj,$$

$$w(A, B, C) = \frac{u(A, B, C)}{v(A, B, C)}, \quad \text{où} \quad j = e^{\frac{2i\pi}{3}}$$

1) Comment sont transformés $u(A, B, C)$, $v(A, B, C)$ et $w(A, B, C)$ quand on remplace les points A, B, C par leurs images :

a) par une translation,

b) par une rotation de centre O,

c) par une homothétie de centre O.

2) Montrer que deux triangles ABC et $A'B'C'$ du plan sont semblables si et seulement si $w(A, B, C) = w(A', B', C')$.

3) Trouver les triangles ABC du plan tels que $u(A, B, C)=0$ ou $v(A, B, C)=0$.

Solution 1) *a*) Soit τ la translation de vecteur $\overrightarrow{OM}$ et m l'affixe de M. alors l'affixe de $\tau(A)$ (resp. $\tau(B)$, $\tau(C)$) est $a + m$ (resp. $b + m$, $c + m$) donc

$$u(\tau(A), \tau(B), \tau(C)) = a + m + (b + m)j + (c + m)j^2 = \\ = a + bj + cj^2 + m(1 + j + j^2),$$

or j est une racine cubique de l'unité donc

$$1 + j + j^2 = \frac{1 - j^3}{1 - j} = 0$$

et

$$u(\tau(A), \tau(B), \tau(C)) = a + bj + cj^2 = u(A, B, C);$$

on démontre de la même manière que $v(\tau(A), \tau(B), \tau(C)) = v(A, B, C)$ et il en résulte que

$$w(\tau(A), \tau(B), \tau(C)) = w(A, B, C).$$

b) Soit ρ la rotation de centre O et d'angle α ; alors l'affixe du point $\rho(A)$ (resp. $\rho(B)$, $\rho(C)$) est $a\,e^{i\alpha}$ (resp. $b\,e^{i\alpha}$, $c\,e^{i\alpha}$) donc

$$u(\rho(A), \rho(B), \rho(C)) = (a + bj + cj^2)\,e^{i\alpha} = u(A, B, C).e^{i\alpha},$$

de même $v(\rho(A), \rho(B), \rho(C)) = v(A, B, C)\,e^{i\alpha}$ donc

$$w(\rho(A), \rho(B), \rho(C)) = w(A, B, C).$$

c) Soit σ l'homothétie de centre O et de rapport k ; alors l'affixe du point $\sigma(A)$ (resp. $\sigma(B)$, $\sigma(C)$) est $k.a$ (resp. $k.b$, $k.c$) donc

$$u(\sigma(A), \sigma(B), \sigma(C)) = k(a + bj + cj^2) = k.u(A, B, C)$$

et on voit de la même manière que

$$v(\sigma(A), \sigma(B), \sigma(C)) = k.v(A, B, C)$$

donc

$$w(\sigma(A), \sigma(B), \sigma(C)) = w(A, B, C).$$

2) Soit D un point de l'axe Ox distinct de O. Si ABC est un triangle du plan, a, b, c étant les affixes des points A, B, C, désignons par τ_{ABC} la translation de vecteur $\overrightarrow{AO}$, par ρ_{ABC} la rotation de centre O et d'angle $\alpha = -\operatorname{Arg}(b - a)$ et par σ_{ABC} l'homothétie de centre O et de rapport $\frac{\| \overrightarrow{OD} \|}{\| \overrightarrow{AB} \|}$. Alors la transformation $\lambda_{ABC} = \sigma_{ABC} \circ \rho_{ABC} \circ \tau_{ABC}$ transforme le triangle ABC en un triangle ODE qui lui est semblable ; de plus, chacune des transformations σ_{ABC}, ρ_{ABC}, τ_{ABC} conserve $w(A, B, C)$ donc $w(O, D, E) = w(A, B, C)$. Soient maintenant ABC et $A'B'C'$ deux triangles du plan, $\tau_{A'B'C'}$, $\rho_{A'B'C'}$, $\sigma_{A'B'C'}$ les transformations définies à partir des points A', B', C' comme l'ont été τ_{ABC}, ρ_{ABC}, σ_{ABC} à partir des points ABC, alors posons $\lambda_{A'B'C'} = \sigma_{A'B'C'} \circ \rho_{A'B'C'} \circ \tau_{A'B'C'}$ et désignons par

ODE' le triangle image du triangle $A'\,B'\,C'$ par la transformation $\lambda_{A'B'C'}$. On a $w(A', B', C') = w(O, D, E')$. Les deux triangles ABC et $A'\,B'\,C'$ sont alors semblables si et seulement si les triangles ODE et ODE' sont égaux. Si d, e, e' sont les affixes des points D, E, E', on a

$$w(O, D, E) = \frac{dj + ej^2}{dj^2 + ej} = \frac{d + ej}{dj + e} \qquad \text{et} \qquad w(O, D, E') = \frac{d + e'j}{dj + e'}.$$

Il est clair que si les triangles ODE et ODE' sont égaux,

$$w(O, D, E) = w(O', D, E') ;$$

réciproquement, si $w(O, D, E) = w(O, D, E')$ on a

$$\frac{d + ej}{dj + e} = \frac{d + e'j}{dj + e'}$$

d'où

$$(d + ej)(dj + e') = (d + e'j)(dj + e)$$

soit $d(e - e') + dj^2(e' - e) = 0$ soit encore $d(1 + j^2)(e' - e) = 0$ or $D \neq O$ donc d n'est pas nul, par suite $e = e'$ et les triangles ODE et ODE' sont égaux. Il en résulte que les triangles ABC et $A'\,B'\,C'$ sont semblables si et seulement si $w(A, B, C) = w(A', B', C')$.

3) Soit ABC un triangle tel que $u(A, B, C) = 0$. Alors, si a, b, c sont les affixes de A, B, C on a : $a + bj + cj^2 = 0$. Désignant par λ_{ABC} la transformation définie précédemment et par ODE le triangle image de ABC par λ_{ABC}, on a, compte tenu des résultats de la question 1, $u(O, D, E) = u(A, B, C)e^{i\alpha}$ avec $\alpha = -\operatorname{Arg}(b - a)$, donc $u(A, B, C) = 0$ si et seulement si $u(O, D, E) = 0$. Désignons par d, e les affixes des points D, E ; alors $u(O, D, E) = dj + ej^2$. Si $u(O, D, E) = 0$ on a $d = -ej$; cette relation signifie que le vecteur $\overrightarrow{OD}$ se déduit du vecteur $\overrightarrow{OE}$ par la rotation de centre O et d'angle $-\frac{\pi}{3}$, donc le triangle ODE est équilatéral. La réciproque est immédiate. Comme les triangles ODE et ABC sont semblables on voit que le triangle ABC est équilatéral si et seulement si $u(A, B, C) = 0$. On démontre de la même manière que les triangles ABC tels que $v(A, B, C) = 0$ sont aussi les triangles équilatéraux.

5

ESPACES VECTORIELS

5.1 Soient E un espace vectoriel sur un corps commutatif et A, B, C trois sous-espaces vectoriels tels que

$$A \cap B = A \cap C \tag{1}$$

$$A + B = A + C \tag{2}$$

$$B \subset C. \tag{3}$$

Montrer que $B = C$.

Solution La relation (3) étant vérifiée, il suffit de prouver que $C \subset B$. Si c est un élément de C, il appartient à $A + C$ donc (2) à $A + B$, par suite il existe un élément a de A et un élément b de B tels que $c = a + b$. D'après (3), b appartient à C donc $a = c - b$ appartient à $A \cap C$ qui est égal à $A \cap B$ et a appartient à B. L'élément c, somme de deux éléments de B est lui-même élément de B, ce qui prouve que $C \subset B$.

5.2 Soit E un espace vectoriel de dimension finie n sur un corps commutatif K. On considère deux sous-espaces vectoriels A et B de E.

1) Montrer que si A et B sont tous deux distincts de E, alors $A \cup B$ est une partie stricte de E.

2) On suppose que $\dim_K A = \dim_K B$. Montrer par récurrence sur l'entier $n - \dim_K A$ qu'il existe un sous-espace vectoriel X de E tel que

$$E = A \oplus X = B \oplus X$$

Solution 1) Examinons deux cas suivant que l'un des sous-espaces A ou B contient l'autre ou pas.

a) Si $A \subset B$ ou $B \subset A$, alors $A \cup B = B$ ou $A \cup B = A$ et comme A et B sont des sous-espaces stricts de E, $A \cup B$ est strictement contenu dans E.

b) Si $A \not\subset B$ et $B \not\subset A$, alors il existe un élément x de B qui n'appartient pas à A et un élément y de A qui n'appartient pas à B. Formons l'élément $z = x + y$. Il n'appartient pas à A sinon $x = z - y$ serait dans A. Il n'appartient pas à B sinon $y = z - x$ serait dans B, donc $z \notin A \cup B$, par suite $A \cup B$ est strictement contenu dans E.

2) Si $n - \dim_K A = 0$, on a $\dim_K A = \dim_K B = \dim_K E$ donc $A = B = E$ et $X = \{ 0 \}$ est un supplémentaire commun à A et B.

Supposons le résultat démontré si $n - \dim_K A = p$ (avec $p \geqslant 0$), c'est-à-dire si $\dim_K A = n - p$. Soient A et B deux sous-espaces vectoriels de E tels que $\dim_K A = \dim_K B$ et $n - \dim_K A = p + 1$. Alors,

$$\dim_K A = \dim_K B = n - p - 1 < n$$

donc A et B sont des sous-espaces stricts de E, par suite (question 1) $A \cup B$ est strictement contenu dans E.

Soit x un élément de $E - (A \cup B)$. Formons les sous-espaces $A' = A \oplus Kx$ et $B' = B \oplus Kx$ (ces sommes sont directes car $x \notin A \cup B$). Alors

$$\dim_K A' = \dim_K B' = \dim_K A + 1 = n - p ,$$

donc $n - \dim_K A' = p$ et (hypothèse de récurrence) il existe un sous-espace X' de E tel que $E = A' \oplus X' = B' \oplus X'$. Alors on a

$$E = A \oplus Kx \oplus X' = B \oplus Kx \oplus X'$$

et en posant $X = Kx \oplus X'$ on définit un sous-espace X de E tel que

$$E = A \oplus X = B \oplus X$$

d'où le résultat.

5.3 Soit K un corps commutatif fini de caractéristique p. Soit e son élément unité.

1) Montrer que p est un nombre premier.

2) Montrer que le sous-corps L engendré par e est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

3) Montrer que l'addition de K et la restriction à $L \times K$ de la multiplication de K munissent K d'une structure d'espace vectoriel sur L.

4) Montrer que K est de dimension finie sur L. Si $\dim {}_L K = n$, calculer le cardinal de K en fonction de p et n.

Solution 1) K étant fini le sous-groupe additif J engendré par e est fini donc (*cf.* Q., Ch. 5, § II, n° 97) la caractéristique p de K est non nulle. Nous savons que p est le plus petit entier positif tel que $p.e = 0$. Si $p = p_1.p_2$ on a

$$(p_1\, e)(p_2\, e) = (p_1\, p_2\, e) = 0\,.$$

Si on suppose $p_1 \neq p$ et $p_2 \neq p$ on a $p_1\, e \neq 0$ et $p_2\, e \neq 0$ donc K admet des diviseurs de zéro ce qui est impossible. Donc p est bien un nombre premier.

2) D'après Q., Ch. 5, § II, n° 97, J est isomorphe à $\mathbf{Z}/p\mathbf{Z}$. Comme p est premier, $\mathbf{Z}/p\mathbf{Z}$ est un corps (*cf.* exercice 3.11). Comme J est un corps contenant e, on a $J \supset L$. D'autre part le groupe sous-jacent à L contient e donc L contient le sous-groupe engendré par e, c'est-à-dire que $L \supset J$. On a alors $L = J$ et L est bien isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

3) K est un groupe abélien additif. Si l, l' sont des éléments de L et k, k' des éléments de K, l'associativité de la multiplication et sa distributivité par rapport à l'addition permettent d'écrire

$$(ll')\,k = l(l'\,k)\,, \quad (l + l')\,k = lk + l'\,k\,, \quad l(k + k') = lk + lk'\,.$$

Comme l'élément unité de L est le même que celui de K on a bien, pour tout élément k de K

$$ek = k\,.$$

On voit que tous les axiomes qui définissent la structure d'espace vectoriel sont vérifiés.

4) Nous savons (*cf.* Q., Ch. 7, § III, n° 135) que tout espace vectoriel admet au moins une base. K étant fini, il ne peut admettre que des bases finies ; il est donc de dimension finie, soit n, sur L. Mais alors (*cf.* Q., Ch. 7, § III, n° 136) K est isomorphe à L^n et par suite à $(\mathbf{Z}/p\mathbf{Z})^n$. On a donc

$$\text{card}\, K = \text{card}\, (\mathbf{Z}/p\mathbf{Z})^n = [\text{card}\, (\mathbf{Z}/p\mathbf{Z})]^n = p^n\,.$$

5.4 Dans l'espace vectoriel $\mathbf{R}^4$ rapporté à sa base canonique, vérifier que les vecteurs

$a = (1, 2, -1, -2)$ $b = (2, 3, 0, -1)$ $c = (1, 3, -1, 0)$ $d = (1, 2, 1, 4)$

sont linéairement indépendants et calculer les coordonnées du vecteur

$$x = (7, 14, -1, 2)$$

sur la base $\{ a, b, c, d \}$.

Solution Nous appliquons la méthode de Q., Ch. 7, § III, n° 138. On obtient successivement les systèmes

a	b	c	d	x
1	2	1	1	7
2	3	3	2	14
−1	0	−1	1	− 1
−2	−1	0	4	2

a	$b'=b-2a$	$c'=c-a$	$d'=d-a$	$x'=x-7a$
1	0	0	0	0
2	−1	1	0	0
−1	2	0	2	6
−2	3	2	6	16

a	b'	$c''=c'+b'$	$d''=d'-c''$	$x''=x'-3c''$
1	0	0	0	0
2	−1	0	0	0
−1	2	2	0	0
−2	3	5	1	1

Sur ce tableau on voit que a, b, c, d sont linéairement indépendants. La relation reliant les cinq vecteurs est $x'' = d''$ ce qui donne $d' - c'' = x' - 3c''$ soit $d' + 2c'' = x'$ soit encore $d - a + 2(c' + b') = x - 7a$ ou

$$d - a + 2(c - a + b - 2a) = x - 7a$$

soit aussi $x = 2b + 2c + d$. Donc les coordonnées de x sur la base $\{a, b, c, d\}$ sont (0, 2, 2, 1).

5.5 1) On considère l'espace vectoriel sur $\mathbf{R}$, $V = \mathbf{R}^3$ muni de sa base canonique. Déterminer suivant les valeurs de α le rang du système suivant

$$a = (1, 1, \alpha) \quad b = (1, \alpha, 1) \quad c = (\alpha, 1, 1)$$

2) Même question pour le même système considéré comme système de vecteurs de l'espace $V = (\mathbf{Z}/2\,\mathbf{Z})^3$ sur le corps $\mathbf{Z}/2\,\mathbf{Z}$.

Solution 1) Nous appliquons la méthode Q., Ch. 7, § III, n° 138. On obtient successivement les systèmes

a	b	c
1	1	α
1	α	1
α	1	1

a	$b-a$	$c-\alpha a$
1	0	0
1	$\alpha-1$	$1-\alpha$
α	$1-\alpha$	$1-\alpha^2$

a	$b-a$	$c-\alpha a+b-a$
1	0	0
1	$\alpha-1$	0
α	$1-\alpha$	$2-\alpha-\alpha^2$

Or $2 - \alpha - \alpha^2 = 0$ si et seulement si $\alpha = 1$ ou $\alpha = -2$.

Si $\alpha = 1$, les trois vecteurs a, b, c sont égaux et le système est de rang 1.

Si $\alpha = -2$, a et b sont linéairement indépendants et $c = (1 + \alpha)a + b$ donc le système est de rang 2.

Enfin si $\alpha \neq 1$ et $\alpha \neq -2$, le système est de rang 3.

2) α ne peut prendre que les valeurs $\bar{0}$ et $\bar{1}$. Si $\alpha = \bar{1}$ les trois vecteurs a, b, c sont égaux et le système est de rang 1. Si $\alpha = \bar{0}$ le calcul précédent montre que a et b sont linéairement indépendants, mais comme $a + b + c = \bar{0}$, le système est de rang 2.

5.6 Soit E l'espace vectoriel sur $\mathbf{R}$ des fonctions définies sur $\mathbf{Z}$ à valeurs réelles.

1) Soient a_1 et a_2 des nombres réels tels que $a_2 \neq 0$ et $a_1^2 \geqslant 4a_2$. Soit F l'ensemble des éléments f de E vérifiant la condition

$$(\forall n \in \mathbf{Z}) \quad \big(f(n) + a_1 f(n-1) + a_2 f(n-2) = 0\big).$$

Montrer que F est un sous-espace vectoriel de E.

2) Si a et b sont deux réels quelconques, montrer qu'il existe un élément f de F et un seul, tel que $f(1) = a$ et $f(2) = b$. Quelle est la dimension de F ?

3) Trouver tous les éléments α de $\mathbf{R}$ tels que la fonction $f(n) = \alpha^n$ $(n \in \mathbf{Z})$ soit dans F.

4) Montrer que si α, β sont deux nombres réels différents, les fonctions $f(n) = \alpha^n$ et $g(n) = \beta^n$ $(n \in \mathbf{Z})$ sont linéairement indépendantes. Trouver une base de F lorsque $a_1^2 > 4a_2$.

5) On suppose que $a_1^2 = 4a_2$. Montrer que si γ est un nombre réel qui vérifie $\gamma^2 + a_1\gamma + a_2 = 0$, la fonction $h(n) = n\gamma^n$ $(n \in \mathbf{Z})$ est dans F. Trouver une base de F.

Solution 1) Soient f_1, f_2 deux éléments de F et λ_1, λ_2 deux réels. Alors on a pour tout entier rationnel n :

$$\begin{aligned}(\lambda_1 f_1 + \lambda_2 f_2)(n) + a_1(\lambda_1 f_1 + \lambda_2 f_2)(n-1) + a_2(\lambda_1 f_1 + \lambda_2 f_2)(n-2) = \\ = \lambda_1\big(f_1(n) + a_1 f_1(n-1) + a_2 f_1(n-2)\big) + \\ + \lambda_2\big(f_2(n) + a_1 f_2(n-1) + a_2 f_2(n-2)\big) = 0\end{aligned}$$

donc $\lambda_1 f_1 + \lambda_2 f_2 \in F$ et F est un sous-espace vectoriel de E.

2) On a nécessairement $f(3) = -a_1 f(2) - a_2 f(1)$. Si on définit de proche en proche f jusqu'à $(n-1)$, on a nécessairement

$$f(n) = -a_1 f(n-1) - a_2 f(n-2).$$

D'autre part

$$f(0) = -\frac{1}{a_2}(a_1 f(1) + f(2))$$

et $$f(-p) = -\frac{1}{a_2}(a_1 f(-p+1) + f(-p+2)).$$

Donc il existe une seule fonction f de F vérifiant $f(1) = a$ et $f(2) = b$. Soient φ_1 la fonction de F définie par $\varphi_1(1) = 1$ et $\varphi_1(2) = 0$ et φ_2 la fonction de F définie par $\varphi_2(1) = 0$ et $\varphi_2(2) = 1$. Pour toute fonction f de F on a

$$f(1) = (f(1)\,\varphi_1 + f(2)\,\varphi_2) \quad (1)$$

et

$$f(2) = (f(1)\,\varphi_1 + f(2)\,\varphi_2)\,(2).$$

Puisque les fonctions de F sont définies par leurs valeurs sur 1 et 2, on a $f = f(1)\,\varphi_1 + f(2)\,\varphi_2$ donc (φ_1, φ_2) est un système générateur de F. D'autre part φ_1 et φ_2 sont linéairement indépendantes car

$$\lambda_1\,\varphi_1 + \lambda_2\,\varphi_2 = 0 \quad ((\lambda_1, \lambda_2) \in \mathbf{R} \times \mathbf{R})$$

entraîne $\lambda_1\,\varphi_1(1) + \lambda_2\,\varphi_2(1) = \lambda_1 = 0$ et $\lambda_1\,\varphi_1(2) + \lambda_2\,\varphi_2(2) = \lambda_2 = 0$. Donc (φ_1, φ_2) est une base de F et dim $F = 2$.

3) Si $f \in F$ on a $\alpha^n + a_1\,\alpha^{n-1} + a_2\,\alpha^{n-2} = 0$ c'est-à-dire $\alpha^2 + a_1\,\alpha + a_2 = 0$. La réciproque est immédiate donc f est dans F si et seulement si α est racine de l'équation $x^2 + a_1\,x + a_2 = 0$.

4) Soient λ et μ deux réels tels que $\lambda f + \mu g = 0$. Pour $n = 0$ on a $\lambda + \mu = 0$ et pour $n = 1$, $\lambda\alpha + \mu\beta = 0$; donc $\lambda = -\mu$ et $\lambda(\alpha - \beta) = 0$. Comme $\alpha \neq \beta$, $\lambda = \mu = 0$. Donc f et g sont linéairement indépendantes. Lorsque $a_1^2 > 4\,a_2$, l'équation $x^2 + a_1\,x + a_2 = 0$ admet deux racines réelles distinctes soient α et β. Les fonctions f et g définies par $f(n) = \alpha^n$, $g(n) = \beta^n$ $(n \in \mathbf{Z})$ étant linéairement indépendantes, forment une base de l'espace vectoriel F de dimension 2. Donc tout élément h de F s'écrit $h(n) = \lambda\alpha^n + \mu\beta^n$ $(n \in \mathbf{Z})$ avec $\lambda \in \mathbf{R}$ et $\mu \in \mathbf{R}$.

5) Comme $a_1^2 = 4\,a_2$ on a

$$\gamma^2 + a_1\,\gamma + \left(\frac{a_1}{2}\right)^2 = \left(\gamma + \frac{a_1}{2}\right)^2 = 0 \quad \text{donc} \quad \gamma = -\frac{a_1}{2}.$$

Soit n un entier rationnel ; on a

$$h(n) + a_1\,h(n-1) + a_2\,h(n-2) = n\gamma^n + a_1(n-1)\,\gamma^{n-1} + a_2(n-2)\,\gamma^{n-2} =$$
$$= n\gamma^{n-2}(\gamma^2 + a_1\,\gamma + a_2) - \gamma^{n-2}(a_1\,\gamma + 2\,a_2) = 0$$

donc $h \in F$. On sait que la fonction $k(n) = \gamma^n$ $(n \in \mathbf{Z})$ est dans F. Montrons que h et k sont linéairement indépendantes. Soient λ et μ deux réels tels que $\lambda h + \mu k = 0$; pour $n = 0$ on a $\mu = 0$ et pour $n = 1$ on a $\lambda\gamma + \mu\gamma = 0$ donc $\lambda = \mu = 0$. Alors (h, k) forme une base de F et tout élément f de F s'écrit

$$f(n) = (\lambda + \mu n)\,\gamma^n.$$

5.7 Soient E_1 et E_2 deux espaces vectoriels sur un corps commutatif K et p une application linéaire surjective de E_1 sur E_2. Si E est un espace vectoriel de dimension finie sur K et f une application linéaire définie sur E à valeurs dans E_2, montrer qu'il existe une application linéaire φ de E dans E_1 telle que $f = p \circ \varphi$.

Solution Soit $\{ e_1, e_2, ..., e_n \}$ une base de E. p étant surjective il existe des éléments a_i de E_1 ($1 \leqslant i \leqslant n$) tels que $p(a_i) = f(e_i)$. Alors (*cf.* Q., Ch. 7, § IV, n° 143, th. 6) il existe une application linéaire φ de E dans E_1 telle que $\varphi(e_i) = a_i$ pour $1 \leqslant i \leqslant n$. On a bien pour $1 \leqslant i \leqslant n$, $p \circ \varphi(e_i) = p(a_i) = f(e_i)$. Les applications $p \circ \varphi$ et f coïncident sur une base donc elles sont égales.

5.8 Soient E un espace vectoriel de dimension finie n sur un corps commutatif K et $\{ a_1, a_2, ..., a_n \}$ une base de E. Démontrer que p éléments de E ($p \leqslant n$) $x_1, x_2, ..., x_p$ sont linéairement indépendants si et seulement s'il existe un endomorphisme f de E tel que $f(x_k) = a_k$ pour $1 \leqslant k \leqslant p$.

Solution Supposons que $x_1, x_2, ..., x_p$ soient linéairement indépendants. On sait (*cf.* Q., Ch. 7, § III, n° 135) que l'on peut trouver des éléments $x_{p+1}, ..., x_n$ de E tels que $\{ x_1, x_2, ..., x_n \}$ soit une base de E. Alors (*cf.* Q., Ch. 7, § IV, n° 143, th. 6) il existe un endomorphisme f de E tel que $f(x_k) = a_k$ pour $1 \leqslant k \leqslant n$.

Réciproquement, supposons l'existence de l'endomorphisme f. Soient $\lambda^1, \lambda^2, ..., \lambda^p$ des éléments de K tels que

$$\sum_{k=1} \lambda^k x_k = 0 .$$

On a alors

$$f(0) = f\left(\sum_{k=1}^{p} \lambda^k x_k\right) = \sum_{k=1}^{p} \lambda^k f(x_k) = \sum_{k=1}^{p} \lambda^k a_k = 0$$

Les éléments a_k ($1 \leqslant k \leqslant p$) étant linéairement indépendants, la dernière égalité entraîne $\lambda^1 = \lambda^2 = \cdots = \lambda^p = 0$, ce qui prouve que les éléments $x_1, x_2, ..., x_p$ forment une famille libre.

5.9 E étant un espace vectoriel sur un corps commutatif K, on appelle *projecteur* tout endomorphisme p de E, tel que $p^2 = p \circ p = p$. On désigne par e l'identité de E.

a) Démontrer que p est un projecteur si et seulement si $e - p$ en est un. Montrer que si p est un projecteur les relations suivantes sont vérifiées

$$\operatorname{Im}(e - p) = \operatorname{Ker} p \tag{1}$$

$$\operatorname{Ker}(e - p) = \operatorname{Im} p\,. \tag{2}$$

b) Démontrer que si p est un projecteur, alors

$$E = \operatorname{Im} p \oplus \operatorname{Ker} p\,.$$

c) Démontrer qu'un projecteur p commute avec un endomorphisme u de E si et seulement si son noyau et son image sont stables par u.

Solution *a*) Supposons que p soit un projecteur. Alors

$$\begin{aligned}(e - p) \circ (e - p) &= e \circ e - p \circ e - e \circ p + p \circ p \\ &= e - p - p + p = e - p\,,\end{aligned}$$

donc $e - p$ est un projecteur. Réciproquement si $e - p$ est un projecteur, $(e - p) \circ (e - p) = e - p$, d'où $e - p = e - p - p + p \circ p$ ce qui entraîne $p \circ p = p$.

Soit y un élément de $\operatorname{Im}(e - p)$; il existe un élément x de E tel que

$$(e - p)(x) = y\,.$$

Mais alors

$$p(y) = p \circ (e - p)(x) = (p - p \circ p)(x) = 0\,,$$

donc $\operatorname{Im}(e - p) \subset \operatorname{Ker} p$. Soit x un élément de $\operatorname{Ker} p$; comme $p(x) = 0$ on a $x = x - p(x) = (e - p)(x)$ ce qui prouve que $\operatorname{Ker} p \subset \operatorname{Im}(e - p)$ d'où l'égalité (1).

Posons $p' = e - p$; la relation (1) devient $\operatorname{Ker} p' = \operatorname{Im}(e - p')$ c'est-à-dire $\operatorname{Ker}(e - p) = \operatorname{Im} p$.

b) Il suffit de montrer que $\operatorname{Im} p \cap \operatorname{Ker} p = \{0\}$ et que $E = \operatorname{Im} p + \operatorname{Ker} p$.

Commençons par montrer que $\operatorname{Im} p \cap \operatorname{Ker} p = \{0\}$. Soit x un élément de cette intersection. Il existe un élément y de E tel que $x = p(y)$; mais

$$0 = p(x) = p \circ p(y) = p(y) = x$$

donc le seul élément de l'intersection est bien 0. Pour montrer que

$$E = \operatorname{Im} p + \operatorname{Ker} p\,,$$

choisissons un élément z de E. On remarque que $z = p(z) + [z - p(z)]$. Comme $p(z - p(z)) = (p - p \circ p)(z) = 0$, $[z - p(z)]$ est un élément de Ker p ; par ailleurs $p(z)$ se trouve dans Im p d'où on déduit que z est somme d'un élément de Ker p et d'un élément de Im p.

c) Supposons que u et p commutent. Soit x un élément de Ker p, alors $p(u(x)) = u(p(x)) = u(0) = 0$ donc $u(x)$ est aussi dans Ker p et Ker p est stable par u. Si y est un élément de Im p, il existe un élément x de E tel que $y = p(x)$ et $u(y) = u(p(x)) = p(u(x))$ est encore dans Im p, donc Im p est stable par u. Réciproquement, supposons l'image et le noyau de p stables par u. Soit x un élément de E. D'après (*b*) nous savons qu'il existe un élément x_1 de Im p et un élément x_2 dans Ker p tels que $x = x_1 + x_2$; alors on a

$$u(p(x)) = u \circ p(x_1) + u \circ p(x_2) = u \circ p(x_1)$$

et

$$p(u(x)) = p \circ u(x_1) + p \circ u(x_2) .$$

Comme Ker p est stable par u, $u(x_2)$ est dans Ker p donc $p \circ u(x_2) = 0$. Im p étant stable par u, $u(x_1)$ est dans Im p et x_1 et $u(x_1)$ s'écrivent respectivement $x_1 = p(x_3)$ et $u(x_1) = p(x_4)$ ou x_3 et x_4 sont des éléments de E. On a alors

$$u \circ p(x) = u \circ p(x_1) = u \circ p \circ p(x_3) = u \circ p(x_3) = u(x_1)$$

et

$$p \circ u(x) = p \circ u(x_1) = p \circ p(x_4) = p(x_4) = u(x_1)$$

ce qui prouve que $u \circ p = p \circ u$.

5.10

Soient E un espace vectoriel de dimension finie n sur un corps commutatif K et f un endomorphisme de E. On pose :

$$f^0 = \mathrm{Id}\, E , \qquad f^k = f^{k-1} \circ f \quad (k \geqslant 1) ,$$
$$N_k = \mathrm{Ker}\, f^k \qquad \text{et} \qquad I_k = \mathrm{Im}\, f^k .$$

a) Démontrer que pour tout entier naturel k, on a

$$N_k \subset N_{k+1} \qquad \text{et} \qquad I_k \supset I_{k+1} .$$

b) Démontrer qu'il existe un entier naturel p tel que pour $k < p$ on ait $N_k \neq N_{k+1}$ et pour $k \geqslant p$, on ait $N_k = N_{k+1}$.

c) Démontrer que pour $k \leqslant p$, $I_k \neq I_{k+1}$ et pour $k \geqslant p$, $I_k = I_{k+1}$.

d) Démontrer que $E = I_p \oplus N_p$.

e) Démontrer que la restriction de f à I_p induit une fonction de I_p dans I_p qui est un automorphisme de I_p.

Solution *a*) Soit x un élément de N_k. On a $f^k(x) = 0$ d'où $f^{k+1}(x) = f[f^k(x)] = f(0) = 0$.
Donc $x \in N_{k+1}$ et $N_k \subset N_{k+1}$.
Soit y un élément de I_{k+1} ; alors il existe un élément x de E tel que $y = f^{k+1}(x) = f^k[f(x)]$ donc y est dans I_k et $I_{k+1} \subset I_k$.

b) La suite $(\dim N_k)_{k \in \mathbf{N}}$ est une suite infinie croissante d'entiers qui ne prend qu'un nombre fini de valeurs puisque pour tout entier k, $\dim N_k \leqslant n$; par suite il existe des entiers r tels que $\dim N_r = \dim N_{r+1}$ et comme $N_r \subset N_{r+1}$ on a $N_r = N_{r+1}$. Soit p le plus petit de ces entiers. On a forcément $N_k \neq N_{k+1}$ si $k < p$. Comme $N_p = N_{p+1}$, il suffit de démontrer que si $N_k = N_{k+1}$ on a $N_{k+1} = N_{k+2}$. On sait déjà que $N_{k+1} \subset N_{k+2}$. Montrons que si $N_k = N_{k+1}$ on a $N_{k+2} \subset N_{k+1}$. Soit x un élément de N_{k+2}. On a

$$f^{k+2}(x) = f^{k+1}(f(x)) = 0$$

donc $f(x)$ est un élément de N_{k+1} donc $f(x)$ est dans N_k et on a

$$f^k(f(x)) = f^{k+1}(x) = 0$$

ce qui prouve que $x \in N_{k+1}$ donc $N_{k+2} \subset N_{k+1}$. Donc p est bien l'entier cherché

c) Nous savons (*cf.* Q., Ch. 7, § IV, n° 143, th. 7) que pour tout entier k

$$\dim I_k = n - \dim N_k .$$

Donc pour $k < p$, $\dim I_k \neq \dim I_{k+1}$ d'où $I_k \neq I_{k+1}$. Pour $k \geqslant p$,

$$\dim I_k = \dim I_{k+1}$$

et comme nous savons que $I_{k+1} \subset I_k$, on a $I_k = I_{k+1}$.

d) Démontrons d'abord que $I_p \cap N_p = \{0\}$; soit y un élément de $I_p \cap N_p$, alors il existe un élément x de E tel que $y = f^p(x)$, on a $f^p(y) = f^{2p}(x) = 0$; comme x est dans N_{2p} qui est égal à N_p, $y = f^p(x) = 0$ donc $I_p \cap N_p = \{0\}$. A présent démontrons que $E = N_p + I_p$; soit x un élément de E, alors $f^p(x) \in I_p$ et $I_p = I_{2p}$ donc il existe un élément y de E tel que $f^p(x) = f^{2p}(y)$ donc $f^p(x - f^p(y)) = 0$ par suite

$$x - f^p(y) \in N_p , \quad f^p(x) \in I_p \quad \text{et} \quad x = (x - f^p(y)) + f^p(y) ,$$

d'où $E = N_p + I_p$ par suite $E = N_p \oplus I_p$.

e) Comme $f(I_p) \subset I_{p+1}$ et $I_{p+1} = I_p$, la restriction de f à I_p induit un endomorphisme de I_p. Comme I_p est de dimension finie, il suffit de montrer que cet endomorphisme est injectif ; soit y un élément de I_p tel que $f(y) = 0$, on a $y = f^p(x)$ avec $x \in E$; alors $f(y) = f^{p+1}(x) = 0$ donc $x \in N_{p+1}$, or $N_{p+1} = N_p$ par suite $x \in N_p$ d'où $y = f^p(x) = 0$ donc la restriction de f à I_p induit un automorphisme de I_p.

5.11 On appellera suite (a_i) toute suite finie strictement croissante de nombres réels vérifiant :

$$0 = a_0 < a_1 < \cdots < a_i < a_{i+1} < \cdots < a_n < a_{n+1} = 1 \qquad (1)$$

(n n'est pas forcément le même pour chaque suite).

On désigne par E l'ensemble des fonctions réelles en escalier définies sur $[0, 1[$, c'est-à-dire des fonctions f telles qu'il existe un entier n, une suite (a_i) vérifiant (1) et une suite (b_i) de $n + 1$ nombres réels quelconques tels que :

$$\text{pour tout } x \in [a_i, a_{i+1}[\text{ on a } f(x) = b_i \quad (i = 0, 1, ..., n). \qquad (2)$$

On désigne par L l'ensemble des fonctions linéaires par morceaux définies sur $[0, 1[$, c'est-à-dire des fonctions g telles qu'il existe un entier n, une suite (a_i) vérifiant (1) et deux suites (b_i) et (c_i) chacune de $n + 1$ nombres réels quelconques tels que :

$$\text{pour tout } x \in [a_i, a_{i+1}[, \text{ on a } g(x) = b_i x + c_i \quad (i = 0, 1, ..., n). \qquad (3)$$

1) *a*) Démontrer que E est un espace vectoriel sur $\mathbf{R}$.

b) Etant donné un nombre réel k tel que $0 \leqslant k < 1$, on désigne par e_k la fonction définie sur $[0, 1[$ en posant :

$$e_k(x) = 0 \quad \text{si} \quad 0 \leqslant x < k \; ; \quad e_k(x) = 1 \quad \text{si} \quad k \leqslant x < 1 .$$

Démontrer que si (k_i) est une suite finie de nombres réels distincts deux à deux ($0 \leqslant k_i < 1$), la famille (e_{k_i}) est une famille libre de E.

c) Démontrer que toute fonction en escalier de E s'écrit, de manière unique, sous forme d'une combinaison linéaire finie de fonctions e_k.

2) *a*) Démontrer que L est un espace vectoriel sur $\mathbf{R}$ et que l'ensemble L' des fonctions g linéaires par morceaux, continues sur $[0, 1[$ et telles que $g(0) = 0$, est un sous-espace vectoriel de L.

b) Etant donné un nombre réel k tel que $0 \leqslant k < 1$, on désigne par l_k la fonction définie sur $[0, 1[$ en posant :

$$l_k(x) = 0 \quad \text{si} \quad 0 \leqslant x < k \; ; \quad l_k(x) = x - k \quad \text{si} \quad k \leqslant x < 1 .$$

Démontrer que si (k_i) est une suite finie de nombres réels distincts deux à deux ($0 \leqslant k_i < 1$), la famille (l_{k_i}) est une famille libre de L.

c) Démontrer que tout élément de L' s'écrit de manière unique sous forme d'une combinaison linéaire finie de fonctions l_k.

d) Démontrer que L est somme directe de E et de L'.

Solution Etant donné deux suites (a_i) et (a'_j) vérifiant la condition (1) de l'énoncé, nous désignerons par $(a_i) * (a'_j)$ la suite (a''_k) dont l'ensemble des termes est la réunion de l'ensemble des termes de la suite (a_i) et de l'ensemble des termes de la suite (a'_j), l'indexation étant faite de manière à ce que la suite (a''_k) soit strictement croissante ; la suite $(a_i) * (a'_j)$ ainsi obtenue vérifie alors la condition (1) de l'énoncé puisque son premier terme est 0 ($a_0 = a'_0 = 0$) et son dernier terme est 1 (dernier terme commun des suites (a_i) et (a'_j)). Observons de plus que tout intervalle de la forme $[a''_k, a''_{k+1}[$ est contenu dans un intervalle et un seul de la forme $[a_i, a_{i+1}[$ et dans un intervalle et un seul de la forme $[a'_j, a'_{j+1}[$.

1) *a*) Il suffit de vérifier que E est un sous-espace vectoriel de $\mathscr{F}([0, 1[, \mathbf{R})$ c'est-à-dire que si $f \in E$, $f' \in E$ et $\alpha \in \mathbf{R}$, on a $(f - f') \in E$ et $\alpha . f \in E$. Soient donc f, f' deux fonctions en escalier sur $[0, 1[$, (a_i) et (b_i) les suites associées à f, (a'_j) et (b'_j) les suites associées à f' ; formons la suite $(a_i) * (a'_j) = (a''_k)$; alors chaque intervalle $[a''_k, a''_{k+1}[$ est contenu dans un intervalle et un seul, de la forme $[a_i, a_{i+1}[$ soit $[a_{i(k)}, a_{i(k)+1}[$ et dans un intervalle et un seul de la forme $[a'_j, a'_{j+1}[$ soit $[a'_{j(k)}, a'_{j(k)+1}[$, donc pour tout $x \in [a''_k, a''_{k+1}[$ on a : $(f - f')(x) = b_{i(k)} - b'_{j(k)}$ ce qui montre que $(f - f')$ est une fonction en escalier définie par les suites $(a_i) * (a'_j)$ et $(b_{i(k)} - b_{j(k)})$.

Par ailleurs, si $\alpha \in \mathbf{R}$, la fonction $\alpha . f$ est la fonction en escalier définie par les suites (a_i) et (αb_i) donc E est un espace vectoriel.

b) Soit $(k_i)_{1 \leqslant i \leqslant n}$ une suite finie d'éléments de $[0, 1[$ distincts deux à deux ; sans restreindre la généralité on peut supposer que ces éléments ont été classés de telle manière que :

$$0 \leqslant k_1 < k_2 < \cdots < k_i < k_{i+1} < \cdots < k_{n-1} < k_n < 1 .$$

Soient $\alpha_1, \alpha_2, \ldots, \alpha_n$ des nombres réels tels que l'on ait :

$$\sum_{i=1}^{n} \alpha_i e_{k_i} = 0 .$$

Nous allons montrer par récurrence sur p que $\alpha_p = 0$ $(1 \leqslant p \leqslant n)$. Tout d'abord soit $x \in [k_1, k_2[$, alors on a $e_{k_1}(x) = 1$ et $e_{k_j}(x) = 0$ si $2 \leqslant j \leqslant n$, donc

$$\sum_{i=1}^{n} \alpha_i e_{k_i}(x) = \alpha_1 e_{k_1}(x) = \alpha_1 = 0 .$$

Supposons que $\alpha_1 = \alpha_2 = \cdots = \alpha_p = 0$ (avec p tel que $1 \leqslant p < n$), alors on a :

$$\sum_{i=1}^{n} \alpha_i e_{k_i} = \sum_{i=p+1}^{n} \alpha_i e_{k_i} ;$$

prenons $x \in [k_{p+1}, k_{p+2}[$ si $p + 1 < n$ ou $x \in [k_n, 1[$ si $p + 1 = n$, alors on a :

$$e_{k_{p+1}}(x) = 1 \qquad \text{et} \qquad e_{k_q}(x) = 0$$

si $q > p + 1$, donc

$$\sum_{i=p+1}^{n} \alpha_i e_{k_i}(x) = \alpha_{p+1} e_{k_{p+1}}(x) = \alpha_{p+1} = 0,$$

par suite $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$, ce qui montre que la famille (e_{k_i}) est une famille libre de E.

c) Observons que si k est un nombre réel $(0 \leqslant k < 1)$ la suite (a_i) attachée à la fonction e_k est la suite a_0, a_1, a_2 avec $a_0 = 0$, $a_1 = k$, $a_2 = 1$, par ailleurs (*cf.* démonstration de *a*) pour tout réel α, la suite (a_i) attachée à la fonction $\alpha . e_k$ est la même que celle qui est attachée à la fonction e_k, et si k et k' sont deux réels distincts $(0 \leqslant k < 1, 0 \leqslant k' < 1)$ avec par exemple $k < k'$, la suite (a_i) attachée à la fonction $e_k + e_{k'}$ (et aussi à toute fonction de la forme $\alpha e_k + \alpha' e_{k'}$; $\alpha \in \mathbf{R}$, $\alpha' \in \mathbf{R}$) est la suite : $0, k, k', 1$. Il résulte de tout ceci que si $k_1, k_2, \ldots, k_n$ sont des nombres réels tels que : $0 \leqslant k_1 < k_2 < \cdots < k_n < 1$ et $\alpha_1, \ldots, \alpha_n$ des nombres réels quelconques, la suite (a_i) attachée à la fonction $\sum_{i=1}^{n} \alpha_i e_{k_i}$ est la suite : $0, k_1, k_2, \ldots, k_n, 1$.

Soient à présent f une fonction en escalier sur $[0, 1[$, $(a_i)_{0 \leqslant i \leqslant n+1}$ et $(b_i)_{0 \leqslant i \leqslant n}$ les suites telles que :

$$0 = a_0 < a_1 < a_2 < \ldots < a_i < a_{i+1} < \cdots < a_n < a_{n+1} = 1 \qquad (1)$$

et que, pour tout $x \in [a_i, a_{i+1}[$ on ait : $f(x) = b_i (i = 0,1, \ldots, n)$.

De la remarque précédente il résulte que si f s'écrit sous la forme $\sum_{i=0}^{m} \alpha_i e_{ki}$ avec $0 = k_0 < k_1 < \cdots < k_i < k_{i+1} < \cdots < k_m < 1$, on a nécessairement $m = n$ et $a_i = k_i$ pour tout $i = 0, 1, \ldots, n$. Cherchons donc une décomposition de f en combinaison linéaire des fonctions $e_{a_0}, e_{a_1}, \ldots, e_{an}$; si $f = \sum_{i=0}^{n} \alpha_i e_{ai}$ on a pour $x \in [a_0, a_1[$, $e_{a_0}(x) = 1$ et $e_{a_j}(x) = 0$ si $1 \leqslant j \leqslant n$, donc

$$f(x) = b_0 = \alpha_0 e_{a_0}(x) = \alpha_0 \quad \text{et} \quad f = b_0 e_{a_0} + \sum_{i=1}^{n} \alpha_i e_{a_i};$$

à présent si $x \in [a_1, a_2[$ on a $e_{a_0}(x) = e_{a_1}(x) = 1$ et $e_{a_j}(x) = 0$ si $2 \leqslant j \leqslant n$, donc $f(x) = b_1 = b_0 + \alpha_1$ et $\alpha_1 = b_1 - b_0$. Supposons que $\alpha_q = b_q - b_{q-1}$ pour $q = 1, 2, \ldots, p$ avec $1 \leqslant p < n$, alors prenons $x \in [a_{p+1}, a_{p+2}[$ si $p + 1 < n$ et $x \in [a_n, 1[$ si $p + 1 = n$; on a $e_{a_0}(x) = e_{a_1}(x) = \cdots = e_{a_{p+1}}(x) = 1$ et $e_{a_q}(x) = 0$ si $q > p + 1$, donc

$$f(x) = b_{p+1} = b_0 + (b_1 - b_0) + \cdots + (b_p - b_{p-1}) + \alpha_{p+1}$$

d'où $\alpha_{p+1} = b_{p+1} - b_p$, par suite pour tout entier $q = 1, 2, \ldots, n$, $\alpha_q = b_q - b_{q-1}$ et

$$f = \sum_{i=0}^{n} \alpha_i e_{a_i}.$$

Si maintenant on suppose que $f = \sum_{i=0}^{m} \alpha'_i e_{a'_i}$ avec

$$0 = a'_0 < a_1 < \cdots < a'_m < a'_{m+1} = 1,$$

on a vu que nécessairement $n = m$ et $a'_i = a_i$ pour $i = 0, 1, ..., n$, donc on a

$$\sum_{i=0}^{n} \alpha'_i e_{a_i} = \sum_{i=0}^{n} \alpha_i e_{a_i} \qquad \text{d'où} \qquad \sum_{i=0}^{n} (\alpha_i - \alpha'_i) e_{a_i} = 0$$

or les éléments de la suite (a_i) étant deux à deux distincts, la famille (e_{a_i}) est une famille libre de E, donc on a $\alpha_i = \alpha'_i$ pour tout $i = 0, 1, ..., n$.

2) *a*) Comme en 1) *a*) il suffit de vérifier que L est un sous-espace vectoriel de $\mathscr{F}([0, 1[, \mathbf{R})$ et L' un sous-espace vectoriel de L. Soient f et f' deux fonctions linéaires par morceaux sur $[0, 1[$ (a_i), (b_i), (c_i) les suites associées à f, et (a'_j), (b'_j), (c'_j) les suites associées à f' ; formons la suite $(a''_k) = (a_i) * (a'_j)$; chaque intervalle $[a''_k, a''_{k+1}[$ est contenu dans un intervalle et un seul de la forme $[a_i, a_{i+1}[$ soit $[a_{i(k)}, a_{i(k)+1}[$ et dans un intervalle et un seul de la forme $[a'_j, a'_{j+1}[$ soit $[a'_{j(k)}, a'_{j(k)+1}[$, donc pour tout $x \in [a''_k, a''_{k+1}[$ on a

$$(f - f')(x) = (b_{i(k)} - b'_{j(k)})\, x + (c_{i(k)} - c'_{j(k)})$$

donc $(f - f') \in L$; par ailleurs si $\alpha \in \mathbf{R}$, la fonction $\alpha.f$ est la fonction linéaire par morceaux définie par les suites (a_i), $(\alpha.b_i)$ et $(\alpha.c_i)$ donc L est un espace vectoriel.

Si maintenant $g \in L'$ et $g' \in L'$, on a $(g - g') \in L$, $g - g'$ est continue et $(g - g')(0) = g(0) - g'(0) = 0$ donc $(g - g') \in L'$; de plus si $\alpha \in \mathbf{R}$, αg est continue et $\alpha g(0) = 0$ donc $\alpha g \in L'$ et L' est un sous-espace vectoriel de L.

b) Soient $(k_i)_{1 \leqslant i \leqslant n}$ une suite finie d'éléments de $[0, 1[$ distincts deux à deux que nous supposons classés de telle manière que :

$$0 \leqslant k_1 < k_2 < \cdots < k_{n-1} < k_n < 1$$

et $\alpha_1, \alpha_2, ..., \alpha_n$ des nombres réels, tels que l'on ait : $\sum_{i=1}^{n} \alpha_i l_{k_i} = 0$; montrons, par récurrence sur p que $\alpha_p = 0$ $(1 \leqslant p \leqslant n)$. Tout d'abord si $x \in]k_1, k_2[$ on a $l_{k_1}(x) = x - k_1$ et $l_{k_j}(x) = 0$ si $2 \leqslant j \leqslant n$, donc

$$\sum_{i=1}^{n} \alpha_i\, l_{k_i}(x) = \alpha_1(x - k_1) = 0$$

or $x - k_1 \neq 0$ donc $\alpha_1 = 0$.

Supposons que $\alpha_1 = \alpha_2 = \cdots = \alpha_p = 0$ (avec p tel que $1 \leqslant p < n$), alors on a :

$$\sum_{i=1}^{n} \alpha_i\, l_{k_i} = \sum_{i=p+1}^{n} \alpha_i\, l_{k_i} = 0\,;$$

prenons $x \in]k_{p+1}, k_{p+2}[$ si $p + 1 < n$ ou $]k_n, 1[$ si $p + 1 = n$, alors on a $l_{k_{p+1}}(x) = x - k_{p+1}$ et $l_{k_q}(x) = 0$ si $q > p + 1$, donc

$$\sum_{i=p+1}^{n} \alpha_i\, l_{k_i}(x) = \alpha_{p+1}(x - k_{p+1}) = 0$$

et $x - k_{p+1} \neq 0$ donc $\alpha_{p+1} = 0$ par suite $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$, ce qui montre que la famille (l_{k_i}) est une famille libre de L.

c) Soient f un élément de L' et $(a_i)_{0 \leqslant i \leqslant n+1}$, $(b_i)_{0 \leqslant i \leqslant n}$ et $(c_i)_{0 \leqslant i \leqslant n}$ les suites associées à f. Alors on a : $c_0 = 0$ et la continuité de f s'exprime par les conditions

$$b_i\, a_{i+1} + c_i = b_{i+1}\, a_{i+1} + c_{i+1} \qquad (i = 0, 1, \ldots, n-1) \tag{1'}$$

qui s'écrivent aussi

$$c_{i+1} = \sum_{j=0}^{i} (b_j - b_{j+1})\, a_{j+1} \qquad (i = 0, 1, \ldots, n-1)\,. \tag{2'}$$

Supposons que $f = \sum_{i=0}^{m} \alpha_i\, l_{k_i}$ où les k_i sont des nombres réels tels que

$$k_0 = 0 < k_1 < k_2 < \cdots < k_m < 1\ ;$$

un argument analogue à celui employé dans 1) *c*) montre que l'on a nécessairement $m = n$ et $k_i = a_i$ pour tout $i = 0, 1, \ldots, n$. Cherchons donc une décomposition de f en combinaison linéaire des fonctions $l_{a_0}, l_{a_1}, \ldots, l_{a_n}$.

Si $f = \sum_{i=0}^{n} \alpha_i\, l_{a_i}$, on a pour tout $x \in\,]a_0, a_1[$, $l_{a_0}(x) = x - a_0$ et $l_{a_j}(x) = 0$ si $1 \leqslant j \leqslant n$, donc $f(x) = b_0\, x = \alpha_0\, x$ d'où $\alpha_0 = b_0$ (car $x \neq 0$) et

$$f = b_0\, l_{a_0} + \sum_{i=1}^{n} \alpha_i\, l_{a_i}\ ;$$

à présent si $x \in\,]a_1, a_2[$ on a $l_{a_0}(x) = x$, $l_{a_1}(x) = x - a_1$ et $l_{a_j}(x) = 0$ si $2 \leqslant j \leqslant n$ donc $f(x) = b_1\, x + c_1 = b_0\, x + \alpha_1(x - a_1) = (b_0 + \alpha_1)\, x - \alpha_1\, a_1$, d'où par identification des coefficients de x, $\alpha_1 = b_1 - b_0$ (l'identification des termes constants fournit alors l'égalité $c_1 = (b_0 - b_1)\, a_1$, vraie en vertu des conditions 2).

Supposons que $\alpha_q = b_q - b_{q-1}$ pour $q = 1, 2, \ldots, p$ avec $1 \leqslant p < n$ et soit $x \in\,]a_{p+1}, a_{p+2}[$ si $p + 1 < n$ ou $x \in\, [a_n, 1[$ si $p + 1 = n$; alors on a

$$l_{a_{p+1}}(x) = x - a_{p+1} \quad \text{et} \quad l_{a_q}(x) = 0 \quad \text{si} \quad q > p + 1\,,$$

donc

$$f(x) = b_{p+1}\, x + c_{p+1} = \sum_{i=0}^{p} \alpha_i\, l_{a_i}(x) + \alpha_{p+1}(x - a_{p+1})$$

$$= \sum_{i=0}^{p} \alpha_i (x - a_i) + \alpha_{p+1}(x - a_{p+1})$$

$$= \sum_{i=0}^{p} \alpha_i\, x - \sum_{i=0}^{p} \alpha_i\, a_i + \alpha_{p+1}\, x - \alpha_{p+1}\, a_{p+1}$$

or

$$\sum_{i=0}^{p} \alpha_i = b_0 + (b_1 - b_0) + \cdots + (b_p - b_{p-1}) = b_p$$

d'où par identification des coefficients de x : $\alpha_{p+1} = b_{p+1} - b_p$ (l'identification des termes constants fournit alors l'égalité

$$c_{p+1} = \sum_{i=0}^{p+1} \alpha_i a_i = \sum_{i=0}^{p} (b_i - b_{i+1}) a_{i+1} \qquad (\text{car } a_0 = 0)$$

qui est vraie en vertu des conditions 2'). On a donc pour tout entier $q = 1, 2, ..., n$,

$$\alpha_q = b_q - b_{q-1} \qquad \text{et} \qquad f = \sum_{i=0}^{n} \alpha_i l_{a_i} .$$

Si maintenant on suppose que $f = \sum_{i=0}^{m} \alpha'_i l_{a'_i}$ avec

$$a'_0 = 0 < a'_1 < a'_2 < \cdots < a'_m < a'_{m+1} = 1 ,$$

on a vu que nécessairement $m = n$ et $a_i = a'_i$ pour $i = 0, 1, ..., n$, donc on a

$$\sum_{i=0}^{n} (\alpha_i - \alpha'_i) l_{a_i} = 0 ,$$

or les éléments de la suite (a_i) sont deux à deux distincts, donc la famille (l_{a_i}) est une famille libre de L, donc on a $\alpha_i = \alpha'_i$ pour tout $i = 0, 1, ..., n$.

d) E et L' sont deux sous-espaces vectoriels de L et on a $E \cap L' = \{ 0 \}$, en effet, si $f \in E \cap L'$, f est une fonction en escalier continue donc constante sur $[0, 1[$ telle que $f(0) = 0$ donc $f = 0$. Pour démontrer que L est somme directe de E et de L' il suffira de démontrer que tout élément de L s'écrit, au moins d'une manière sous la forme d'une somme d'un élément de E et d'un élément de L'. Soient f une fonction linéaire par morceaux sur $[0, 1[$ et $(a_i)_{0 \leqslant i \leqslant n+1}$, $(b_i)_{0 \leqslant i \leqslant n}$ et $(c_i)_{0 \leqslant i \leqslant n}$ les suites associées à f ; nous allons définir une fonction en escalier g sur $[0, 1[$ telle que $(f - g) \in L'$ (on aura alors $f = (f - g) + g$ d'où le résultat). Si g est une fonction en escalier sur $[0, 1[$ définie par les suites (a_i) (intervenant dans la définition de f) et $(d_i)_{0 \leqslant i \leqslant n}$ alors, pour tout $x \in [a_i, a_{i+1}[$ on a $(f - g)(x) = b_i x + c_i - d_i$ $(i = 0, 1, ..., n)$ or $(f - g) \in L'$ si et seulement si $(f - g)(0) = 0$ et

$$c_{i+1} - d_{i+1} = \sum_{j=0}^{i} (b_j - b_{j+1}) a_{j+1} \qquad (i = 0, 1, ..., n - 1)$$

(conditions 2' exprimant la continuité de $(f - g)$), donc en posant $d_0 = c_0$ et

$$d_{i+1} = c_{i+1} - \sum_{j=0}^{i} (b_j - b_{j+1}) a_{j+1} \qquad (i = 0, 1, ..., n - 1)$$

on définit une fonction en escalier g sur $[0, 1[$ telle que $f - g \in L'$ d'où $L = E \oplus L'$.

5.12 E étant un espace vectoriel de dimension finie supérieure ou égale à 2 sur un corps commutatif K, on désigne par f un endomorphisme non nul de E commutant avec tout automorphisme de E.

a) Montrer que si x et y sont deux éléments linéairement indépendants de E, il existe un automorphisme u de E tel que $u(x) = x$ et $u(y) = x + y$.

b) Soit a un élément de E n'appartenant pas à Ker f. Démontrer que les vecteurs a et $b = f(a)$ sont liés. En déduire l'existence d'un élément $\lambda(a)$ de K tel que $f(a) = \lambda(a).a$.

c) Démontrer que $\lambda(a)$ ne dépend pas de a.

d) Quel est le centre de l'anneau $\mathscr{L}(E)$?

Solution *a*) Soit n la dimension de E. Si x et y sont linéairement indépendants on sait (*cf.* Q., Ch. 7, § III, n° 135, th. 4) qu'il existe des éléments $e_3, ..., e_n$ dans E tels que $\{ x, y, e_3, ..., e_n \}$ forme une base de E. On définit l'application linéaire u par ses valeurs sur cette base : $u(x) = x$, $u(y) = x + y$, $u(e_i) = e_i (3 \leqslant i \leqslant n)$. Pour voir que u est un automorphisme il suffit de prouver que

$$\{ x, x + y, e_3, ..., e_n \}$$

est une base de E (*cf.* Q. Ch. 7. § IV, n° 143) et pour ceci, il suffit de vérifier que ces n vecteurs sont linéairement indépendants. Soient $\lambda_1, \lambda_2, ..., \lambda_n$ des éléments de K tels que $\lambda_1 x + \lambda_2(x + y) + \lambda_3 e_3 + \cdots + \lambda_n e_n = 0$. On a alors

$$(\lambda_1 + \lambda_2) x + \lambda_2 y + \lambda_3 e_3 + \cdots + \lambda_n e_n = 0$$

et comme les vecteurs $x, y, e_3, ..., e_n$ sont linéairement indépendants :

$$\lambda_1 + \lambda_2 = \lambda_2 = \lambda_3 = \cdots = \lambda_n = 0 \quad \text{d'où} \quad \lambda_1 = \lambda_2 = \lambda_3 = \cdots = \lambda_n = 0 .$$

Par suite u est un automorphisme de E répondant à la question.

b) Supposons que a et b soient linéairement indépendants (supposition justifiée puisque $b \neq 0$). Soit u un automorphisme de E tel que

$$u(a) = a \quad \text{et} \quad u(b) = a + b .$$

Alors $f \circ u(a) = f(a) = b$ et $u \circ f(a) = u(b) = a + b$ donc f et u ne commutent pas ce qui contredit l'hypothèse. Les vecteurs a et b étant liés il existe un scalaire $\lambda(a)$ tel que $b = f(a) = \lambda(a).a$.

c) Considérons deux éléments a_1 et a_2 de E, distincts et non nuls. Soit v un automorphisme de E tel que $v(a_1) = a_2$. Comme f et v commutent on a

$$f \circ v(a_1) = f(a_2) = \lambda(a_2).a_2 = v \circ f(a_1) = v(\lambda(a_1).a_1)$$
$$= \lambda_1(a_1).v(a_1) = \lambda(a_1).a_2 .$$

Comme $a_2 \neq 0$, $\lambda(a_2).a_2 - \lambda(a_1).a_2 = 0$ entraîne $\lambda(a_1) = \lambda(a_2)$ ce qui prouve que $\lambda(a)$ ne dépend pas de a.

d) On a démontré que tout élément f du centre de $\mathscr{L}(E)$ est de la forme $f(x) = \lambda.x$ où $\lambda \in K$. Réciproquement si λ est un élément de K, f l'endomorphisme de E défini par $f(x) = \lambda.x$ et u un endormophisme de E, on a pour tout élément x de E, $f(u(x)) = \lambda.u(x) = u(\lambda x) = u(f(x))$ donc $f \circ u = u \circ f$. Par suite, le centre de $\mathscr{L}(E)$ est l'ensemble des homothéties de E.

5.13 E_0, E_1, E_2 étant des espaces vectoriels sur le même corps commutatif K, f_0 une application linéaire de E_0 dans E_1 et f_1 une application linéaire de E_1 dans E_2 on dira que

$$E_0 \xrightarrow{f_0} E_1 \xrightarrow{f_1} E_2$$

est une *suite exacte* si et seulement si $\operatorname{Im} f_0 = \operatorname{Ker} f_1$.

$E_0, E_1, \ldots, E_n$ étant des espaces vectoriels sur K et f_k $(0 \leqslant k \leqslant n-1)$ des applications linéaires définies sur E_k à valeurs dans E_{k+1}, on dit que la suite

$$E_0 \xrightarrow{f_0} E_1 \xrightarrow{f_1} E_2 \xrightarrow{f_2} \ldots \xrightarrow{f_{n-2}} E_{n-1} \xrightarrow{f_{n-1}} E_n$$

est *exacte en* E_k $(1 \leqslant k \leqslant n-1)$ si et seulement si la suite

$$E_{k-1} \xrightarrow{f_{k-1}} E_k \xrightarrow{f_k} E_{k+1}$$

est exacte.

La suite

$$E_0 \xrightarrow{f_0} E_1 \xrightarrow{f_1} E_2 \xrightarrow{f_2} \ldots \xrightarrow{f_{n-2}} E_{n-1} \xrightarrow{f_{n-1}} E_n$$

sera dite *exacte* si et seulement si pour tout k, $1 \leqslant k \leqslant n-1$, elle est exacte en E_k. Si $E_k = \{0\}$ on le notera 0 et on n'écrira pas f_{k-1} et f_k puisque ces applications sont uniquement déterminées.

a) Démontrer que f_0 est injective si et seulement si

$$0 \to E_0 \xrightarrow{f_0} E_1$$

est une suite exacte.

b) Démontrer que f_0 est surjective si et seulement si

$$E_0 \xrightarrow{f_0} E_1 \to 0$$

est une suite exacte.

c) E et F étant des espaces vectoriels, f une application linéaire de E dans F et G un sous-espace vectoriel de E, montrer que l'on a les suites exactes :

$$0 \to G \xrightarrow{i_1} E \xrightarrow{s_1} E/G \to 0 \qquad (1)$$

$$0 \to \operatorname{Ker} f \xrightarrow{i_2} E \xrightarrow{f} F \xrightarrow{s_2} F/\operatorname{Im} f \to 0 \qquad (2)$$

où i_1 et i_2 désignent les injections canoniques de G et $\operatorname{Ker} f$ dans E et s_1, s_2 les surjections canoniques.

Solution *a*) f_0 est injective si et seulement si $\operatorname{Ker} f_0 = \{ 0 \}$ (*cf.* Q., Ch. 7, § IV, n° 140) ce qui est équivalent à l'exactitude de la suite

$$0 \to E_0 \xrightarrow{f_0} E_1 .$$

b) f_0 est surjective si et seulement si $\operatorname{Im} f_0 = E_1$ c'est-à-dire si et seulement si, la suite

$$E_0 \xrightarrow{f_0} E_1 \to 0$$

est exacte.

c) (1) i_1 étant injective et s_1 surjective, les résultats (*a*) et (*b*) permettent d'affirmer que la suite (1) est exacte en G et E/G. Comme on a

$$i_1(G) = G = \operatorname{Ker} s_1 ,$$

la suite (1) est aussi exacte en E donc est exacte.

(2) Comme précédemment la suite (2) est exacte en $\operatorname{Ker} f$ et $F/\operatorname{Im} f$ parce que i_2 est injective et s_2 surjective. Comme $i_2(\operatorname{Ker} f) = \operatorname{Ker} f$ et $\operatorname{Ker} s_2 = \operatorname{Im} f$, la suite (2) est exacte en E et F donc est exacte.

5.14 *a*) Soient $E_0, E_1, \ldots, E_n$ des espaces vectoriels de dimension finie et $f_0, f_1, \ldots, f_{n-1}$ des applications linéaires telles que la suite

$$0 \to E_0 \xrightarrow{f_0} E_1 \xrightarrow{f_1} E_2 \xrightarrow{f_2} \ldots \xrightarrow{f_{n-2}} E_{n-1} \xrightarrow{f_{n-1}} E_n \to 0$$

soit exacte (*cf.* exercice 5.13).

Montrer que

$$\sum_{1 \leqslant 2h+1 \leqslant n} \dim E_{2h+1} = \sum_{0 \leqslant 2h \leqslant n} \dim E_{2h}$$

et que

$$\sum_{k=0}^{n} (-1)^k \dim E_k = 0 .$$

b) E et F étant deux espaces vectoriels de dimension finie, soient

$$f : E \cap F \to E \qquad \text{et} \qquad g : E \cap F \to F$$

les injections canoniques. On définit une fonction h sur $E \oplus F$ à valeurs dans $E + F$ de la manière suivante : si x est un élément de $E \oplus F$, il s'écrit de manière unique $x = x_1 + x_2$ avec $x_1 \in E$ et $x_2 \in F$. On pose $h(x) = x_1 - x_2$. Montrer que h est une application linéaire et que la suite

$$0 \to E \cap F \xrightarrow{f+g} E \oplus F \xrightarrow{h} E + F \to 0$$

est exacte. En déduire que

$$\dim (E \cap F) + \dim (E + F) = \dim E + \dim F .$$

Solution *a*) On sait (*cf.* Q., Ch. 7, § IV, n° 143, th. 7) que

$$\operatorname{rg} f_k = \dim E_k - \dim \operatorname{Ker} f_k \qquad (0 \leqslant k \leqslant n-1).$$

La suite étant exacte on a $\operatorname{Ker} f_k = \operatorname{Im} f_{k-1}$ donc

$$\operatorname{rg} f_k = \dim E_k - \operatorname{rg} f_{k-1}.$$

Comme $\operatorname{Ker} f_0 = 0$ et $\operatorname{Im} f_{n-1} = E_n$, on trouve :

$$\begin{aligned}
\dim E_0 &= \operatorname{rg} f_0 \\
\dim E_1 &= \operatorname{rg} f_1 + \operatorname{rg} f_0 \\
&\vdots \\
\dim E_{n-1} &= \operatorname{rg} f_{n-1} + \operatorname{rg} f_{n-2} \\
\dim E_n &= \operatorname{rg} f_{n-1}.
\end{aligned}$$

En sommant membre à membre ces égalités, on obtient :

$$\sum_{1 \leqslant 2h+1 \leqslant n} \dim E_{2h+1} = \sum_{1 \leqslant 2h+1 \leqslant n} \operatorname{rg} f_{2h+1} + \sum_{0 \leqslant 2h \leqslant n} \operatorname{rg} f_{2h} = \sum_{k=0}^{n} \operatorname{rg} f_k$$

$$\sum_{0 \leqslant 2h \leqslant n} \dim E_{2h} = \sum_{0 \leqslant 2h \leqslant n} \operatorname{rg} f_{2h} + \sum_{1 \leqslant 2h-1 \leqslant n} \operatorname{rg} f_{2h-1} = \sum_{k=0}^{n} \operatorname{rg} f_k.$$

On a donc bien

$$\sum_{1 \leqslant 2h+1 \leqslant n} \dim E_{2h+1} = \sum_{0 \leqslant 2h \leqslant n} \dim E_{2h}$$

d'où en mettant tous les termes de cette égalité dans un même membre

$$\sum_{k=0}^{n} (-1)^k \dim E_k = 0.$$

b) *Linéarité de h.* Soient x et y deux éléments de $E \oplus F$, $x = x_1 + x_2$, $y = y_1 + y_2$ leurs décompositions en somme d'un élément de E et d'un élément de F et λ et μ deux éléments de K. Alors on a :

$$\lambda x + \mu y = \lambda(x_1 + x_2) + \mu(y_1 + y_2) = (\lambda x_1 + \mu y_1) + (\lambda x_2 + \mu y_2).$$

Comme $\lambda x_1 + \mu y_1$ est dans E et $\lambda x_2 + \mu y_2$ dans F, on a nécessairement :

$$(\lambda x + \mu y)_1 = \lambda x_1 + \mu y_1 \qquad \text{et} \qquad (\lambda x + \mu y)_2 = \lambda x_2 + \mu y_2 ;$$

donc

$$h(\lambda x + \mu y) = (\lambda x_1 + \mu y_1) - (\lambda x_2 + \mu y_2) = \lambda(x_1 - x_2) + \mu(y_1 - y_2) = \\ = \lambda h(x) + \mu h(y) ;$$

ce qui prouve que h est une application linéaire.

Exactituae en $E \cap F$. Il suffit de démontrer que $\operatorname{Ker}(f+g) = \{0\}$. Soit a un élément de $E \cap F$ tel que $(f+g)(a) = f(a) + g(a) = 0$. Comme $f(a)$ est dans E et $g(a)$ dans F et comme 0 se décompose de manière unique en somme d'un élément de E et d'un élément de F, on a nécessairement $f(a) = g(a) = 0$ d'où $a = 0$ puisque f est injective.

Exactitude en $E \oplus F$. Montrons d'abord que $\operatorname{Im}(f+g) \subset \operatorname{Ker} h$. Soit y un élément de $\operatorname{Im}(f+g)$; il existe un élément a de $E \cap F$ tel que

$$y = (f+g)(a) = f(a) + g(a) .$$

Comme $f(a)$ est dans E et $g(a)$ dans F, on a

$$y_1 = f(a) , y_2 = g(a) \quad \text{d'où} \quad h(y) = f(a) - g(a) = a - a = 0 .$$

Il en résulte que $\operatorname{Im}(f+g) \subset \operatorname{Ker} h$.

A présent soit x un élément de $E \oplus F$ tel que $h(x) = x_1 - x_2 = 0$; alors $x_1 = x_2$ est un élément de $E \cap F$ et $x = x_1 + x_2 = f(x_1) + g(x_1) = (f+g)(x_1)$; on a donc aussi $\operatorname{Ker} h \subset \operatorname{Im}(f+g)$ donc $\operatorname{Ker} h = \operatorname{Im}(f+g)$.

Exactitude en $E + F$. Il faut montrer que h est surjective. Soit z un élément de $E + F$; il existe un élément x de E et un élément y de F tel que $z = x + y$; alors $h(x - y) = x - (-y) = x + y = z$, il en résulte que la suite est exacte en $E + F$.

En appliquant à la suite exacte

$$0 \to E \cap F \xrightarrow{f+g} E \oplus F \xrightarrow{h} E + F \to 0$$

le résultat (*a*) on trouve

$$\dim(E \cap F) + \dim(E + F) = \dim(E \oplus F) = \dim E + \dim F .$$

5.15 Soit E une algèbre sur un corps commutatif K. On désigne par $\mathscr{L}(E)$ l'algèbre des endomorphismes de E (considérée comme espace vectoriel sur K). Un endomorphisme D de E est appelé une *dérivation* dans E s'il vérifie la condition suivante :

$$(\forall (x, y) \in E \times E) \quad [D(xy) = D(x)\, y + xD(y)] . \tag{1}$$

On désigne par $\mathscr{D}(E)$ l'ensemble des dérivations de E. Pour tout endomorphisme f de E on pose $f^0 = \operatorname{Id} E$ et pour tout entier naturel $n > 0$, $f^n = f^{n-1} \circ f$.

a) Soit e l'élément neutre de E. Montrer que l'application φ de K dans E définie par $\varphi(\alpha) = \alpha e$ pour tout $\alpha \in K$ est un homomorphisme d'anneaux injectif. Dans la suite du problème on identifiera K et $\varphi(K)$ au moyen de φ.

b) Soit D une dérivation de E. Calculer $D(e)$ et $D(\alpha)$ pour $\alpha \in K$.

c) Montrer que si $a \in E$, l'application D_a de E dans E définie par

$$D_a(x) = ax - xa$$

pour tout élément x de E, est une dérivation.

d) Montrer que $\mathscr{D}(E)$ est un sous-espace vectoriel de l'espace vectoriel $\mathscr{L}(E)$.

e) Montrer qu'en général, $\mathscr{D}(E)$ n'est pas une sous-algèbre de l'algèbre $\mathscr{L}(E)$.

f) Montrer que si D_1 et D_2 sont des éléments de $\mathscr{D}(E)$, il en est de même de $[D_1, D_2] = D_1 \circ D_2 - D_2 \circ D_1$.

g) Supposons que E soit une algèbre commutative et soit D une dérivation dans E. Calculer $D(x^n)$ pour $x \in E$, $n \in \mathbf{N}$ et $n \geqslant 2$. Démontrer que si $x \in E$, $y \in E$ et $p \in \mathbf{N}^*$, alors on a

$$D^p(xy) = \sum_{k=0}^{p} C_p^k \, D^k(x) \, D^{p-k}(y) \,. \tag{2}$$

Solution *a*) Si α et β sont dans K, on a

$$\varphi(\alpha + \beta) = (\alpha + \beta)\, e = \alpha e + \beta e = \varphi(\alpha) + \varphi(\beta) \,;$$
$$\varphi(\alpha\beta) = (\alpha\beta)\, e = (\alpha e).(\beta e) = \varphi(\alpha)\, \varphi(\beta) \,;$$

enfin si $\varphi(\alpha) = \varphi(\beta)$ on a $\alpha e = \beta e$ ce qui entraîne $\alpha = \beta$, donc φ est un homomorphisme injectif et il n'y a aucun inconvénient à considérer $K \subset E$.

b) $D(e) = D(ee) = eD(e) + D(e)\, e = D(e) + D(e)$; on a donc $D(e) = 0$. Si $\alpha \in K$, on a $D(\alpha) = D(\alpha e) = \alpha D(e) = \alpha 0 = 0$.

c) Montrons d'abord que D_a est un endomorphisme ; si α et β sont dans K et x et y dans E, on a

$$D_a(\alpha x + \beta y) = a(\alpha x + \beta y) - (\alpha x + \beta y)\, a = \alpha ax + \beta ay - \alpha xa - \beta ya$$
$$= \alpha(ax - xa) + \beta(ay - ya) = \alpha D_a(x) + \beta D_a(y) \,.$$

Vérifions l'égalité (1)

$$D_a(x)\, y + xD_a(y) = (ax - xa)\, y + x(ay - ya) = a(xy) - (xy)\, a = D_a(xy) \,.$$

d) Soient D_1 et D_2 deux éléments de $\mathscr{D}(E)$ et α_1, α_2 deux éléments de K. Nous savons que $\alpha_1 D_1 + \alpha_2 D_2$ est un endomorphisme de E. Vérifions que c'est une dérivation :

$$(\alpha_1 D_1 + \alpha_2 D_2)(xy) = \alpha_1 D_1(xy) + \alpha_2 D_2(xy) = \alpha_1 D_1(x)\, y + \alpha_1 xD_1(y) +$$
$$+ \alpha_2 D_2(x)\, y + \alpha_2 xD_2(y) = (\alpha_1 D_1 + \alpha_2 D_2)(x)\, y + x(\alpha_1 D_1 + \alpha_2 D_2)(y) \,.$$

$\mathscr{D}(E)$ est donc un sous-espace vectoriel de $\mathscr{L}(E)$.

e) Pour que $\mathscr{D}(E)$ soit une sous-algèbre de $\mathscr{L}(E)$, il doit être stable pour la composition des applications. Soient D_1 et D_2 deux éléments de $\mathscr{D}(E)$; calculons $D_1 \circ D_2(xy)$ où x, y sont deux éléments de E :

$$(D_1 \circ D_2)(xy) = D_1\big(D_2(x)\, y + xD_2(y)\big) = D_1\big(D_2(x)\, y\big) + D_1\big(xD_2(y)\big) =$$
$$= (D_1 \circ D_2)(x)\, y + D_2(x)\, D_1(y) + D_1(x)\, D_2(y) + x(D_1 \circ D_2)(y) \,;$$

comme en général $D_2(x)\, D_1(y) + D_1(x)\, D_2(y) \neq 0$, $D_1 \circ D_2$ n'est pas une dérivation dans E.

f) $[D_1, D_2]$ est évidemment un endomorphisme de E. Pour calculer $[D_1, D_2](xy)$ $(x \in E,\ y \in E)$ nous pouvons utiliser le calcul précédent, on obtient :

$$\begin{aligned}[D_1, D_2](xy) &= (D_1 \circ D_2)(xy) - (D_2 \circ D_1)(xy)\\ &= (D_1 \circ D_2)(x)\, y + D_2(x)\, D_1(y) + D_1(x)\, D_2(y) +\\ &\quad + x(D_1 \circ D_2)(y) - (D_1 \circ D_2)(x)\, y - D_1(x)\, D_2(y)\\ &\quad - D_2(x)\, D_1(y) - x(D_2 \circ D_1)(y)\\ &= (D_1 \circ D_2 - D_2 \circ D_1)(x)\, y + x(D_1 \circ D_2 - D_2 \circ D_1)(y) :\end{aligned}$$

donc $[D_1, D_2]$ est bien une dérivation de E.

g) Calculons d'abord $D(x^2) = D(xx) = xD(x) + D(x)\, x = 2\, xD(x)$; supposons qu'on ait $D(x^n) = nx^{n-1}\, D(x)$; calculons $D(x^{n+1})$: on a

$$\begin{aligned}D(x^{n+1}) &= D(xx^n) = D(x)\, x^n + xD(x^n)\\ &= D(x)\, x^n + nx^n\, D(x) = (n + 1)\, x^n\, D(x)\,.\end{aligned}$$

On a donc pour tout entier $n \geqslant 2$:

$$D(x^n) = nx^{n-1}\, D(x)\,.$$

Pour $p = 1$ l'égalité (2) coïncide avec (1) et est vérifiée par définition. Supposons-la vraie pour tous les entiers strictement inférieurs à p. On a alors

$$\begin{aligned}D^p(xy) &= D\big(D^{p-1}(xy)\big) = D\left(\sum_{k=0}^{p-1} C_{p-1}^k\, D^k(x)\, D^{p-k-1}(y)\right)\\ &= \sum_{k=0}^{p-1} C_{p-1}^k\, D\big(D^k(x)\, D^{p-k-1}(y)\big)\\ &= \sum_{k=0}^{p-1} C_{p-1}^k \big[D^{k+1}(x)\, D^{p-k-1}(y) + D^k(x)\, D^{p-k}(y)\big]\\ &= D^0(x)\, D^p(y) + \sum_{k=1}^{p-1} (C_{p-1}^k + C_{p-1}^{k-1})\, D^k(x)\, D^{p-k}(y) + D^p(x)\, D^0(y)\\ &= \sum_{k=0}^{p} C_p^k\, D^k(x)\, D^{p-k}(y)\,, \quad \text{car } C_{p-1}^k + C_{p-1}^{k-1} = C_p^k\end{aligned}$$

(*cf.* Q., Ch. 2, § III, n° 41). La formule proposée est donc vraie.

5.16 1) Considérons les formes linéaires $(f_i)_{1 \leqslant i \leqslant 4}$ sur $\mathbf{R}^4$ définies au moyen de leurs coordonnées dans la base duale de la base canonique de $\mathbf{R}^4$, par :

$$f_1 = (1, 0, -\lambda, 0) \quad f_2 = \left(0, 1, 0, -\frac{1}{\lambda}\right)$$

$$f_3 = (1, 0, 0, -\mu) \quad f_4 = \left(0, 1, 0, -\frac{1}{\mu}\right)$$

où λ et μ sont des nombres réels non nuls.

Etudier l'indépendance linéaire de ces formes et trouver lorsqu'elles sont indépendantes la base de $\mathbf{R}^4$ duale de la base $\{f_1, f_2, f_3, f_4\}$.

2) Mêmes questions pour les formes définies par :

$$g_1 = (1, 0, -\sin\alpha, -\cos\alpha), \quad g_2 = (0, 1, -\cos\alpha, \sin\alpha),$$
$$g_3 = (1, 0, \sin\beta, -\cos\beta), \quad g_4 = (0, 1, -\cos\beta, -\sin\beta),$$

où α et β sont des nombres réels.

Solution 1) En utilisant la méthode Q., Ch. 7, § III, n° 138, on trouve la relation

$$f_4 - f_2 = \left(0, 0, 0, -\frac{1}{\mu} + \frac{1}{\lambda}\right);$$

donc les formes données sont linéairement indépendantes si et seulement si $\lambda \neq \mu$. Supposons $\lambda \neq \mu$; la base duale de $\{f_1, f_2, f_3, f_4\}$ est formée des vecteurs e_1, e_2, e_3, e_4 qui vérifient les conditions

$$f_i(e_j) = \delta_{ij} \quad (1 \leqslant i \leqslant 4,\ 1 \leqslant j \leqslant 4).$$

Soient $x_i^1, x_i^2, x_i^3, x_i^4$ les coordonnées de e_i $(1 \leqslant i \leqslant 4)$ sur la base canonique de $\mathbf{R}^4$. On a alors

$$f_1(e_1) = x_1^1 - \lambda x_1^3 = 1$$
$$f_2(e_1) = x_1^2 - \frac{1}{\lambda} x_1^4 = 0$$
$$f_3(e_1) = x_1^1 - \mu x_1^4 = 0$$
$$f_4(e_1) = x_1^2 - \frac{1}{\mu} x_1^4 = 0.$$

De la deuxième et de la quatrième équation on tire $x_1^2 = x_1^4 = 0$, de la troisième $x_1^1 = 0$ et de la première $x_1^3 = -\frac{1}{\lambda}$, donc $e_1 = \left(0, 0, -\frac{1}{\lambda}, 0\right)$.

Le système correspondant à e_2 est

$$x_2^1 - \lambda x_2^3 = 0$$
$$x_2^2 - \frac{1}{\lambda} x_2^4 = 1$$
$$x_2^1 - \mu x_2^4 = 0$$
$$x_2^2 - \frac{1}{\mu} x_2^4 = 0.$$

De la deuxième et de la quatrième équation on déduit

$$x_2^4 = \frac{\lambda\mu}{\lambda - \mu} \qquad \text{et} \qquad x_2^2 = \frac{\lambda}{\lambda - \mu},$$

de la troisième équation on tire

$$x_2^1 = \frac{\lambda\mu^2}{\lambda - \mu}$$

et de la première

$$x_2^3 = \frac{\mu^2}{\lambda - \mu},$$

donc

$$e_2 = \left(\frac{\lambda\mu^2}{\lambda - \mu}, \frac{\lambda}{\lambda - \mu}, \frac{\mu^2}{\lambda - \mu}, \frac{\lambda\mu}{\lambda - \mu}\right).$$

Le système correspondant à e_3 est

$$\begin{aligned} x_3^1 - \lambda x_3^3 &= 0 \\ x_3^2 - \frac{1}{\lambda} x_3^4 &= 0 \\ x_3^1 - \mu x_3^4 &= 1 \\ x_3^2 - \frac{1}{\mu} x_3^4 &= 0 . \end{aligned}$$

En appliquant la même méthode que ci-dessus, on trouve

$$x_3^2 = x_3^4 = 0, \quad x_3^1 = 1, \quad x_3^3 = \frac{1}{\lambda}$$

donc,

$$e_3 = \left(1, 0, \frac{1}{\lambda}, 0\right).$$

Le système correspondant à e_4 est

$$\begin{aligned} x_4^1 - \lambda x_4^3 &= 0 \\ x_4^2 - \frac{1}{\lambda} x_4^4 &= 0 \\ x_4^1 - \mu x_4^4 &= 0 \\ x_4^2 - \frac{1}{\mu} x_4^4 &= 1 . \end{aligned}$$

On trouve

$$x_4^4 = \frac{\mu\lambda}{\mu - \lambda}, \quad x_4^2 = \frac{\mu}{\mu - \lambda}, \quad x_4^1 = \frac{\lambda\mu^2}{\mu - \lambda}, \quad x_4^3 = \frac{\mu^2}{\mu - \lambda}$$

d'où

$$e_4 = \left(\frac{\lambda\mu^2}{\mu-\lambda}, \frac{\mu}{\mu-\lambda}, \frac{\mu^2}{\mu-\lambda}, \frac{\mu\lambda}{\mu-\lambda}\right).$$

2) Appliquons la méthode de Q., Ch. 7, § III, n° 138, on obtient les systèmes suivants :

g_1	g_2	g_3	g_4
1	0	1	0
0	1	0	1
$-\sin\alpha$	$-\cos\alpha$	$\sin\beta$	$-\cos\beta$
$-\cos\alpha$	$\sin\alpha$	$-\cos\beta$	$-\sin\beta$

g_1	g_2	$g'_3 = g_3 - g_1$	$g'_4 = g_4 - g_2$
1	0	0	0
0	1	0	0
$-\sin\alpha$	$-\cos\alpha$	$\sin\alpha + \sin\beta$	$\cos\alpha - \cos\beta$
$-\cos\alpha$	$\sin\alpha$	$\cos\alpha - \cos\beta$	$-(\sin\alpha + \sin\beta)$.

On voit donc que la condition $\sin\alpha + \sin\beta \neq 0$ est nécessaire à l'indépendance linéaire des formes g_i $(1 \leqslant i \leqslant 4)$. Supposons cette condition satisfaite, alors le dernier système ci-dessus est de même rang que le système

g_1	g_2	g'_3	$g''_4 = g'_4 - \dfrac{\cos\alpha - \cos\beta}{\sin\alpha + \sin\beta} \cdot g'_3$
1	0	0	0
0	1	0	0
$-\sin\alpha$	$-\cos\alpha$	$\sin\alpha + \sin\beta$	0
$-\cos\alpha$	$\sin\alpha$	$\cos\alpha - \cos\beta$	$-(\sin\alpha + \sin\beta) - \dfrac{(\cos\alpha - \cos\beta)^2}{\sin\alpha + \sin\beta}$.

Il résulte de tout ceci que les formes g_i $(1 \leqslant i \leqslant 4)$, sont linéairement indépendantes si et seulement si

$$\sin\alpha + \sin\beta \neq 0 \quad \text{et} \quad (\cos\alpha - \cos\beta)^2 + (\sin\alpha + \sin\beta)^2 \neq 0$$

donc si et seulement si $\sin\alpha + \sin\beta \neq 0$ et $\cos\alpha - \cos\beta \neq 0$ ce qui équivaut aux conditions $\alpha \neq \pi + \beta \pmod{2\pi}$ et $\alpha \neq -\beta \pmod{2\pi}$.

Supposons ces conditions satisfaites. Si on appelle $\{a_1, a_2, a_3, a_4\}$ la base duale de $\{g_1, g_2, g_3, g_4\}$ et y_i^j $(1 \leqslant j \leqslant 4)$ les coordonnées de a_i sur la base canonique de $\mathbf{R}^4$, et si on applique la même méthode que pour (1), on trouve

$$g_1(a_1) = y_1^1 - \sin\alpha . y_1^3 - \cos\alpha . y_1^4 = 1$$

$$g_2(a_1) = y_1^2 - \cos\alpha . y_1^3 + \sin\alpha . y_1^4 = 0$$

$$g_3(a_1) = y_1^1 + \sin\beta . y_2^3 - \cos\beta . y_1^4 = 0$$

$$g_4(a_1) = y_1^2 - \cos\beta . y_1^3 - \sin\beta . y_1^4 = 0 .$$

En faisant la différence de la première et de la troisième équation, et de la deuxième et de la quatrième, on trouve

$$-(\sin\alpha + \sin\beta)\, y_1^3 + (\cos\beta - \cos\alpha)\, y_1^4 = 1$$

$$(\cos\beta - \cos\alpha)\, y_1^3 + (\sin\alpha + \sin\beta)\, y_1^4 = 0$$

qui donne

$$y_1^3 = \frac{\sin\alpha + \sin\beta}{2[\cos(\alpha+\beta) - 1]} = -\frac{\cos\dfrac{\alpha-\beta}{2}}{2\sin\dfrac{\alpha+\beta}{2}}$$

et

$$y_1^4 = \frac{\cos\beta - \cos\alpha}{2[\cos(\alpha+\beta) - 1]} = \frac{\sin\dfrac{\alpha-\beta}{2}}{2\sin\dfrac{\alpha+\beta}{2}}.$$

On obtient ensuite

$$y_1^1 = -\sin\beta . y_1^3 + \cos\beta . y_1^4 = \frac{1}{2}$$

et

$$y_1^2 = \cos\alpha . y_1^3 - \sin\alpha . y_1^4 = -\frac{1}{2}\operatorname{cotg}\frac{\alpha+\beta}{2}.$$

En résolvant les trois autres systèmes de la même manière on trouve

$$a_1 = \left(\frac{1}{2}, -\frac{1}{2}\operatorname{cotg}\frac{\alpha+\beta}{2}, \frac{-\cos\dfrac{\alpha-\beta}{2}}{2\sin\dfrac{\alpha+\beta}{2}}, \frac{\sin\dfrac{\alpha-\beta}{2}}{2\sin\dfrac{\alpha+\beta}{2}}\right)$$

$$a_2 = \left(\frac{1}{2}\operatorname{cotg}\frac{\alpha+\beta}{2}, \frac{1}{2}, \frac{\sin\dfrac{\alpha-\beta}{2}}{2\sin\dfrac{\alpha+\beta}{2}}, \frac{\cos\dfrac{\alpha-\beta}{2}}{2\sin\dfrac{\alpha+\beta}{2}}\right)$$

$$a_3 = \left(\frac{1}{2}, \frac{1}{2}\operatorname{cotg}\frac{\alpha+\beta}{2}, \frac{\cos\dfrac{\alpha-\beta}{2}}{2\sin\dfrac{\alpha+\beta}{2}}, \frac{-\sin\dfrac{\alpha-\beta}{2}}{2\sin\dfrac{\alpha+\beta}{2}}\right)$$

$$a_4 = \left(-\frac{1}{2}\operatorname{cotg}\frac{\alpha+\beta}{2}, \frac{1}{2}, \frac{-\sin\dfrac{\alpha-\beta}{2}}{2\sin\dfrac{\alpha+\beta}{2}}, \frac{-\cos\dfrac{\alpha-\beta}{2}}{2\sin\dfrac{\alpha+\beta}{2}}\right).$$

5.17 Soient F et G deux sous-espaces vectoriels d'un espace vectoriel E de dimension finie sur un corps commutatif K. Démontrer que

$$(F + G)^{\perp} = F^{\perp} \cap G^{\perp} \tag{1}$$

$$(F \cap G)^{\perp} = F^{\perp} + G^{\perp}. \tag{2}$$

En déduire que si $E = F \oplus G$, on a $E^* = F^{\perp} \oplus G^{\perp}$.

Solution 1) $(F + G)^{\perp}$ est l'ensemble des formes linéaires sur E qui s'annulent sur $F + G$; comme $F \subset F + G$ et $G \subset F + G$, une forme linéaire qui s'annule sur $F + G$ s'annule sur F et sur G donc appartient à $F^{\perp} \cap G^{\perp}$ et on a

$$(F + G)^{\perp} \subset F^{\perp} \cap G^{\perp}.$$

Soit maintenant f un élément de $F^{\perp} \cap G^{\perp}$. Tout élément y de $F + G$ s'écrit $y = x_1 + x_2$ avec $x_1 \in F$ et $x_2 \in G$ et on a $f(x) = f(x_1) + f(x_2) = 0$, donc $f \in (F + G)^{\perp}$ et $F^{\perp} \cap G^{\perp} \subset (F + G)^{\perp}$ par suite $F^{\perp} \cap G^{\perp} = (F + G)^{\perp}$.

2) Nous savons (*cf.* Q., Ch. 7, § VI, n° 151) que pour tout sous-espace vectoriel H d'un espace vectoriel E de dimension finie, on a $(H^{\perp})^{\perp} = H$. Alors $(F \cap G)^{\perp} = [(F^{\perp})^{\perp} \cap (G^{\perp})^{\perp}]^{\perp}$. En appliquant (1) aux sous-espaces $F^{\perp}$ et $G^{\perp}$ de E^*, on obtient $(F^{\perp})^{\perp} \cap (G^{\perp})^{\perp} = (F^{\perp} + G^{\perp})^{\perp}$ d'où

$$(F \cap G)^{\perp} = [(F^{\perp} + G^{\perp})^{\perp}]^{\perp} = F^{\perp} + G^{\perp}.$$

Si $E = F \oplus G$, on a

$$F^{\perp} + G^{\perp} = (F \cap G)^{\perp} = \{0_E\}^{\perp} = E^*$$

et

$$F^{\perp} \cap G^{\perp} = (F + G)^{\perp} = E^{\perp} = \{0_{E^*}\} ;$$

donc on a bien $F^* = F^{\perp} \oplus G^{\perp}$.

5.18 E et F étant deux espaces vectoriels de dimension finie sur le même corps commutatif K, V étant un sous-espace vectoriel de E, on désigne par $\mathscr{L}_V(E ; F)$ l'ensemble des applications linéaires de E dans F qui s'annulent sur V. On désigne par W un supplémentaire de V dans E.

a) Démontrer que $\mathscr{L}_V(E ; F)$ est un sous-espace vectoriel de $\mathscr{L}(E ; F)$ isomorphe à $\mathscr{L}(W ; F)$ et à $\mathscr{L}(E/V ; F)$.

b) Démontrer que $V^{\perp}$ est isomorphe à W^*.

c) Démontrer que si f est une application linéaire de E dans F, ${}^t f(F^*)$ est isomorphe à $[f(E)]^*$.

Solution *a*) Si g_1 et g_2 sont deux éléments de $\mathscr{L}_V(E\,;\,F)$ et λ_1 et λ_2 deux éléments de K, on a $(\lambda_1 g_1 + \lambda_2 g_2)(V) = \lambda_1 g_1(V) + \lambda_2 g_2(V) = 0$, ce qui prouve que $\lambda_1 g_1 + \lambda_2 g_2$ appartient à $\mathscr{L}_V(E\,;\,F)$ qui est donc un sous-espace vectoriel de $\mathscr{L}(E\,;\,F)$. Définissons une fonction φ de $\mathscr{L}_V(E\,;\,F)$ dans $\mathscr{L}(W\,;\,F)$ de la manière suivante : si g est un élément de $\mathscr{L}_V(E\,;\,F)$, $\varphi(g) = g_{|W}$ (restriction de g à W) ; $\varphi(g)$ est bien un élément de $\mathscr{L}(W\,;\,F)$; si g_1, g_2 sont des éléments de $\mathscr{L}_V(E, F)$ et λ_1, λ_2 des éléments de K on a

$$\varphi(\lambda_1 g_1 + \lambda_2 g_2) = (\lambda_1 g_1 + \lambda_2 g_2)_{|W} = \lambda_1 g_{1|W} + \lambda_2 g_{2|W}$$
$$= \lambda_1 \varphi(g_1) + \lambda_2 \varphi(g_2)\,,$$

donc φ est une application linéaire. Si $\varphi(g) = g_{|W} = 0$, g est nulle sur deux sous-espaces supplémentaires donc $g = 0$ ce qui prouve que φ est injective. Soit h un élément de $\mathscr{L}(W\,;\,F)$. L'application linéaire h' définie par $h'_{|V} = 0$ et $h'_{|W} = h$ est un élément de $\mathscr{L}_V(E\,;\,F)$ tel que $\varphi(h') = h$, donc φ est surjective par suite φ est un isomorphisme de $\mathscr{L}_V(E\,;\,F)$ sur $\mathscr{L}(W\,;\,F)$; d'autre part on sait (*cf.* Q., Ch. 7, § III, n° 131) que E/V est isomorphe à W donc $\mathscr{L}(W\,;\,F)$ est isomorphe à $\mathscr{L}(E/V\,;\,F)$.

b) $V^\perp = \mathscr{L}_V(E\,;\,K)$; $W^* = \mathscr{L}(W\,;\,K)$. En appliquant (*a*) on voit que $V^\perp$ est isomorphe à W^*.

c) Soit A un supplémentaire de $\operatorname{Ker} f$ dans E. D'après (*b*), $(\operatorname{Ker} f)^\perp$ est isomorphe à A^*. On sait (*cf.* Q., Ch. 7, § IV, n° 141) que A et $f(E)$ sont isomorphes, donc $[f(E)]^*$ est isomorphe à A^*. On sait aussi (*cf.* Q., Ch. 7, § VI, n° 153) que $(\operatorname{Ker} f)^\perp = {}^t f(F^*)$; donc $[f(E)]^*$ est isomorphe à ${}^t f(F^*)$.

5.19 Soient K un corps commutatif ; A_1, A_2 et B des espaces vectoriels sur K. On note $\mathscr{L}(A_i\,;\,B)$ l'espace vectoriel sur K des applications linéaires de A_i $(i = 1, 2)$ dans B et $\mathscr{B}(A_1 \times A_2\,;\,B)$ l'espace vectoriel sur K des applications bilinéaires de $A_1 \times A_2$ dans B.

1) Soit f un élément de $\mathscr{B}(A_1 \times A_2\,;\,B)$.

a) Si x est un élément de A_1 on note f_x l'application qui à tout élément y de A_2 associe $f_x(y) = f(x, y)$. Montrer que f_x est un élément de $\mathscr{L}(A_2\,;\,B)$.

b) On appelle $\bar{f}$ l'application qui à chaque élément x de E_1 associe $\bar{f}(x) = f_x$. Montrer que $\bar{f}$ est un élément de $\mathscr{L}\big(A_1\,;\,\mathscr{L}(A_2\,;\,B)\big)$.

2) Soit φ l'application qui à tout élément f de $\mathscr{B}(A_1 \times A_2\,;\,B)$ associe $\varphi(f) = \bar{f}$. Montrer que φ est un isomorphisme de $\mathscr{B}(A_1 \times A_2\,;\,B)$ sur $\mathscr{L}\big(A_1\,;\,\mathscr{L}(A_2\,;\,B)\big)$.

Solution 1) *a*) f_x est bien une application de A_2 dans B. Soient y, y' des éléments de A_2 et λ, λ' des éléments de K ; comme f est bilinéaire, on a
$f_x(\lambda y + \lambda' y') = f(x, \lambda y + \lambda' y') = \lambda f(x, y) + \lambda' f(x, y') = \lambda f_x(y) + \lambda' f_x(y')$
ce qui prouve que f_x est une application linéaire donc $f_x \in \mathscr{L}(A_2\,;\,B)$.

b) Comme $f_x \in \mathscr{L}(A_2 ; B)$, $\bar{f}$ est bien une application de A_1 dans $\mathscr{L}(A_2 ; B)$. Soient x et x' des éléments de A_1 et λ, λ' des éléments de K ; alors on a

$$\bar{f}(\lambda x + \lambda' x') = f_{\lambda x + \lambda' x'} \qquad \text{et} \qquad \lambda \bar{f}(x) + \lambda' \bar{f}(x') = \lambda f_x + \lambda' f_{x'} .$$

Pour prouver l'égalité de ces deux fonctions il suffit de démontrer que leurs valeurs coïncident pour tout élément y de A_2 ; or

$$f_{\lambda x + \lambda' x'}(y) = f(\lambda x + \lambda' x', y) = \lambda f(x, y) + \lambda' f(x', y)$$

$$= \lambda f_x(y) + \lambda' f_{x'}(y) = (\lambda f_x + \lambda' f_{x'})(y) .$$

Pour écrire ces égalités on a utilisé la bilinéarité de f et la définition des lois dans l'espace vectoriel $\mathscr{L}(A_2 ; B)$. Donc $\bar{f}$ est bien linéaire.

2) Soient f, f' deux éléments de $\mathscr{B}(A_1 \times A_2 ; B)$ et λ, λ' deux éléments de K. On a

$$\varphi(\lambda f + \lambda' f') = \overline{\lambda f + \lambda' f'} \qquad \text{et} \qquad \lambda \varphi(f) + \lambda' \varphi(f') = \lambda \bar{f} + \lambda' \bar{f}' .$$

Pour comparer ces fonctions calculons leurs valeurs pour un élément x de A_1 :

$$\overline{(\lambda f + \lambda' f')}(x) = (\lambda f + \lambda' f')_x = (\lambda \bar{f} + \lambda' \bar{f}')(x)$$

$$= \lambda \bar{f}(x) + \lambda' \bar{f}'(x) = \lambda f_x + \lambda' f'_x .$$

Or, pour tout élément y de A_2 on a

$$(\lambda f + \lambda' f')_x(y) = (\lambda f + \lambda' f')(x, y) = \lambda f(x, y) + \lambda' f'(x, y) =$$

$$= \lambda f_x(y) + \lambda' f'_x(y) = (\lambda f_x + \lambda' f'_x)(y);$$

par suite pour tout élément x de A_1 on a : $\overline{(\lambda f + \lambda' f')}(x) = (\lambda \bar{f} + \lambda' \bar{f}')(x)$ c'est-à-dire $\varphi(\lambda f + \lambda' f') = \lambda \varphi(f) + \lambda' \varphi(f')$ ce qui prouve que φ est linéaire.

Montrons que φ est injective ; soient f et g deux éléments de $\mathscr{B}(A_1 \times A_2 ; B)$ tels que $\varphi(f) = \varphi(g) = \bar{f} = \bar{g}$. Alors pour tout élément x de A_1 on a

$$\bar{f}(x) = \bar{g}(x) = f_x = g_x$$

et pour tout élément y de A_2, $f_x(y) = g_x(y) = f(x, y) = g(x, y)$; par suite pour tout élément (x, y) de $A_1 \times A_2$ on a $f(x, y) = g(x, y)$ ce qui prouve bien que $f = g$.

Pour montrer que φ est surjective choisissons un élément u de

$$\mathscr{L}(A_1 ; \mathscr{L}(A_2 ; B)) .$$

Soit h l'application de $A_1 \times A_2$ dans B définie par

$$h(x, y) = u(x)(y) \quad ((x, y) \in A_1 \times A_2) .$$

Montrons d'abord que h est bilinéaire. Soient x, x' des éléments de A_1, y, y' des éléments de A_2 et λ, λ' des éléments de K. Alors on a

$$h(\lambda x + \lambda' x', y) = u(\lambda x + \lambda' x')(y) = (\lambda u(x) + \lambda' u(x'))(y)$$
$$= \lambda u(x)(y) + \lambda' u(x')(y) = \lambda h(x, y) + \lambda' h(x', y)$$

et

$$h(x, \lambda y + \lambda' y') = u(x)(\lambda y + \lambda' y') = \lambda u(x)(y) + \lambda' u(x)(y')$$
$$= \lambda h(x, y) + \lambda' h(x, y').$$

Calculons maintenant $\varphi(h) = \bar{h}$. On a pour tout x de A_1 et tout y de A_2, $h(x) = h_x$ et $h_x(y) = h(x, y) = u(x)(y)$; donc $h_x = u(x)$ et $\bar{h} = u$ ce qui prouve bien que φ est surjective, donc φ est un isomorphisme.

5.20 Soient V un espace vectoriel sur **C** et E un espace vectoriel sur **R** ou **C**. Une application f de E dans V est dite **R**-linéaire si, pour tout élément x de E, tout élément y de E et tout nombre réel λ, on a

$$f(x + y) = f(x) + f(y) \quad \text{et} \quad f(\lambda x) = \lambda . f(x).$$

Si E est un espace vectoriel sur **C**, f est dite **C**-linéaire si pour tout élément x de E, tout élément y de E et tout nombre complexe α, on a

$$f(x + y) = f(x) + f(y) \quad \text{et} \quad f(\alpha x) = \alpha . f(x).$$

a) Soient A et B deux espaces vectoriels sur **C** et f une application **R**-linéaire de A dans B. Démontrer que f est **C**-linéaire si et seulement si $f(ix) = if(x)$ pour tout élément x de A.

b) Dans la suite du problème E désigne un espace vectoriel sur **R**. On considère $E \times E$ muni de l'addition interne

$$(x, y) + (x', y') = (x + x', y + y') \quad ((x, y) \in E \times E,\ (x', y') \in E \times E)$$

et de la loi externe

$$\alpha . (x, y) = (ax - by, bx + ay) \quad ((x, y) \in E \times E,\ \alpha \in \mathbf{C} \text{ et } \alpha = a + b\,\mathrm{i}).$$

Montrer que $E \times E$ muni de ces deux lois est un espace vectoriel sur **C** qui sera noté $E_{\mathbf{C}}$.

c) Soit J l'application de E dans $E_{\mathbf{C}}$ définie par $J(x) = (x, 0)$ pour tout élément x de E. Montrer que J est **R**-linéaire et injective, et que pour tout élément (x, y) de $E_{\mathbf{C}}$, $(x, y) = J(x) + \mathrm{i}J(y)$.

d) Montrer que $E_{\mathbf{C}}$ et J possèdent la propriété suivante :

(*P*) Pour tout espace vectoriel V sur **C** et toute application **R**-linéaire f, de E dans V, il existe une application **C**-linéaire $\bar{f}$ de $E_{\mathbf{C}}$ dans V, et une seule, telle que $f = \bar{f} \circ J$.

e) Montrer que si E' est un espace vectoriel sur **C** et φ une application **R**-linéaire de E dans E' qui possèdent la propriété (P), alors E' est isomorphe à $E_{\mathbf{C}}$.

f) Soient E et F deux espaces vectoriels sur **R**. On construit comme ci-dessus $E_{\mathbf{C}}$ et J, et $F_{\mathbf{C}}$ et J_1 respectivement. Soit f une application **R**-linéaire de E dans F. Montrer qu'il existe une application **C**-linéaire $f_{\mathbf{C}}$ de $E_{\mathbf{C}}$ dans $F_{\mathbf{C}}$ et une seule, telle que $f_{\mathbf{C}} \circ J = J_1 \circ f$.

g) Si G est un espace vectoriel sur **R**, J_2 et $G_{\mathbf{C}}$ construits comme ci-dessus, g une application **R**-linéaire de F dans G, et $g_{\mathbf{C}}$ l'application **C** — linéaire dans $G_{\mathbf{C}}$ correspondante ; montrer que $(g \circ f)_{\mathbf{C}} = g_{\mathbf{C}} \circ f_{\mathbf{C}}$.

h) Montrer que $(\mathrm{Id}\, E)_{\mathbf{C}} = \mathrm{Id}\,(E_{\mathbf{C}})$ et que si f est un isomorphisme, alors $f_{\mathbf{C}}$ est un isomorphisme.

Solution *a*) Si f est **C**-linéaire, on a par définition pour tout élément x de E,

$$f(\mathrm{i}x) = \mathrm{i}f(x)\,.$$

Réciproquement si cette dernière condition est satisfaite et si λ est un nombre complexe, alors $\lambda = a + \mathrm{i}b$ avec a et b réels et la **R**-linéarité de f et l'hypothèse permettent d'écrire pour tout élément x de E :

$$\begin{aligned} f(\lambda x) &= f((a + \mathrm{i}b)\,x) = f(ax + \mathrm{i}bx) = f(ax) + f(\mathrm{i}bx) \\ &= af(x) + \mathrm{i}bf(x) = (a + \mathrm{i}b) f(x) = \lambda f(x)\,, \end{aligned}$$

donc f est **C**-linéaire.

b) Nous savons (*cf.* Q., Ch. 4, § IV, n° 79) que $E \times E$ muni de cette addition est un groupe abélien. Vérifions les autres axiomes. Si x, x', y, y' sont des éléments de E, et λ, μ des nombres complexes qui s'écrivent $\lambda = a + \mathrm{i}b$, $\mu = c + \mathrm{i}d$ avec a, b, c, d, réels, alors on a tout d'abord

$$\begin{aligned} (\lambda\mu)\,(x, y) &= [(a + \mathrm{i}b)\,(c + \mathrm{i}d)]\,(x, y) = [(ac - bd) + \mathrm{i}(ad + bc)]\,(x, y) \\ &= [(ac - bd)\,x - (ad + bc)\,y,\ (ad + bc)\,x + (ac - bd)\,y] \\ &= [a(cx - dy) - b(dx + cy),\ b(cx - dy) + a(dx + cy)] \\ &= (a + \mathrm{i}b)\,(cx - dy,\ dx + cy) = (a + \mathrm{i}b)\,[(c + \mathrm{i}d)\,(x, y)] \\ &= \lambda(\mu(x, y))\,. \end{aligned}$$

On a aussi

$$\begin{aligned} \lambda[(x, y) + (x', y')] &= (a + \mathrm{i}b)\,[x + x', y + y'] \\ &= [a(x + x') - b(y + y'),\ b(x + x') + a(y + y')] \\ &= (ax - by + ax' - by',\ bx + ay + bx' + ay') \\ &= (ax - by,\ bx + ay) + (ax' - by',\ bx' + ay') \\ &= (a + \mathrm{i}b)\,(x, y) + (a + \mathrm{i}b)\,(x', y') = \lambda(x, y) + \lambda(x', y')\,. \end{aligned}$$

On a encore

$$\begin{aligned}(\lambda + \mu)(x, y) &= [(a + c) + i(b + d)](x, y)\\ &= ((a + c)x - (b + d)y, (b + d)x + (a + c)y)\\ &= (ax - by + cx - dy, bx + ay + dx + cy)\\ &= (ax - by, bx + ay) + (cx - dy, dx + cy)\\ &= (a + ib)(x, y) + (c + id)(x, y) = \lambda(x, y) + \mu(x, y)\end{aligned}$$

On a enfin

$$1(x, y) = (1 + i\,0)(x, y) = (1.x - 0.y, 0.x + 1.y) = (x, y)\,.$$

Donc $E \times E$ est bien un espace vectoriel sur $\mathbf{C}$.

c) Soient x, y deux éléments de E et a un nombre réel. On a

$$J(x + y) = (x + y, 0) = (x, 0) + (y, 0) = J(x) + J(y)$$

et

$$J(ax) = (ax, 0) = a(x, 0) = a.J(x)\,.$$

Donc J est $\mathbf{R}$-linéaire et il est clair qu'elle est injective ; de plus on a

$$\begin{aligned}J(x) + iJ(y) &= (x, 0) + (0 + 1.i)(y, 0) = (x, 0) + (0.y - 1.0, 0 + 1.y)\\ &= (x, 0) + (0, y) = (x, y)\,.\end{aligned}$$

La formule proposée est donc vraie.

d) Soient V un espace vectoriel sur $\mathbf{C}$ et f une application $\mathbf{R}$-linéaire de E dans V. Supposons qu'il existe une application $\mathbf{C}$-linéaire $\bar{f}$ de $E_{\mathbf{C}}$ dans V telle que $\bar{f} \circ J = f$. On a alors pour tout élément (x, y) de $E_{\mathbf{C}}$,

$$\begin{aligned}\bar{f}(x, y) &= \bar{f}(J(x) + iJ(y)) = \bar{f}(J(x)) + \bar{f}(iJ(y))\\ &= (\bar{f} \circ J)(x) + i(\bar{f} \circ J)(y) = f(x) + if(y)\,.\end{aligned}$$

Donc si $\bar{f}$ existe, elle est définie par $\bar{f}(x, y) = f(x) + if(y)$ pour tout élément (x, y) de $E_{\mathbf{C}}$, ce qui prouve son unicité. Montrons que cette fonction est bien celle que l'on cherche. On a tout d'abord pour tout élément x de E,

$$(\bar{f} \circ J)(x) = \bar{f}(x, 0) = f(x) + if(0) = f(x) \qquad \text{donc} \qquad \bar{f} \circ J = f\,.$$

Soient maintenant (x, y), (x', y') deux éléments de $E_{\mathbf{C}}$ et a un nombre réel, alors on a

$$\begin{aligned}\bar{f}((x, y) + (x', y')) &= \bar{f}(x + x', y + y') = f(x + x') + if(y + y') =\\ &= f(x) + f(x') + if(y) + if(y') = (f(x) + if(y)) + (f(x') + if(y'))\\ &= \bar{f}(x, y) + \bar{f}(x', y')\end{aligned}$$

$$\begin{aligned}\text{et}\quad \bar{f}(a(x, y)) &= \bar{f}(ax, ay) = f(ax) + if(ay)\\ &= af(x) + iaf(y) = a(f(x) + if(y)) = a\bar{f}(x, y)\,.\end{aligned}$$

Donc la **R**-linéarité de $\bar{f}$ résulte de la **R**-linéarité de f. D'après (a) pour que $\bar{f}$ soit **C**-linéaire il faut et suffit que pour tout élément (x, y) de $E_{\mathbf{C}}$ on ait

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

or on a précisément

$$\begin{aligned}\bar{f}(\mathrm{i}(x, y)) &= \bar{f}((0 + 1\,\mathrm{i})(x, y)) = \bar{f}(-y, x) \\ &= f(-y) + \mathrm{i}f(x) = \mathrm{i}(\mathrm{i}f(y) + f(x)) = \mathrm{i}\bar{f}(x, y)\,.\end{aligned}$$

Donc $\bar{f}$ est la seule application **C**-linéaire de $E_{\mathbf{C}}$ dans V telle que $f = \bar{f} \circ J$.

e) Comme $(E_{\mathbf{C}}, J)$ satisfait à (P) il existe une application **C**-linéaire $\bar{J}'$ de $E_{\mathbf{C}}$ dans E' et une seule, telle que $J' = \bar{J}' \circ J$. Comme (E', J') satisfait à (P), il existe une application **C**-linéaire $\bar{J}$ de E' dans $E_{\mathbf{C}}$ et une seule, telle que $J = \bar{J} \circ J'$. Mais alors $J = (\bar{J} \circ \bar{J}') \circ J$; d'autre part on a aussi $J = \mathrm{Id}\,E_{\mathbf{C}} \circ J$, et la propriété (P) appliquée à $(E_{\mathbf{C}}, J)$ nous assure l'unicité d'une application **C**-linéaire h de $E_{\mathbf{C}}$ dans $E_{\mathbf{C}}$ telle que $J = h \circ J$ donc $h = \mathrm{Id}\,E_{\mathbf{C}} = \bar{J} \circ \bar{J}'$. Un raisonnement semblable appliqué aux égalités $J' = (\bar{J}' \circ \bar{J}) \circ J' = \mathrm{Id}\,E' \circ J'$ montre que $\bar{J}' \circ \bar{J} = \mathrm{Id}\,E'$. Donc $\bar{J}$ est un isomorphisme de E' sur $E_{\mathbf{C}}$.

f) $J_1 \circ f$ est une application **R**-linéaire de E dans $F_{\mathbf{C}}$. La propriété (P) assure l'existence et l'unicité d'une application **C**-linéaire $f_{\mathbf{C}}$ de $E_{\mathbf{C}}$ dans $F_{\mathbf{C}}$ telle que $J_1 \circ f = f_{\mathbf{C}} \circ J$.

g) On a $J_2 \circ g = g_{\mathbf{C}} \circ J_1$ et $J_1 \circ f = f_{\mathbf{C}} \circ J$. Donc

$$J_2 \circ (g \circ f) = g_{\mathbf{C}} \circ J_1 \circ f = (g_{\mathbf{C}} \circ f_{\mathbf{C}}) \circ J\,.$$

En raison de l'unicité de l'application $(g \circ f)_{\mathbf{C}}$ on a $(g \circ f)_{\mathbf{C}} = g_{\mathbf{C}} \circ f_{\mathbf{C}}$.

h) On a évidemment $J \circ \mathrm{Id}\,E = \mathrm{Id}\,(E_{\mathbf{C}}) \circ J$ donc $\mathrm{Id}\,(E_{\mathbf{C}}) = (\mathrm{Id}\,E)_{\mathbf{C}}$. Soit h l'application réciproque de f. On a $h \circ f = \mathrm{Id}\,E$ et $f \circ h = \mathrm{Id}\,F$ donc

$$h_{\mathbf{C}} \circ f_{\mathbf{C}} = (h \circ f)_{\mathbf{C}} = (\mathrm{Id}\,E)_{\mathbf{C}} = \mathrm{Id}\,(E_{\mathbf{C}})$$

et

$$f_{\mathbf{C}} \circ h_{\mathbf{C}} = (f \circ h)_{\mathbf{C}} = (\mathrm{Id}\,F)_{\mathbf{C}} = \mathrm{Id}\,(F_{\mathbf{C}})\,.$$

Donc $f_{\mathbf{C}}$ est un isomorphisme de $E_{\mathbf{C}}$ sur $F_{\mathbf{C}}$.

6

MATRICES

6.1 On considère pour chaque nombre réel x, la matrice

$$A(x) = \begin{pmatrix} \operatorname{ch} x & \operatorname{sh} x \\ \operatorname{sh} x & \operatorname{ch} x \end{pmatrix}.$$

1) x, y étant deux nombres réels calculer $A(x).A(y)$.

2) Si x est un nombre réel, calculer $(A(x))^n$ pour tout entier rationnel n.

Solution 1)

$$A(x).A(y) = \begin{pmatrix} \operatorname{ch} x \operatorname{ch} y + \operatorname{sh} x \operatorname{sh} y & \operatorname{sh} x \operatorname{ch} y + \operatorname{sh} y \operatorname{ch} x \\ \operatorname{sh} x \operatorname{ch} y + \operatorname{sh} y \operatorname{ch} x & \operatorname{ch} x \operatorname{ch} y + \operatorname{sh} x \operatorname{sh} y \end{pmatrix}$$

or on a

$$\operatorname{ch} x \operatorname{ch} y + \operatorname{sh} y \operatorname{sh} x = \operatorname{ch} (x + y)$$

et

$$\operatorname{sh} x \operatorname{ch} y + \operatorname{sh} y \operatorname{ch} x = \operatorname{sh} (x + y)$$

donc

$$A(x).A(y) = \begin{pmatrix} \operatorname{ch} (x + y) & \operatorname{sh} (x + y) \\ \operatorname{sh} (x + y) & \operatorname{ch} (x + y) \end{pmatrix} = A(x + y).$$

2) On a $(A(x))^2 = A(x + x) = A(2x)$. Soit n un entier strictement plus grand que 2 ; supposons que $(A(x))^{n-1} = A((n - 1)x)$, alors

$$(A(x))^n = (A(x))^{n-1}.A(x) = A((n - 1)x + x) = A(nx)$$

par suite pour tout entier $n \geqslant 1$ on a $(A(x))^n = A(nx)$. Observons maintenant que

$$A(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

donc pour tout nombre réel x on a $(A(x))^0 = I_2 = A(0)$. De plus, si x est un nombre réel on a

$$A(x).A(-x) = A(0) = I_2 = A(-x).A(x)$$

donc $A(-x) = (A(x))^{-1}$. Il en résulte que pour tout entier $p < 0$ et tout nombre réel x on a $(A(x))^p = [(A(-x))^{-1}]^p = (A(-x))^{-p} = A(p.x)$, par suite pour tout entier rationnel n et tout nombre réel x on a $(A(x))^n = A(nx)$.

6.2

On considère les matrices

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \qquad I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad B = A - I .$$

1) Calculer B^n pour $n \in \mathbf{N}$.

2) Calculer A^n pour $n \in \mathbf{N}$.

Solution

1) On a $B^0 = I$ et

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

donc

$$B^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

et

$$B^3 = B^2.B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Donc pour tout entier $n \geqslant 3$, on a $B^n = 0$.

2) Comme B et I commutent, on peut employer la formule du binôme et on a

$$A^n = (B + I)^n = I^n + C_n^1 I^{n-1} B + C_n^2 I^{n-2} B^2 = I + nB + \frac{n(n-1)}{2} B^2.$$

On a donc

$$A^n = \begin{pmatrix} 1 & n & \dfrac{n(n-1)}{2} \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}.$$

6.3 Soit $\mathcal{M}_2(\mathbf{R})$ l'ensemble des matrices carrées d'ordre 2 à coefficients réels. Trouver toutes les matrices A de $\mathcal{M}_2(\mathbf{R})$ qui vérifient $A^2 = A$.

Solution Posons

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

où a, b, c, d sont des nombres réels. On a

$$A^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix}$$

d'où le système d'équations :

$$\begin{cases} a^2 + bc = a & (1) \\ b(a + d) = b & (2) \\ c(a + d) = c & (3) \\ bc + d^2 = d\,. & (4) \end{cases}$$

Supposons $b = 0$. De (1) on déduit $a^2 - a = 0$ donc $a = 1$ ou $a = 0$. De (4) on déduit $d^2 - d = 0$ donc $d = 1$ ou $d = 0$. Si $a + d \neq 1$ on a $c = 0$; si $a + d = 1$, c peut prendre n'importe quelle valeur. On trouve donc les matrices :

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix} \quad (c \in \mathbf{R})\,.$$

Supposons $b \neq 0$. De (2) on déduit $a + d = 1$ et de (1) $c = \dfrac{a - a^2}{b}$. On trouve donc dans ce cas les matrices

$$\begin{pmatrix} a & b \\ \dfrac{a^2 - a}{b} & 1 - a \end{pmatrix} \quad \text{avec} \quad b \in \mathbf{R}^* \quad \text{et} \quad a \in \mathbf{R}\,.$$

6.4 On considère la matrice

$$A = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}.$$

Trouver toutes les matrices à coefficients réels X, X' telles que $AX = A$ et $X'A = A$.

Solution Posons

$$X = \begin{pmatrix} x & y \\ z & t \end{pmatrix},$$

alors

$$A.X = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} 2x + z & 2y + t \\ 2x + z & 2y + t \end{pmatrix}$$

d'où le système

$$\begin{cases} 2x + z = 2 \\ 2y + t = 1 \end{cases} \quad \text{soit} \quad \begin{cases} z = 2 - 2x \\ t = 1 - 2y \end{cases}.$$

Les matrices X telles que $AX = A$ sont donc les matrices de la forme

$$X = \begin{pmatrix} x & y \\ 2 - 2x & 1 - 2y \end{pmatrix} \qquad (x \in \mathbf{R},\ y \in \mathbf{R}).$$

De la même manière si on pose

$$X' = \begin{pmatrix} x' & y' \\ z' & t' \end{pmatrix}$$

on a

$$X'.A = \begin{pmatrix} x' & y' \\ z' & t' \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 2x' + 2y' & x' + y' \\ 2z' + 2t' & z' + t' \end{pmatrix}$$

d'où le système

$$\begin{cases} x' + y' = 1 \\ z' + t' = 1 \end{cases} \quad \text{soit} \quad \begin{cases} y' = 1 - x' \\ t' = 1 - z' \end{cases}.$$

Les matrices X' telles que $X'A = A$ sont donc les matrices de la forme

$$X' = \begin{pmatrix} x' & 1 - x' \\ z' & 1 - z' \end{pmatrix} \qquad (x' \in \mathbf{R},\ z' \in \mathbf{R}).$$

6.5 Soient $A_{11}, A_{12}, A_{21}, A_{22}, B_{11}, B_{12}, B_{21}, B_{22}$ des matrices carrées d'ordre n à coefficients dans un corps commutatif K. On définit des matrices carrées d'ordre $2n$ en posant

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \qquad B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}.$$

Démontrer que

$$A.B = \begin{pmatrix} A_{11}\,B_{11} + A_{12}\,B_{21} & A_{11}\,B_{12} + A_{12}\,B_{22} \\ A_{21}\,B_{11} + A_{22}\,B_{21} & A_{21}\,B_{12} + A_{22}\,B_{22} \end{pmatrix}.$$

Solution Posons

$$A = (a_{ij})_{\substack{1 \leqslant i \leqslant 2n \\ 1 \leqslant j \leqslant 2n}}, \quad B = (b_{ij})_{\substack{1 \leqslant i \leqslant 2n \\ 1 \leqslant j \leqslant 2n}}, \quad A.B = (c_{ij})_{\substack{1 \leqslant i \leqslant 2n \\ 1 \leqslant j \leqslant 2n}}.$$

Pour toute matrice M à coefficients dans K, on notera $(M)_{ij}$ le coefficient de la i-ième ligne et j-ième colonne. On a

$$c_{ij} = \sum_{k=1}^{2n} a_{ik}\,b_{kj} = \sum_{k=1}^{n} a_{ik}\,b_{kj} + \sum_{k=n+1}^{2n} a_{ik}\,b_{kj}.$$

Examinons les quatre cas suivants :

1) $i \leqslant n$ et $j \leqslant n$. Alors pour $1 \leqslant k \leqslant n$,

$$a_{ik} = (A_{11})_{ik} \qquad \text{et} \qquad b_{kj} = (B_{11})_{kj}$$

et pour $n + 1 \leqslant k \leqslant 2n$,

$$a_{ik} = (A_{12})_{i,k-n} \qquad \text{et} \qquad b_{kj} = (B_{21})_{k-n,j},$$

par suite

$$c_{ij} = \sum_{k=1}^{n} (A_{11})_{ik}\,(B_{11})_{kj} + \sum_{k=n+1}^{2n} (A_{12})_{i,k-n}\,(B_{21})_{k-n,j}$$

soit

$$c_{ij} = \sum_{k=1}^{n} (A_{11})_{ik}\,(B_{11})_{kj} + \sum_{l=1}^{n} (A_{12})_{il}\,(B_{21})_{lj}$$

donc

$$c_{ij} = (A_{11}\,B_{11})_{ij} + (A_{12}\,B_{21})_{ij} = (A_{11}\,B_{11} + A_{12}\,B_{21})_{ij}.$$

2) $i \leqslant n$ et $n+1 \leqslant j \leqslant 2n$. Pour $k \leqslant n$, on a $(a_{ik})=(A_{11})_{ik}$ et $b_{kj}=(B_{12})_{k,j-n}$ et pour $n+1 \leqslant k \leqslant 2n$ on a $a_{ik}=(A_{12})_{i,k-n}$, $b_{kj}=(B_{22})_{k-n,j-n}$. On trouve

$$c_{ij} = \sum_{k=1}^{n} (A_{11})_{ik} (B_{12})_{k,j-n} + \sum_{k=n+1}^{2n} (A_{12})_{i,k-n} (B_{22})_{k-n,j-n}$$

$$= (A_{11} B_{12} + A_{12} B_{22})_{i,j-n} .$$

3) $n+1 \leqslant i \leqslant 2n$ et $j \leqslant n$. De la même manière on trouve

$$c_{ij} = (A_{21} B_{11} + A_{22} B_{21})_{i-n,j} .$$

4) $n+1 \leqslant i \leqslant 2n$ et $n+1 \leqslant j \leqslant 2n$. On trouve aussi

$$c_{ij} = (A_{21} B_{12} + A_{22} B_{22})_{i-n,j-n}$$

d'où le résultat.

Ce procédé s'appelle « multiplication des matrices par blocs ».

6.6 A étant une matrice de type (m, n) à coefficients dans un corps commutatif K montrer que $A\,{}^tA$ et ${}^tAA$ sont des matrices carrées symétriques.

Solution Posons

$$A = (a_{ij})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}} \qquad \text{et} \qquad {}^tA = (b_{kl})_{\substack{1 \leqslant k \leqslant n \\ 1 \leqslant l \leqslant m}} .$$

Alors on a $b_{kl} = a_{lk}$ si $1 \leqslant k \leqslant n$ et $1 \leqslant l \leqslant m$. $A\,{}^tA$ est une matrice carrée d'ordre m et ${}^tAA$ une matrice carrée d'ordre n. Posons

$$A\,{}^tA = (c_{ij})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant m}} \qquad \text{et} \qquad {}^tAA = (d_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} .$$

Montrons que ces matrices sont symétriques. On a

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = \sum_{k=1}^{n} a_{ik} a_{jk} \qquad (1 \leqslant i \leqslant m, 1 \leqslant j \leqslant m)$$

et

$$c_{ji} = \sum_{k=1}^{n} a_{jk} b_{ki} = \sum_{k=1}^{n} a_{jk} a_{ik} \qquad (1 \leqslant i \leqslant m, 1 \leqslant j \leqslant m)$$

d'où

$$c_{ij} = c_{ji} \qquad (1 \leqslant i \leqslant m, \quad 1 \leqslant j \leqslant m) .$$

De la même manière on a

$$d_{ij} = \sum_{k=1}^{m} b_{ik} a_{kj} = \sum_{k=1}^{m} a_{ki} a_{kj}$$

et

$$d_{ji} = \sum_{k=1}^{m} b_{jk}\, a_{ki} = \sum_{k=1}^{m} a_{kj}\, a_{ki}$$

donc

$$d_{ij} = d_{ji} \qquad (1 \leqslant i \leqslant n, \quad 1 \leqslant j \leqslant n)$$

6.7 Soient n un entier supérieur à 2 et

$$a = \cos\frac{2\pi}{n} + \mathrm{i}\sin\frac{2\pi}{n}.$$

On désigne par X et Y les matrices de $\mathscr{M}_n(\mathbf{C})$ de termes généraux respectifs :

$$x_{pq} = a^{(p-1)(q-1)}, \qquad y_{pq} = a^{-(p-1)(q-1)}$$

Calculer X^2, Y^2, XY, YX. Quel est l'inverse de X ?

Solution Posons

$$X^2 = (z_{pq})_{\substack{1 \leqslant p \leqslant n \\ 1 \leqslant q \leqslant n}}.$$

On a alors

$$z_{pq} = \sum_{r=1}^{n} x_{pr}\, x_{rq} = \sum_{r=1}^{n} a^{(p-1)(r-1)}\, a^{(r-1)(q-1)} = \sum_{r=1}^{n} (a^{p+q-2})^{r-1}.$$

Si $p + q = 2$ ou $p + q = n + 2$, $a^{p+q-2} = 1$ et $z_{pq} = n$. Dans tous les autres cas,

$$z_{pq} = \frac{(a^{p+q-2})^n - 1}{a^{p+q-2} - 1} = 0$$

donc

$$X^2 = \begin{pmatrix} n & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & \iddots & n \\ 0 & \cdots & \iddots & \iddots & 0 \\ \vdots & \iddots & \iddots & \iddots & \vdots \\ 0 & n & 0 & \cdots & 0 \end{pmatrix}.$$

Posons

$$Y^2 = (u_{pq})_{\substack{1 \leqslant p \leqslant n \\ 1 \leqslant q \leqslant n}}.$$

Alors on a

$$u_{pq} = \sum_{r=1}^{n} y_{pr}\, y_{rq} = \sum_{r=1}^{n} a^{-(p-1)(r-1)}\, a^{-(r-1)(q-1)} = \sum_{r=1}^{n} (a^{2-p-q})^{r-1}.$$

Si $p + q = 2$ ou $p + q = n + 2$, on a $a^{2-p-q} = 1$ et $u_{pq} = n$. Dans tous les autres cas $u_{pq} = 0$ donc $Y^2 = X^2$. Posons

$$XY = (v_{pq})_{\substack{1 \leqslant p \leqslant n \\ 1 \leqslant q \leqslant n}},$$

alors on a

$$v_{pq} = \sum_{r=1}^{n} x_{pr}\, y_{rq} = \sum_{r=1}^{n} a^{(p-1)(r-1)}\, a^{-(r-1)(q-1)} = \sum_{r=1}^{n} (a^{p-q})^{(r-1)}.$$

Comme précédemment, $v_{pq} = 0$ sauf si $a^{p-q} = 1$ auquel cas $v_{pq} = n$. La seule possibilité pour que $a^{p-q} = 1$ est $p = q$, donc $XY = nI_n$.

Posons

$$YX = (t_{pq})_{\substack{1 \leqslant p \leqslant n \\ 1 \leqslant q \leqslant n}}.$$

Alors on a

$$t_{pq} = \sum_{r=1}^{n} y_{pr}\, x_{rq} = \sum_{r=1}^{n} a^{-(p-1)(r-1)}\, a^{(r-1)(q-1)} = \sum_{r=1}^{n} (a^{q-p})^{r-1}$$

Il est clair que $XY = YX = n.I_n$, donc $X^{-1} = \frac{1}{n} Y$.

6.8 Si A est une matrice de $\mathcal{M}_n(\mathbf{R})$ on note $(A)_{ij}$ le coefficient de la i-ième ligne et de la j-ième colonne de A. On pose

$$N(A) = n \sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} \left| (A)_{ij} \right|.$$

a) Montrer que l'application N de $\mathcal{M}_n(\mathbf{R})$ dans $\mathbf{R}_+$ ainsi définie, est une norme.

b) Montrer que si A et B sont deux matrices de $\mathcal{M}_n(\mathbf{R})$, on a

$$N(A.B) \leqslant N(A).N(B).$$

Solution *a*) Pour montrer que N est une norme, il faut vérifier les trois conditions

α) $N(A) = 0$ équivaut à $A = 0$;

β) Si λ est un nombre réel $N(\lambda A) = |\lambda| N(A)$;

γ) Si A et B sont deux éléments de $\mathscr{M}_n(\mathbf{R})$,

$$N(A + B) \leqslant N(A) + N(B).$$

α) Il est clair que $N(0) = 0$; réciproquement, si $N(A) = 0$ on a

$$\sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} |(A)_{ij}| = 0$$

donc $(A)_{ij} = 0$ si $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$, par suite $A = 0$.

β) $$N(\lambda A) = n \sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} |(\lambda A)_{ij}|$$

or $(\lambda A)_{ij} = \lambda (A)_{ij}$ donc

$$N(\lambda A) = n \sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} |\lambda (A)_{ij}| = n |\lambda| \sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} |(A)_{ij}| = |\lambda| N(A).$$

γ) Si A et B sont deux éléments de $\mathscr{M}_n(\mathbf{R})$, on a

$$N(A + B) = n \sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} |(A + B)_{ij}|$$

or $(A+B)_{ij} = (A)_{ij} + (B)_{ij}$ donc $|(A+B)_{ij}| \leqslant |(A)_{ij}| + |(B)_{ij}|$ par suite on a

$$N(A + B) \leqslant n \sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} (|(A)_{ij}| + |(B)_{ij}|) \leqslant n \sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} |(A)_{ij}| + n \sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} |(B)_{ij}$$

soit $N(A + B) \leqslant N(A) + N(B)$.

b) $$N(AB) = n \sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} |(AB)_{ij}|$$

or

$$(AB)_{ij} = \sum_{k=1}^{n} (A)_{ik} (B)_{kj}$$

donc

$$|(AB)_{ij}| \leqslant \sum_{k=1}^{n} |(A)_{ik}| |(B)_{kj}| \leqslant n \sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} |(A)_{ij}| \sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} |(B)_{ij}|.$$

Par suite

$$N(AB) \leqslant n^2 \sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} |(A)_{ij}| \sup_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} |(B)_{ij}| = N(A) N(B).$$

6.9 On dit qu'une matrice A de $\mathscr{M}_n(\mathbf{R})$ est *nilpotente* s'il existe un entier positif p tel que $A^p = 0$. (Pour les propriétés des éléments nilpotents d'un anneau voir l'exercice 3.4.) Soit A une matrice nilpotente de $\mathscr{M}_n(\mathbf{R})$; on définit la matrice e^A de $\mathscr{M}_n(\mathbf{R})$ par

$$e^A = \sum_{p \geqslant 0} \frac{1}{p!} A^p .$$

a) Montrer que si A et B sont deux éléments de $\mathscr{M}_n(\mathbf{R})$ qui commutent, on a

$$e^{A+B} = e^A e^B .$$

b) Calculer e^A, e^B, e^C pour

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad C = \begin{pmatrix} 0 & 1 & -\frac{1}{2} \\ -1 & 0 & \frac{\sqrt{3}}{2} \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \end{pmatrix}.$$

Solution *a*) Comme A et B commutent on peut appliquer la formule du binôme à $A + B$ et on a

$$e^A e^B = \left(\sum_{p \geqslant 0} \frac{1}{p!} A^p \right) \left(\sum_{q \geqslant 0} \frac{1}{q!} B^q \right) = \sum_{p \geqslant 0} \sum_{q \geqslant 0} \frac{1}{p!\, q!} A^p B^q$$

d'où

$$e^A e^B = \sum_{n \geqslant 0} \sum_{k=0}^{n} \frac{1}{k!\,(n-k)!} A^k B^{n-k} = \sum_{n \geqslant 0} \frac{1}{n!} \sum_{k=0}^{n} C_n^k A^k B^{n-k}$$

$$= \sum_{n \geqslant 0} \frac{1}{n!} (A + B)^n = e^{A+B}.$$

b) On a

$$A^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

donc

$$e^A = I + A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

d'autre part on a

$$B^2 = \begin{pmatrix} 0 & 1 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{et} \quad B^3 = 0,$$

donc $e^B = I + B + \frac{1}{2} B^2$ soit

$$e^B = \begin{pmatrix} 1 & 1 & \frac{7}{2} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

enfin on a

$$C^2 = \begin{pmatrix} 0 & 1 & -\frac{1}{2} \\ -1 & 0 & \frac{\sqrt{3}}{2} \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & -\frac{1}{2} \\ -1 & 0 & \frac{\sqrt{3}}{2} \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \end{pmatrix} = \begin{pmatrix} -\frac{3}{4} & -\frac{\sqrt{3}}{4} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{4} & -\frac{1}{4} & \frac{1}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} & 1 \end{pmatrix}$$

et

$$C^3 = C.C^2 = \begin{pmatrix} 0 & 1 & -\frac{1}{2} \\ -1 & 0 & \frac{\sqrt{3}}{2} \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \end{pmatrix} \begin{pmatrix} -\frac{3}{4} & -\frac{\sqrt{3}}{4} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{4} & -\frac{1}{4} & \frac{1}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} & 1 \end{pmatrix} = 0$$

donc $e^C = I + C + \frac{1}{2} C^2$ soit

$$e^C = \begin{pmatrix} \frac{5}{8} & 1 - \frac{\sqrt{3}}{8} & -\frac{1}{2} - \frac{\sqrt{3}}{4} \\ -1 - \frac{\sqrt{3}}{8} & \frac{7}{8} & \frac{\sqrt{3}}{2} + \frac{1}{4} \\ -\frac{1}{2} - \frac{\sqrt{3}}{4} & \frac{\sqrt{3}}{2} - \frac{1}{4} & \frac{3}{2} \end{pmatrix}.$$

6.10

Si

$$A = (a_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}$$

est une matrice carrée d'ordre n à coefficients réels, on définit la *trace* de la matrice A, soit Tr A en posant

$$\text{Tr } A = \sum_{i=1}^{n} a_{ii} .$$

a) Montrer que l'application Tr de $\mathcal{M}_n(\mathbf{R})$ dans $\mathbf{R}$ est une forme linéaire sur $\mathcal{M}_n(\mathbf{R})$ (considéré comme espace vectoriel sur $\mathbf{R}$).

b) Si A et B sont deux matrices de $\mathcal{M}_n(\mathbf{R})$ montrer que Tr (AB) = Tr (BA).

c) Soient X et Y deux matrices de $\mathcal{M}_n(\mathbf{R})$ représentant le même endomorphisme de $\mathbf{R}^n$ par rapport à des bases différentes. Montrer que Tr X = Tr Y.

Solution *a*) Soient

$$A = (a_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}, \qquad B = (b_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}$$

deux matrices de $\mathcal{M}_n(\mathbf{R})$ et λ un nombre réel. Alors on a

$$\text{Tr } (A + B) = \sum_{i=1}^{n} (a_{ii} + b_{ii}) = \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} b_{ii} = \text{Tr } A + \text{Tr } B ,$$

et

$$\text{Tr } (\lambda A) = \sum_{i=1}^{n} \lambda a_{ii} = \lambda \sum_{i=1}^{n} a_{ii} = \lambda \text{ Tr } A ,$$

donc l'application Tr est une forme linéaire sur $\mathcal{M}_n(\mathbf{R})$.

b) Posons

$$C = (c_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} = AB \qquad \text{et} \qquad D = (d_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} = BA ,$$

alors

$$\text{Tr } C = \sum_{i=1}^{n} c_{ii} = \sum_{i=1}^{n} \sum_{k=1}^{n} a_{ik} b_{ki}$$

et

$$\text{Tr } D = \sum_{i=1}^{n} d_{ii} = \sum_{i=1}^{n} \sum_{k=1}^{n} b_{ik} a_{ki}$$

donc Tr C = Tr D soit Tr (AB) = Tr (BA).

c) Si X et Y représentent le même endomorphisme, il existe une matrice P inversible telle que $Y = P^{-1} XP$. Alors d'après la question précédente,

$$\text{Tr } Y = \text{Tr } (P^{-1} XP) = \text{Tr } (XPP^{-1}) = \text{Tr } X .$$

6.11 Soit E l'ensemble des matrices de la forme

$$M(a, b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

où a et b sont des nombres réels.

1) Montrer que E est un sous-espace vectoriel de $\mathcal{M}_2(\mathbf{R})$ (considéré comme espace vectoriel sur $\mathbf{R}$) et un sous-anneau de $\mathcal{M}_2(\mathbf{R})$. Quelle est la dimension de E ?

2) Soit φ l'application de $\mathbf{C}$ dans E définie par $\varphi(a + ib) = M(a, b)$. Montrer que φ est un isomorphisme d'espace vectoriel et d'anneau. E a-t-il une structure de corps ?

Solution 1) Si a, b, a', b', λ sont des nombres réels, on a

$$M(a, b) - M(a', b') = \begin{pmatrix} a - a' & b - b' \\ b' - b & a - a' \end{pmatrix} = M(a - a', b - b'),$$

$$\lambda . M(a, b) = \lambda \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ -\lambda b & \lambda a \end{pmatrix} = M(\lambda a, \lambda b),$$

et

$$M(a, b).M(a', b') = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} aa' - bb' & ab' + ba' \\ -(ab' + ba') & aa' - bb' \end{pmatrix}$$

donc $M(a, b).M(a', b') = M(aa' - bb', ab' + ba')$. Par suite E est un sous-espace vectoriel et un sous-anneau de $\mathcal{M}_2(\mathbf{R})$. Posons

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix};$$

alors I et J forment un système générateur de E puisque pour tout a et tout b dans $\mathbf{R}$ on a $M(a, b) = aI + bJ$. Montrons que I et J forment un système libre ; si λ et μ sont deux nombres réels et si $\lambda I + \mu J = 0$, alors $M(\lambda, \mu) = 0$ donc $\lambda = \mu = 0$; par suite I et J forment une base de E sur $\mathbf{R}$ et E est de dimension 2.

2) Montrons que φ est une application linéaire ; si a, b, a', b', λ sont des nombres réels, on a

$$\varphi[(a + ib) + (a' + ib')] = \varphi((a + a') + i(b + b')) = M(a + a', b + b') = \\ = M(a, b) + M(a', b') = \varphi(a + ib) + \varphi(a' + ib'),$$

et

$$\varphi(\lambda(a + ib)) = \varphi(\lambda a + i\lambda b) = M(\lambda a, \lambda b) = \lambda M(a, b) = \lambda \varphi(a + ib) ;$$

donc φ est bien linéaire ; φ est surjective par définition, de plus si

$$\varphi(a + ib) = M(a, b) = 0$$

on a $a = b = 0$ donc $a + ib = 0$ par suite Ker $\varphi = \{ 0 \}$ et φ est injective. φ est donc un isomorphisme d'espaces vectoriels. On a aussi

$$\varphi[(a+ib)(a'+ib')] = \varphi(aa' - bb' + i(ab' + ba')) = M(aa' - bb', ab' + ba') = \\ = M(a, b) \cdot M(a', b') = \varphi(a+ib) \cdot \varphi(a'+ib'),$$

donc φ est un isomorphisme d'anneaux. E étant un anneau isomorphe au corps $\mathbf{C}$ est lui-même un corps.

6.12 Soit E l'ensemble des matrices carrées d'ordre trois à coefficients rationnels, de la forme

$$M(a, b, c) = \begin{pmatrix} a & b & c \\ 3c & a - 3c & b \\ 3b & -3b + 3c & a - 3c \end{pmatrix}$$

où a, b, c sont dans $\mathbf{Q}$.

a) Trouver trois matrices I, J, K de E, indépendantes de a, b, c, telles que toute matrice de E s'écrive sous la forme $M(a, b, c) = aI + bJ + cK$.

b) Montrer que E muni de l'addition des matrices et de la multiplication par un scalaire, est un sous-espace vectoriel de $\mathcal{M}_3(\mathbf{Q})$. Quelle est sa dimension ?

c) Calculer J^2, $J.K$, $K.J$, K^2.

d) En déduire que E muni de l'addition et de la multiplication des matrices est un sous-anneau commutatif de $\mathcal{M}_3(\mathbf{Q})$.

Solution *a*) Posons

$$I = M(1, 0, 0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$J = M(0, 1, 0) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 3 & -3 & 0 \end{pmatrix}$$

$$K = M(0, 0, 1) = \begin{pmatrix} 0 & 0 & 1 \\ 3 & -3 & 0 \\ 0 & 3 & -3 \end{pmatrix}.$$

Il est alors immédiat de vérifier que si a, b, c sont des nombres rationnels on a $M(a, b, c) = aI + bJ + cK$.

b) Soient $M(a, b, c)$ et $M(a', b', c')$ deux éléments de E et λ un nombre rationnel ; alors on a

$$M(a, b, c) - M(a', b', c') = aI + bJ + cK - a'I - b'J - c'K =$$
$$= (a - a')I + (b - b')J + (c - c')K = M(a - a', b - b', c - c')$$

et

$$\lambda M(a, b, c) = \lambda(aI + bJ + cK) = \lambda aI + \lambda bJ + \lambda cK = M(\lambda a, \lambda b, \lambda c).$$

E est donc un sous-espace vectoriel de $\mathcal{M}_3(\mathbf{Q})$.

Les matrices I, J, K engendrent E puisque tout élément de E est combinaison linéaire de ces matrices. Soient λ, μ, ν des nombres rationnels tels que

$$\lambda I + \mu J + \nu K = 0,$$

alors

$$M(\lambda, \mu, \nu) = \begin{pmatrix} \lambda & \mu & \nu \\ 3\nu & \lambda - 3\nu & \mu \\ 3\mu & -3\mu + 3\nu & \lambda - 3\nu \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

par suite $\lambda = \mu = \nu = 0$, ce qui prouve que les matrices I, J, K sont linéairement indépendantes. Donc I, J, K forment une base de E qui est de dimension 3.

c) On a

$$J^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 3 & -3 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 3 & -3 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 3 & -3 & 0 \\ 0 & 3 & -3 \end{pmatrix} = K,$$

$$K^2 = \begin{pmatrix} 0 & 0 & 1 \\ 3 & -3 & 0 \\ 0 & 3 & -3 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 3 & -3 & 0 \\ 0 & 3 & -3 \end{pmatrix} = \begin{pmatrix} 0 & 3 & -3 \\ -9 & 9 & 3 \\ 3 & -18 & 9 \end{pmatrix} = 3J - 3K,$$

$$J.K = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 3 & -3 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 3 & -3 & 0 \\ 0 & 3 & -3 \end{pmatrix} = \begin{pmatrix} 3 & -3 & 0 \\ 0 & 3 & -3 \\ -9 & 9 & 3 \end{pmatrix} = 3I - 3J,$$

$$K.J = \begin{pmatrix} 0 & 0 & 1 \\ 3 & -3 & 0 \\ 0 & 3 & -3 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 3 & -3 & 0 \end{pmatrix} = \begin{pmatrix} 3 & -3 & 0 \\ 0 & 3 & -3 \\ -9 & 9 & 3 \end{pmatrix} = 3I - 3J.$$

d) Nous avons déjà vu que E est un sous-groupe additif de $\mathcal{M}_3(\mathbf{Q})$. Soient $M(a, b, c)$ et $M(a', b', c')$ deux matrices de E ; alors on a

$$M(a, b, c).M(a', b', c') = (aI + bJ + cK)(a'I + b'J + c'K) =$$
$$= aa'I + ab'J + ac'K + ba'J + bb'J^2 + bc'JK + ca'K + cb'KJ + cc'K^2$$

soit, compte tenu des résultats de la question précédente :

$$M(a, b, c).M(a', b', c') = ad'\,I + ab'\,J + ac'\,K + ba'\,J + bb'\,K + bc'(3\,I - 3\,J) + ca'\,K + cb'(3\,I - 3\,J) + cc'(3\,J - 3\,K) = (aa' + 3\,bc' + 3\,cb')\,I + (ab' + ba' - 3(bc' + cb') + 3\,cc')\,J + (ac' + bb' + ca' - 3\,cc')\,K.$$

Le produit de deux matrices de E étant dans E, celui-ci est un sous-anneau de $\mathcal{M}_3(\mathbf{Q})$. Comme on a $I.J = J.I$, $I.K = K.I$, $J.K = K.J$, ce sous-anneau est commutatif.

6.13 Soit E l'ensemble des matrices carrées d'ordre n ($n \geqslant 2$) à coefficients réels, de la forme

$$M(a, b) = \begin{pmatrix} a & b & \cdots & b \\ b & a & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ b & \cdots & b & a \end{pmatrix} \qquad (a, b) \in \mathbf{R} \times \mathbf{R}).$$

a) Montrer qu'il existe dans E deux matrices I et J ne dépendant ni de a ni de b telles que l'on ait

$$M(a, b) = aI + bJ \qquad ((a, b) \in \mathbf{R} \times \mathbf{R}).$$

b) Montrer que E muni de l'addition des matrices et de la multiplication par un scalaire réel, est un sous-espace vectoriel de $\mathcal{M}_n(\mathbf{R})$. Quelle est sa dimension ?

c) Montrer que E muni de l'addition et de la multiplication des matrices est un sous-anneau de $\mathcal{M}_n(\mathbf{R})$.

d) Déterminer les éléments inversibles de E.

Solution *a*) Soient

$$I = M(1, 0) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

la matrice unité de $\mathscr{M}_n(\mathbf{R})$ et

$$J = M(0, 1) = \begin{pmatrix} 0 & 1 & & & 1 \\ 1 & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 1 \\ 1 & \cdots & \cdots & 1 & 0 \end{pmatrix}$$

Il est clair que pour tous nombres réels a et b on a

$$M(a, b) = aI + bJ .$$

b) Soient $M(a, b)$ et $M(a', b')$ deux éléments de E et λ un nombre réel ; alors on a

$$M(a, b)-M(a', b')=aI+bJ-a' I-b' J=(a-a') I+(b-b') J=M(a-a', b-b')$$

et

$$\lambda M(a, b)=\lambda(aI+bJ)=\lambda aI+\lambda bJ=M(\lambda a, \lambda b) ,$$

donc E est un sous-espace vectoriel de $\mathscr{M}_n(\mathbf{R})$. Nous savons déjà que I et J engendrent E ; d'autre part il est évident que si

$$\lambda I + \mu J = 0 \qquad ((\lambda, \mu) \in \mathbf{R} \times \mathbf{R})$$

alors $M(\lambda, \mu) = 0$ donc $\lambda = \mu = 0$, par suite I et J sont linéairement indépendantes et forment une base de E qui est donc de dimension 2.

c) Nous avons déjà montré que E est un sous-groupe additif de $\mathscr{M}_n(\mathbf{R})$. Pour vérifier que la multiplication est stable dans E, il suffit de montrer que les produits formés à partir de I et J sont encore dans E. Or $I^2 = I$ et $I.J=J.I=J$ car I est l'identité. Pour calculer J^2 posons

$$J = (a_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} \quad \text{et} \quad J^2 = (b_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} :$$

alors $a_{ij} = 1$ si $i \neq j$ et $a_{ij} = 0$ si $i = j$, et on sait que

$$b_{ik} = \sum_{j=1}^{n} a_{ij}\, a_{jk} .$$

Les seuls termes nuls de cette somme sont ceux où figurent a_{ii} ou a_{kk}, les autres étant égaux à 1, donc $b_{ik} = n - 2$ si $i \neq k$ et $b_{ii} = n - 1$, d'où

$$J^2 = (n - 1) I + (n - 2) J .$$

Alors si $M(a, b)$ et $M(a', b')$ sont deux matrices de E on a

$$\begin{aligned} M(a, b).M(a', b')&=(aI+bJ)(a' I+b' J)=aa' I+(ab'+ba') J+bb' J^2= \\ &=(aa'+(n-1) bb') I+((ab'+ba')+(n-2) bb') J= \\ &=M(aa'+(n-1) bb', (ab'+ba')+(n-2) bb') \end{aligned}$$

donc E est un sous-anneau de $\mathscr{M}_n(\mathbf{R})$.

d) Soit $M(a, b)$ un élément non nul de E ; cherchons à quelle condition il existe une matrice $M(x, y)$ de E telle que $M(a, b).M(x, y) = I$. On a d'après la question précédente

$$M(a, b).M(x, y) = M(ax + (n-1)by,\ ay + bx + (n-2)by),$$

d'où le système

$$\begin{cases} ax + (n-1)by = 1 \\ ay + bx + (n-2)by = 0 . \end{cases}$$

Si $b = 0$, a est non nul et on trouve $x = \frac{1}{a}$, $y = 0$ donc

$$[M(a, 0)]^{-1} = M\left(\frac{1}{a}, 0\right).$$

Si $b \neq 0$ et $a = 0$, on a

$$y = \frac{1}{(n-1)b} \qquad \text{et} \qquad x = \frac{2-n}{(n-1)b}$$

donc

$$[M(0, b)]^{-1} = M\left(\frac{2-n}{(n-1)b}, \frac{1}{(n-1)b}\right).$$

Si $a \neq 0$ et $b \neq 0$ en éliminant x on trouve

$$[a^2 + (n-2)ab - (n-1)b^2]y = -b .$$

La condition nécessaire et suffisante pour qu'une solution existe est

$$a^2 + (n-2)ab - (n-1)b^2 \neq 0 .$$

En résolvant l'équation du second degré en a, $a^2 + (n-2)ab - (n-1)b^2 = 0$ on trouve les solutions $a = b$ ou $a = -(n-1)b$. Les éléments inversibles de E sont donc les matrices $M(a, b)$ telles que $a \neq b$ et $a \neq -(n-1)b$ et l'inverse de $M(a, b)$ est :

$$M\left(\frac{a + (n-2)b}{a^2 + (n-2)ab - (n-1)b^2}, \quad \frac{-b}{a^2 + (n-2)ab - (n-1)b^2}\right)$$

6.14

On dit qu'une matrice

$$A = (a_{ij})_{\substack{1 \leqslant i \leqslant 3 \\ 1 \leqslant j \leqslant 3}}$$

de $\mathcal{M}_3(\mathbf{R})$ est *magique* si les huit sommes

$$\sum_{i=1}^{3} a_{i,4-i} ; \quad \sum_{i=1}^{3} a_{ij} (j = 1, 2, 3) ; \quad \sum_{j=1} a_{ij} (i = 1, 2, 3) ; \quad \sum_{i=1}^{3} a_{ii}$$

sont égales. Si A est une matrice magique, on notera $s(A)$ la valeur des huit sommes ci-dessus.

a) Démontrer que l'ensemble $\mathscr{M}$ des matrices magiques muni de l'addition des matrices et de la multiplication par un scalaire est un sous-espace vectoriel de $\mathscr{M}_3(\mathbf{R})$.

b) Soit $\mathscr{A}$ l'ensemble des matrices magiques antisymétriques. Montrer que $\mathscr{A}$ est un sous-espace vectoriel de $\mathscr{M}$. Quelle est la valeur commune des huit sommes d'une matrice de $\mathscr{A}$? Déterminer toutes les matrices de $\mathscr{A}$.

c) Soit $\mathscr{S}$ l'ensemble des matrices magiques symétriques. Montrer qu'une matrice de $\mathscr{S}$ s'écrit comme somme de deux matrices magiques symétriques dont l'une admet 0 comme valeur des huit sommes.

d) Déterminer toutes les matrices de $\mathscr{S}$.

e) Quelle est la dimension de $\mathscr{M}$?

Solution *a*) Soient

$$A = (a_{ij})_{\substack{1 \leqslant i \leqslant 3 \\ 1 \leqslant j \leqslant 3}} \qquad \text{et} \qquad B = (b_{ij})_{\substack{1 \leqslant i \leqslant 3 \\ 1 \leqslant j \leqslant 3}}$$

deux éléments de $\mathscr{M}$. Si

$$C = (c_{ij})_{\substack{1 \leqslant i \leqslant 3 \\ 1 \leqslant j \leqslant 3}}$$

est leur somme, on a

$$c_{ij} = a_{ij} + b_{ij} \qquad (1 \leqslant i \leqslant 3,\ 1 \leqslant j \leqslant 3),$$

$$\sum_{i=1}^{3} c_{ij} = \sum_{i=1}^{3} (a_{ij} + b_{ij}) = \sum_{i=1}^{3} a_{ij} + \sum_{i=1}^{3} b_{ij} \quad (1 \leqslant j \leqslant 3)$$

$$\sum_{j=1}^{3} c_{ij} = \sum_{j=1}^{3} (a_{ij} + b_{ij}) = \sum_{j=1}^{3} a_{ij} + \sum_{j=1}^{3} b_{ij} \quad (1 \leqslant i \leqslant 3)$$

$$\sum_{i=1}^{3} c_{ii} = \sum_{i=1}^{3} (a_{ii} + b_{ii}) = \sum_{i=1}^{3} a_{ii} + \sum_{i=1}^{3} b_{ii}$$

et

$$\sum_{i=1}^{3} c_{i,4-i} = \sum_{i=1}^{3} (a_{i,4-i} + b_{i,4-i}) = \sum_{i=1}^{3} a_{i,4-i} + \sum_{i=1}^{3} b_{i,4-i}.$$

Les matrices A et B étant magiques, ces sommes sont égales et de plus

$$s(C) = s(A) + s(B).$$

Si λ est un nombre réel et

$$D = (d_{ij})_{\substack{1 \leqslant i \leqslant 3 \\ 1 \leqslant j \leqslant 3}}$$

la matrice λA, on a

$$\sum_{i=1}^{3} d_{ij} = \sum_{i=1}^{3} \lambda a_{ij} = \lambda \sum_{i=1}^{3} a_{ij} \quad (1 \leqslant j \leqslant 3)$$

$$\sum_{j=1}^{3} d_{ij} = \sum_{j=1}^{3} \lambda a_{ij} = \lambda \sum_{j=1}^{3} a_{ij} \quad (1 \leqslant i \leqslant 3)$$

$$\sum_{i=1}^{3} d_{ii} = \sum_{i=1}^{3} \lambda a_{ii} = \lambda \sum_{i=1}^{3} a_{ii}$$

et

$$\sum_{i=1}^{3} d_{i,4-i} = \sum_{i=1}^{3} \lambda a_{i,4-i} = \lambda \sum_{i=1}^{3} a_{i,4-i}\,.$$

Comme A est une matrice magique toutes ces sommes sont égales et on a

$$s(D) = \lambda s(A)\,,$$

par suite $\mathscr{M}$ est un sous-espace vectoriel de $\mathscr{M}_3(\mathbf{R})$.

b) Soient

$$A = (a_{ij})_{\substack{1 \leqslant i \leqslant 3 \\ 1 \leqslant j \leqslant 3}} \qquad \text{et} \qquad B = (b_{ij})_{\substack{1 \leqslant i \leqslant 3 \\ 1 \leqslant j \leqslant 3}}$$

deux éléments de $\mathscr{A}$ et

$$C = (c_{ij})_{\substack{1 \leqslant i \leqslant 3 \\ 1 \leqslant j \leqslant 3}}$$

leur somme. Alors on a

$$c_{ji} = a_{ji} + b_{ji} = -a_{ij} - b_{ij} = -c_{ij} \quad (1 \leqslant i \leqslant 3,\ 1 \leqslant j \leqslant 3)$$

donc C est une matrice antisymétrique. De même si λ est un nombre réel et

$$D = (d_{ij})_{\substack{1 \leqslant i \leqslant 3 \\ 1 \leqslant j \leqslant 3}}$$

la matrice λA, on a

$$d_{ji} = \lambda a_{ji} = -\lambda a_{ij} = -d_{ij} \quad (1 \leqslant i \leqslant 3,\ 1 \leqslant j \leqslant 3)$$

donc D est une matrice antisymétrique, par suite $\mathscr{A}$ est un sous-espace vectoriel de $\mathscr{M}$. On sait que les termes diagonaux d'une matrice antisymétrique à coefficients réels sont nuls, donc si A est une matrice magique antisymétrique on a

$$s(A) = \sum_{i=1}^{3} a_{ii} = 0\,.$$

En regardant les autres sommes on trouve $a_{13} = -a_{12}$ et $a_{23} = -a_{13} = a_{12}$. Si on pose $a_{12} = a$, on trouve la forme générale des matrices magiques antisymétriques

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

c) Le fait que $\mathscr{S}$ soit un sous-espace vectoriel de $\mathscr{M}$ se démontre de la même manière que pour $\mathscr{A}$. Soit

$$B = (b_{ij})_{\substack{1 \leqslant i \leqslant 3 \\ 1 \leqslant j \leqslant 3}}$$

une matrice de $\mathscr{S}$ et soit $s = s(B)$ la valeur commune des huit sommes de B. Une décomposition répondant à la question est

$$\begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} = \begin{pmatrix} b_{11} - \frac{s}{3} & b_{12} - \frac{s}{3} & b_{13} - \frac{s}{3} \\ b_{21} - \frac{s}{3} & b_{22} - \frac{s}{3} & b_{23} - \frac{s}{3} \\ b_{31} - \frac{s}{3} & b_{32} - \frac{s}{3} & b_{33} - \frac{s}{3} \end{pmatrix} + \begin{pmatrix} \frac{s}{3} & \frac{s}{3} & \frac{s}{3} \\ \frac{s}{3} & \frac{s}{3} & \frac{s}{3} \\ \frac{s}{3} & \frac{s}{3} & \frac{s}{3} \end{pmatrix}$$

En effet les deux matrices de cette somme sont dans $\mathscr{S}$ et

$$\left(b_{11} - \frac{s}{3}\right) + \left(b_{22} - \frac{s}{3}\right) + \left(b_{33} - \frac{s}{3}\right) = b_{11} + b_{22} + b_{33} - s = s - s = 0$$

d) Soit

$$C = (c_{ij})_{\substack{1 \leqslant i \leqslant 3 \\ 1 \leqslant j \leqslant 3}}$$

une matrice de $\mathscr{S}$ telle que $s(C) = 0$. Comme

$$c_{13} + c_{22} + c_{31} = 0 = 2\,c_{13} + c_{22},$$

on a

$$c_{13} = -\frac{c_{22}}{2}, \qquad \text{alors} \qquad c_{12} = -c_{11} - c_{13} = -c_{11} + \frac{c_{22}}{2}.$$

$$c_{33} = -c_{11} - c_{22} \qquad \text{et} \qquad c_{23} = -c_{13} - c_{33} = c_{11} + \frac{3\,c_{22}}{2}.$$

D'autre part $c_{32} = -c_{12} - c_{22} = c_{11} - \frac{3\,c_{22}}{2}$. En écrivant $c_{23} = c_{32}$ on trouve $c_{22} = 0$. En posant $c_{11} = c$ on trouve la forme générale des matrices C de $\mathscr{S}$ telles que $s(C) = 0$; soit

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

Donc la forme générale des matrices A de $\mathscr{S}$ telles que $s(A) = s$ est

$$c\begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix} + \frac{s}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

e) Toute matrice

$$A = (a_{ij})_{\substack{1 \leqslant i \leqslant 3 \\ 1 \leqslant j \leqslant 3}}$$

de $\mathscr{M}$ s'écrit comme somme d'une matrice symétrique et d'une matrice antisymétrique,

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} a_{11} & \frac{a_{12}+a_{21}}{2} & \frac{a_{13}+a_{31}}{2} \\ \frac{a_{12}+a_{21}}{2} & a_{22} & \frac{a_{23}+a_{32}}{2} \\ \frac{a_{31}+a_{13}}{2} & \frac{a_{23}+a_{32}}{2} & a_{33} \end{pmatrix} +$$

$$+ \begin{pmatrix} 0 & \frac{a_{12}-a_{21}}{2} & \frac{a_{13}-a_{31}}{2} \\ \frac{a_{21}-a_{12}}{2} & 0 & \frac{a_{23}-a_{32}}{2} \\ \frac{a_{31}-a_{13}}{2} & \frac{a_{32}-a_{23}}{2} & 0 \end{pmatrix}$$

donc les trois matrices

$$X = \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

engendrent l'espace vectoriel $\mathscr{M}$.

Soient λ, μ, ν trois nombres réels tels que $\lambda X + \mu Y + \nu Z = 0$. On a $\mu + \nu = 0$ $\lambda - \mu + \nu = 0$ et $-\lambda + \nu = 0$ d'où $\lambda = \mu = \nu = 0$. Les trois matrices X, Y, Z forment donc une base de $\mathscr{M}$ qui est par conséquent de dimension 3.

6.15 Soient a, b, c trois nombres complexes et f l'endomorphisme de $\mathbf{C}^3$ dont la matrice par rapport à la base canonique $\{ e_1, e_2, e_3 \}$ est

$$A = \begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix}.$$

Trouver la matrice de f par rapport à la base

$$e'_1 = e_1 + e_2 + e_3\,, \quad e'_2 = e_2\,, \quad e'_3 = e_3\,.$$

Solution La matrice de passage P de la base $\{ e_1, e_2, e_3 \}$ à la base $\{ e'_1, e'_2, e'_3 \}$ (*cf.* Q., Ch. 8, § III, n° 160) est

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

On a $e_1 = e'_1 - e'_2 - e'_3$, $e_2 = e'_2$ et $e_3 = e'_3$, donc l'inverse de la matrice P est

$$P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}.$$

La matrice de f par rapport à la base $\{ e'_1, e'_2, e'_3 \}$ est $P^{-1}AP$ (*cf.* Q., Ch. 8, § III, n° 161) soit

$$P^{-1}AP = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

soit encore,

$$P^{-1}AP = \begin{pmatrix} a & b & c \\ -a+b & -b+c & -c+a \\ -a+c & -b+a & -c+b \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

soit aussi,

$$P^{-1}AP = \begin{pmatrix} a+b+c & b & c \\ 0 & -b+c & -c+a \\ 0 & -b+a & -c+b \end{pmatrix}.$$

6.16 Soit f l'endomorphisme de l'espace vectoriel $\mathbf{R}^3$ (sur $\mathbf{R}$) dont la matrice par rapport à la base canonique $\{ e_1, e_2, e_3 \}$ est

$$M = \begin{pmatrix} 0 & 1 & -\sin\theta \\ -1 & 0 & \cos\theta \\ -\sin\theta & \cos\theta & 0 \end{pmatrix}$$

θ étant un nombre réel donné.

a) Démontrer que $f^3 = 0$.

b) Pour tout nombre réel t on définit l'application linéaire

$$g_t = h + tf + \frac{t^2}{2} f^2$$

où h est l'application identique. Montrer que l'ensemble G décrit par g_t lorsque t décrit $\mathbf{R}$ est un groupe abélien pour la composition des applications.

c) On pose

$$e'_1 = e_1 \cos\theta + e_2 \sin\theta\,,\quad e'_2 = f(e_1)\,,\quad e'_3 = f(e_2)\,;$$

démontrer que (e'_1, e'_2, e'_3) est une base de $\mathbf{R}^3$.

Déterminer la matrice de f par rapport à cette base.

Solution *a*) Il suffit de montrer que $M^3 = 0$, or

$$M^2 = \begin{pmatrix} 0 & 1 & -\sin\theta \\ -1 & 0 & \cos\theta \\ -\sin\theta & \cos\theta & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & -\sin\theta \\ -1 & 0 & \cos\theta \\ -\sin\theta & \cos\theta & 0 \end{pmatrix}$$

$$= \begin{pmatrix} -\cos^2\theta & -\sin\theta\cos\theta & \cos\theta \\ -\sin\theta\cos\theta & -\sin^2\theta & \sin\theta \\ -\cos\theta & -\sin\theta & 1 \end{pmatrix}$$

et $M^3 = M^2.M = 0$.

b) Calculons $g_t \circ g_{t'}$ où t, t' sont des nombres réels ;

$$g_t \circ g_{t'} = \left(h + tf + \frac{t^2}{2} f^2\right) \circ \left(h + t'f + \frac{t'^2}{2} f^2\right)$$

$$= h + t'f + \frac{t'^2}{2} f^2 + tf + tt'f^2 + \frac{t^2}{2} f^2$$

$$= h + (t + t')f + \frac{1}{2}(t + t')^2 f^2 = g_{t+t'}\,.$$

Donc G est stable pour la composition des applications, de plus $h = g_0$ donc $h \in G$ et pour tout t, $g_t \circ g_{-t} = g_0 = h = g_{-t} \circ g_t$, donc $(g_t)^{-1} = g_{-t}$ et G est un groupe pour la composition des applications ; il est abélien car si t, t' sont des nombres réels on a

$$g_t \circ g_{t'} = g_{t+t'} = g_{t'+t} = g_{t'} \circ g_t\,.$$

c) La matrice de passage P (*cf.* Q., Ch. 8, § III, n° 160) est

$$P = \begin{pmatrix} \cos\theta & 0 & 1 \\ \sin\theta & -1 & 0 \\ 0 & -\sin\theta & \cos\theta \end{pmatrix}$$

car $f(e_1) = -e_2 - e_3 \sin\theta$ et $f(e_2) = e_1 + e_3 \cos\theta$; on a donc

$$\begin{cases} e'_1 = e_1 \cos\theta + e_2 \sin\theta \\ e'_2 = -e_2 - e_3 \sin\theta \\ e'_3 = e_1 + e_3 \cos\theta . \end{cases}$$

En résolvant ce système on trouve

$$\begin{cases} e_1 = e'_1 \cos\theta + e'_2 \sin\theta \cos\theta + e'_3 \sin^2\theta \\ e_2 = e'_1 \sin\theta - e'_2 \cos^2\theta - e'_3 \sin\theta \cos\theta \\ e_3 = -e'_1 - e'_2 \sin\theta + e'_3 \cos\theta \end{cases}$$

d'où la matrice inverse de P

$$P^{-1} = \begin{pmatrix} \cos\theta & \sin\theta & -1 \\ \sin\theta\cos\theta & -\cos^2\theta & -\sin\theta \\ \sin^2\theta & -\sin\theta\cos\theta & \cos\theta \end{pmatrix}.$$

On sait (*cf.* Q., Ch. 8, § III, n° 161) que la matrice de f par rapport à la base $\{ e'_1, e'_2, e'_3 \}$ est égale à $P^{-1}MP$. Or

$$MP = \begin{pmatrix} \sin\theta & -\cos^2\theta & -\sin\theta\cos\theta \\ \cos\theta & -\sin\theta\cos\theta & -\sin^2\theta \\ 0 & -\cos\theta & -\sin\theta \end{pmatrix},$$

donc

$$P^{-1}MP = \begin{pmatrix} 0 & 0 & 0 \\ -\cos\theta & \sin\theta\cos\theta & \sin^2\theta \\ \sin\theta & -\cos^2\theta & -\sin\theta\cos\theta \end{pmatrix}.$$

6.17 K étant un corps commutatif de caractéristique différente de 2 et E un espace vectoriel de dimension finie n sur K, on considère un endomorphisme f de E tel que $f \circ f = \mathrm{Id}\, E$. On pose $g = \mathrm{Id}\, E + f$ et $h = \mathrm{Id}\, E - f$.

a) Montrer que $g(E)$ et $h(E)$ sont stables par f et sont deux sous-espaces supplémentaires de E. Quelles sont les applications induites par f respectivement dans $g(E)$ et $h(E)$?

b) En déduire que toute matrice M de $\mathcal{M}_n(K)$ telle que $M^2 = I_n$ est semblable à une matrice de la forme

$$\begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix}$$

où $p \in \mathbf{N}$, $q \in \mathbf{N}$ et $p + q = n$.

Solution *a*) Soit y un élément de $g(E)$, il existe un élément x de E tel que

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

on a donc $f(y) = f\big(x + f(x)\big) = f(x) + f \circ f(x) = x + f(x) = y$ par suite $g(E)$ est stable par f et l'application induite par f dans $g(E)$ est Id $g(E)$. Soit z un élément de $h(E)$, il existe un élément x de E tel que $z = h(x) = x - f(x)$; on a donc $f(z) = f\big(x - f(x)\big) = f(x) - x = -z$ par suite $h(E)$ est stable par f et f induit l'application $-$ Id $h(E)$ dans $h(E)$.

On a $g(E) \cap h(E) = \{ 0 \}$ car si x est un élément de $g(E) \cap h(E)$, d'après ce qu'on a vu $f(x) = x = -x$ donc $2x = 0$ et comme K n'est pas de caractéristique 2, $x = 0$.

Par ailleurs si y est un élément de E on peut écrire

$$y = \tfrac{1}{2} y + \tfrac{1}{2} f(y) + \tfrac{1}{2} y - \tfrac{1}{2} f(y)$$

(l'inverse de 2 existe dans K puisque la caractéristique de K n'est pas 2). Mais $\frac{1}{2} y + \frac{1}{2} f(y) = g(\frac{1}{2} y)$ et $\frac{1}{2} y - \frac{1}{2} f(y) = h(\frac{1}{2} y)$ donc nous avons écrit y sous la forme d'une somme d'un élément de $g(E)$ et d'un élément de $h(E)$, par suite

$$E = g(E) + h(E) \quad \text{donc} \quad E = g(E) \oplus h(E) .$$

b) Soit f l'endomorphisme de K^n dont la matrice par rapport à la base canonique est M ; comme $M^2 = I_n$ on a $f^2 = \text{Id}\, E$. D'après (*a*) il existe deux sous-espaces supplémentaires P et Q de E dans lesquels f induit respectivement Id P et $-$ Id Q. Si $p = \dim P$ et $q = \dim Q$, on a $n = p + q$ et il existe une base de E dont les p premiers éléments forment une base de P et les q derniers une base de Q. Par rapport à une telle base la matrice de f est

$$\begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix}$$

et cette matrice est semblable à M puisqu'elle définit le même endomorphisme de K^n que M.

6.18 Soit E un espace vectoriel de dimension finie sur $\mathbf{R}$. On désigne par f un endomorphisme de E tel que $f \circ f = -\text{Id}\, E$, et on définit une loi externe sur $\mathbf{C} \times E$ en posant pour tout nombre complexe $a + ib$ et pour tout élément x de E

$$(a + ib) * x = ax - bf(x) .$$

a) Soit E' l'ensemble sous-jacent à E muni de l'addition de E et de la multiplication définie ci-dessus. Montrer que E' a une structure d'espace vectoriel sur $\mathbf{C}$.

b) Montrer que si $\{ a_1, a_2, ..., a_n \}$ est une base de E', alors

$$\{ a_1, a_2, ..., a_n, f(a_1), f(a_2), ..., f(a_n) \}$$

est une base de E. En déduire que s'il existe un endomorphisme f de E tel que $f \circ f = -\operatorname{Id} E$, E est de dimension paire.

c) Trouver la matrice de f relativement à la base trouvée en (*b*). En déduire que sur tout espace vectoriel E de dimension paire sur **R**, il existe au moins un endomorphisme f tel que $f \circ f = -\operatorname{Id} E$.

d) Soit g une application de E dans lui-même.

Démontrer que les deux propriétés suivantes sont équivalentes :

α) g est un endomorphisme de l'espace vectoriel E sur **R** qui commute avec f.

β) g est un endomorphisme de l'espace vectoriel E' sur **C**.

e) Soit G une matrice de $\mathscr{M}_n(\mathbf{C})$; on pose $G = A + iB$ où A et B sont des matrices de $\mathscr{M}_n(\mathbf{R})$ et

$$\varphi(G) = \begin{pmatrix} A & B \\ -B & A \end{pmatrix}.$$

Démontrer que φ est un homomorphisme de l'anneau $\mathscr{M}_n(\mathbf{C})$ dans l'anneau $\mathscr{M}_{2n}(\mathbf{R})$. Démontrer que Im φ est l'ensemble des matrices de $\mathscr{M}_{2n}(\mathbf{R})$ qui commutent avec la matrice

$$\begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}.$$

Solution *a*) E' est un groupe abélien pour l'addition puisque l'addition est la même que celle de E. Il reste à vérifier les axiomes relatifs à la multiplication (*cf.* Q. Ch. 7, § I, n° 125).

Si a, b, c, d sont des nombres réels et x un élément de E' on a

$$\begin{aligned} [(a + ib)(c + id)] * x &= (ac - bd + i(ad + bc)) * x \\ &= (ac - bd)x - (ad + bc) f(x) \\ &= a(cx - df(x)) - b(cf(x) - df \circ f(x)) \\ &= (a + ib) * [(c + id) * x]. \end{aligned}$$

Si a, b sont des nombres réels et x, y des éléments de E', on a

$$\begin{aligned} (a + ib) * (x + y) = a(x + y) - bf(x + y) &= ax - bf(x) + ay - bf(y) \\ &= (a + ib) * x + (a + ib) * y. \end{aligned}$$

Si a, b, c, d sont des nombres réels et x un élément de E on a

$$((a + ib) + (c + id)) * x = (a + c)\,x - (b + d)f(x) =$$
$$= ax - bf(x) + cx - df(x) = (a + ib) * x + (c + id) * x,$$

enfin si x est un élément de E on a

$$1 * x = (1 + 0.i) * x = x - 0.f(x) = x.$$

Donc E' est un espace vectoriel sur $\mathbf{C}$.

b) Montrons que les $2n$ vecteurs proposés sont linéairement indépendants dans E. Soient $\lambda_1, \lambda_2, \ldots, \lambda_n, \mu_1, \mu_2, \ldots, \mu_n$ des nombres réels tels que

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n + \mu_1 f(a_1) + \mu_2 f(a_2) + \cdots + \mu_n f(a_n) = 0$$

on a

$$\lambda_j a_j + \mu_j f(a_j) = (\lambda_j - i\mu_j) * a_j \qquad \text{si} \qquad 1 \leqslant j \leqslant n$$

donc

$$(\lambda_1 - i\mu_1) * a_1 + (\lambda_2 - i\mu_2) * a_2 + \cdots + (\lambda_n - i\mu_n) * a_n = 0,$$

or $a_1, a_2, \ldots, a_n$ est une base de E' donc $\lambda_1 - i\mu_1 = \lambda_2 - i\mu_2 = \cdots = \lambda_n - i\mu_n = 0$ par suite $\lambda_1 = \lambda_2 = \cdots = \lambda_n = \mu_1 = \mu_2 = \cdots = \mu_n = 0$. Montrons maintenant que les vecteurs $a_1, a_2, \ldots, a_n, f(a_1), f(a_2), \ldots, f(a_n)$ engendrent E. Soit x un élément de E ; comme élément de E', x s'écrit sur la base $a_1, a_2, \ldots, a_n$

$$x = (\alpha_1 + i\beta_1) * a_1 + (\alpha_2 + i\beta_2) * a_2 + \cdots + (\alpha_n + i\beta_n) * a_n$$

soit

$$x = \alpha_1 a_1 - \beta_1 f(a_1) + \alpha_2 a_2 - \beta_2 f(a_2) + \cdots + \alpha_n a_n - \beta_n f(a_n)$$

donc x est bien combinaison linéaire des vecteurs proposés, par suite

$$\dim E = 2n = 2 \dim E',$$

donc s'il existe un endomorphisme f tel que $f \circ f = -\operatorname{Id} E$, la dimension de E est paire.

c) Si on appelle $\{ e_1, e_2, \ldots, e_{2n} \}$ la base ci-dessus de E, on a $e_i = a_i$ si $1 \leqslant i \leqslant n$ et $e_j = f(a_{j-n})$ si $n + 1 \leqslant j \leqslant 2n$, donc $f(e_i) = e_{n+i}$ si $1 \leqslant i \leqslant n$ et $f(e_j) = f \circ f(a_{j-n}) = -a_{j-n} = -e_{j-n}$ si $n + 1 \leqslant j \leqslant 2n$. La matrice de f sur cette base est

$$\begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}$$

où I_n est la matrice unité d'ordre n et 0 la matrice nulle d'ordre n.

Si E est un espace vectoriel de dimension paire $2n$, muni d'une base, la matrice ci-dessus définit un endomorphisme dont le carré est $-\operatorname{Id} E$ car

$$\begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \begin{pmatrix} 0 & -I_n \\ I_n & \end{pmatrix} = \begin{pmatrix} -I_n & 0 \\ 0 & -I_n \end{pmatrix} = -I_{2n}$$

(la multiplication est effectuée par blocs, *cf.* exercice 6.5).

d) Supposons (α) vérifiée. Pour démontrer (β) il suffit d'étudier le comportement de g par rapport à la multiplication ; soient $a + ib$ un nombre complexe et x un élément de E', on a

$$g[(a + ib) * x] = g(ax - bf(x)) = ag(x) - bg(f(x)) =$$
$$= ag(x) - bf(g(x)) = (a + ib) * g(x),$$

donc g est un endomorphisme de E'.

Supposons maintenant (β) vraie et soit x un élément de E, on a

$$g(f(x)) = g(-i * x) = -i * g(x) = f(g(x))$$

donc f et g commutent.

e) Soient $G = A + iB$, $G' = A' + iB'$ deux matrices de $\mathscr{M}_n(\mathbf{C})$ et leurs décompositions en matrices de $\mathscr{M}_n(\mathbf{R})$, on a

$$\varphi(G + G') = \begin{pmatrix} A + A' & B + B' \\ -B - B' & A + A' \end{pmatrix} =$$

$$= \begin{pmatrix} A & B \\ -B & A \end{pmatrix} + \begin{pmatrix} A' & B' \\ -B' & A' \end{pmatrix} = \varphi(G) + \varphi(G'),$$

et

$$\varphi(GG') = \varphi(AA' - BB' + i(AB' + BA')) = \begin{pmatrix} AA' - BB' & AB' + BA' \\ -(AB' + BA') & AA' - BB' \end{pmatrix} =$$

$$= \begin{pmatrix} A & B \\ -B & A \end{pmatrix} \begin{pmatrix} A' & B' \\ -B' & A' \end{pmatrix} = \varphi(G)\,\varphi(G'),$$

donc φ est un homomorphisme de l'anneau $\mathscr{M}_n(\mathbf{C})$ dans l'anneau $\mathscr{M}_{2n}(\mathbf{R})$. Les matrices de Im φ commutent avec la matrice donnée car

$$\begin{pmatrix} A & B \\ -B & A \end{pmatrix} \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} = \begin{pmatrix} B & -A \\ A & B \end{pmatrix} = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \begin{pmatrix} A & B \\ -B & A \end{pmatrix}$$

d'autre part cherchons à quelle condition une matrice $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ de $\mathscr{M}_{2n}(\mathbf{R})$ commute avec la matrice $\begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}$; on a

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} = \begin{pmatrix} B & -A \\ D & -C \end{pmatrix} \text{ et } \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} -C & -D \\ A & B \end{pmatrix}$$

on trouve donc $A = D$ et $B = -C$ c'est-à-dire que la matrice doit être de la forme $\varphi(A + iB)$ avec $A + iB$ dans $\mathscr{M}_n(\mathbf{C})$.

6.19 Trouver le rang des matrices suivantes à coefficients dans $\mathbf{Q}$.

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

b)
$$\begin{pmatrix} 1 & 7 & 5 & 3 & -2 \\ 0 & 4 & 2 & 2 & 0 \\ 2 & -2 & 4 & 0 & 1 \\ 3 & -1 & 7 & 1 & 3 \end{pmatrix}.$$

Solution La méthode est la même que celle qui sert à déterminer le rang d'un système de vecteurs (*cf.* Q. Ch. 7, § III, n° 138).

a)
$$\begin{array}{ccc} v_1 & v_2 & v_3 \\ 2 & -3 & -4 \\ 3 & 1 & 5 \\ -1 & 0 & -1 \\ 0 & 2 & 4 \end{array}$$

est un système de vecteurs de $\mathbf{Q}^4$ de même rang que le système suivant

$$\begin{array}{ccc} v_1 & v_2' = 2v_2 + 3v_1 & v_3' = v_3 + 2v_1 \\ 2 & 0 & 0 \\ 3 & 11 & 11 \\ -1 & -3 & -3 \\ 0 & 4 & 4 \end{array}$$

On a $v_2' = v_3'$ et les vecteurs v_1, v_2 forment une famille libre, par suite la matrice proposée est de rang 2.

b) Le système de vecteurs de $\mathbf{Q}^4$

$$\begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \\ 1 & 7 & 5 & 3 & -2 \\ 0 & 4 & 2 & 2 & 0 \\ 2 & -2 & 4 & 0 & 1 \\ 3 & -1 & 7 & 1 & 3 \end{array}$$

est de même rang que le système suivant

$$\begin{array}{ccccc} v_1 & v_2' = v_2 - 7v_1 & v_3' = v_3 - 5v_1 & v_4' = v_4 - 3v_1 & v_5' = v_5 + 2v_1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 4 & 2 & 2 & 0 \\ 2 & -16 & -6 & -6 & 5 \\ 3 & -22 & -8 & -8 & 9 \end{array}$$

Comme $v_3' = v_4'$ le rang du système ci-dessus est le même que celui du système $\{ v_1, v_2', v_3', v_5' \}$ qui est égal à celui des systèmes suivants

v_1	v_2'	$v_3'' = v_3' - \frac{1}{2} v_2'$	v_5'
1	0	0	0
0	4	0	0
2	−16	2	5
3	−22	3	9

v_1	v_2'	v_3''	$v_5'' = 2 v_5' - 5 v_3''$
1	0	0	0
0	4	0	0
2	−16	2	0
3	−22	3	3

Ce dernier système étant de rang 4, le rang de la matrice proposée est 4.

6.20 Trouver le rang des matrices suivantes à coefficients dans C.

a)
$$\begin{pmatrix} 1 & -1 & 3 \\ -1 & \mathrm{i} & -1-2\,\mathrm{i} \\ \mathrm{i} & 1 & \mathrm{i}-2 \end{pmatrix}.$$

b)
$$\begin{pmatrix} 1 & -\mathrm{i} & -\mathrm{i} & 1 \\ \mathrm{i} & 1 & 1 & \mathrm{i} \\ 1 & 1 & 3\,\mathrm{i} & 3 \end{pmatrix}.$$

Solution Nous appliquons la méthode utilisée dans l'exercice précédent.

a) La matrice proposée fournit le système de vecteurs de $\mathbf{C}^3$

v_1	v_2	v_3
1	−1	3
−1	i	−1−2 i
i	1	i−2

donc le rang est celui du système suivant

v_1	$v_2' = v_1 + v_2$	$v_3' = v_3 - 3 v_1$
1	0	0
−1	i−1	2−2 i
i	i+1	−2 i−2

Il est clair que $v_3' = -2 v_2'$ donc la matrice est de rang 2.

b) Le système de vecteurs de $\mathbf{C}^3$

v_1	v_2	v_3	v_4
1	$-i$	$-i$	1
i	1	1	i
1	i	3 i	3

est de même rang que le système

v_1	$v_2' = v_2 + iv_1$	$v_3' = v_3 + iv_1$	$v_4' = v_4 - v_1$
1	0	0	0
i	0	0	0
1	2 i	4 i	2

or on a $v_3' = 2v_2'$ et $v_4' = iv_2'$; comme v_1 et v_2' sont lineairement indépendants ce système est de rang 2 ainsi que la matrice proposée.

6.21 Trouver le rang des matrices suivantes à coefficients dans **R**.

a)
$$\begin{pmatrix} a & 0 & b \\ b & a & 0 \\ 0 & b & a \end{pmatrix}.$$

b)
$$\begin{pmatrix} a & 0 & 0 & b \\ b & a & 0 & 0 \\ 0 & b & a & 0 \\ 0 & 0 & b & a \end{pmatrix}.$$

Solution *a*) Il est clair que si $a = b = 0$ le rang de la matrice est 0 est que si $a = 0$, $b \neq 0$, la matrice est de rang 3. Supposons maintenant $a \neq 0$, alors les systèmes suivants de vecteurs de $\mathbf{R}^3$ sont de même rang

v_1	v_2	v_3
a	0	b
b	a	0
0	b	a

v_1	v_2	$v_3' = av_3 - bv_1$
a	0	0
b	a	$-b^2$
0	b	a^2

v_1	v_2	$v_3'' = av_3' + b^2 v_2$
a	0	0
b	a	0
0	b	a^3+b^3

si $a = -b$ la matrice est de rang 2, si $a \neq -b$ elle est de rang 3.

b) Comme en (*a*) si $a = b = 0$ la matrice est de rang 0 et si $a = 0$ et $b \neq 0$, elle est de rang 4. Supposons donc $a \neq 0$; alors les systèmes suivants de vecteurs de $\mathbf{R}^4$ sont de même rang

v_1	v_2	v_3	v_4
a	0	0	b
b	a	0	0
0	b	a	0
0	0	b	a

v_1	v_2	v_3	$v_4' = av_4 - bv_1$
a	0	0	0
b	a	0	$-b^2$
0	b	a	0
0	0	b	a^2

v_1	v_2	v_3	$v_4'' = av_4' + b^2 v_2$
a	0	0	0
b	a	0	0
0	b	a	b^3
0	0	b	a^3

v_1	v_2	v_3	$v_4''' = av_4'' - b^3 v_3$
a	0	0	0
b	a	0	0
0	b	a	0
0	0	b	$a^4 - b^4$

Donc si $a^2 \neq b^2$ la matrice est de rang 4 et si $a = b$ ou si $a = -b$, le rang de la matrice est 3.

7

DÉTERMINANTS ET ÉQUATIONS LINÉAIRES

7.1 Soient E, F, G trois espaces vectoriels sur un même corps commutatif K. Démontrer que la seule application linéaire de $E \times F$ dans G qui soit aussi une application bilinéaire de $E \times F$ dans G, est l'application nulle.

Solution Soit f une application linéaire et bilinéaire de $E \times F$ dans G ; comme f est linéaire on a $f(0, 0) = 0$. Soit (x, y) un élément quelconque de $E \times F$; calculons $f(x, y) = f(x + 0, y + 0)$ en utilisant le fait que f est bilinéaire, il vient

$$f(x + 0, y + 0) = f(x, y) + f(x, 0) + f(0, y) + f(0, 0)$$

donc nous avons $f(x, 0) + f(0, y) = 0$ et puisque f est linéaire,

$$(x, 0) + f(0, y) = f[(x, 0) + (0, y)] = f(x, y) = 0 .$$

Par suite, pour tout élément (x, y) de $E \times F$ on a $f(x, y) = 0$ donc f est l'application nulle de $E \times F$ dans G.

7.2 Calculer les déterminants suivants :

$$a) \quad D_1 = \begin{vmatrix} 112 & 127 \\ 97 & 110 \end{vmatrix} \qquad D_2 = \begin{vmatrix} 66 & 106 \\ 41 & 66 \end{vmatrix} \qquad D_3 = \begin{vmatrix} 92 & 72 \\ 74 & 59 \end{vmatrix}$$

$$b) \quad D_4 = \begin{vmatrix} 1 & \log_b a \\ \log_a b & 1 \end{vmatrix} \qquad D_5 = \begin{vmatrix} a+b & b+d \\ a+c & c+d \end{vmatrix} \qquad D_6 = \begin{vmatrix} \omega & \omega \\ -1 & \omega \end{vmatrix}$$

où a, b, c, d sont des nombres réels avec $a > 0$, $a \neq 1$ et $b > 0$, $b \neq 1$, et où

$$\omega = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}.$$

Solution *a*) Remplaçons la première ligne par la différence entre la première et la seconde ligne, nous obtenons

$$D_1 = \begin{vmatrix} 112 & 127 \\ 97 & 110 \end{vmatrix} = \begin{vmatrix} 15 & 17 \\ 97 & 110 \end{vmatrix}.$$

Remplaçons la seconde colonne par la différence entre la seconde et la première colonne, il vient

$$D_1 = \begin{vmatrix} 15 & 17 \\ 97 & 110 \end{vmatrix} = \begin{vmatrix} 15 & 2 \\ 97 & 13 \end{vmatrix}.$$

Remplaçons la seconde ligne par la différence entre la seconde ligne et 6 fois la première

$$D_1 = \begin{vmatrix} 15 & 2 \\ 97 & 13 \end{vmatrix} = \begin{vmatrix} 15 & 2 \\ 7 & 1 \end{vmatrix} = 15 \times 1 - 2 \times 7 = 1$$

donc $D_1 = 1$ et un calcul analogue permet de montrer que $D_2 = 10$ et $D_3 = 100$.

b) Puisque

$$\log_a b = \frac{\operatorname{Log} b}{\operatorname{Log} a} \quad \text{et} \quad \log_b a = \frac{\operatorname{Log} a}{\operatorname{Log} b} \quad \text{on a} \quad D_4 = 0.$$

Des combinaisons linéaires entre lignes et colonnes montrent que $D_5 = (b - c)(d - a)$.

Nous avons $D_6 = \omega^2 + \omega$; comme ω est une racine cubique de 1, nous avons $\omega^2 + \omega + 1 = 0$ d'où $D_6 = -1$.

7.3 Démontrer que si a, b, c sont des nombres réels

$$D = \begin{vmatrix} a - b - c & 2a & 2a \\ 2b & b - c - a & 2b \\ 2c & 2c & c - a - b \end{vmatrix} = (a + b + c)^3.$$

Solution Remplaçons la première ligne par la somme des trois lignes ; nous obtenons

$$D = \begin{vmatrix} a-b-c & 2a & 2a \\ 2b & b-c-a & 2b \\ 2c & 2c & c-a-b \end{vmatrix} = \begin{vmatrix} a+b+c & a+b+c & a+b+c \\ 2b & b-c-a & 2b \\ 2c & 2c & c-a-b \end{vmatrix}.$$

Remplaçons la deuxième (resp. troisième) colonne par la différence entre la deuxième (resp. troisième) colonne et la première ; nous obtenons,

$$\begin{vmatrix} a+b+c & a+b+c & a+b+c \\ 2b & b-c-a & 2b \\ 2c & 2c & c-a-b \end{vmatrix} = \begin{vmatrix} a+b+c & 0 & 0 \\ 2b & -a-b-c & 0 \\ 2c & 0 & -a-b-c \end{vmatrix}$$

d'où en développant ce déterminant par rapport à sa première ligne,

$$D = (a + b + c)^3 .$$

7.4 Calculer

$$D = \begin{vmatrix} 1 & \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} & \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} \\ \cos\frac{\pi}{3} - i\sin\frac{\pi}{3} & 1 & \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} \\ \cos\frac{\pi}{4} - i\sin\frac{\pi}{4} & \cos\frac{2\pi}{3} - i\sin\frac{2\pi}{3} & 1 \end{vmatrix}$$

Solution Posons, pour chaque nombre réel α, $e^{i\alpha} = \cos\alpha + i\sin\alpha$. Le déterminant D s'écrit alors

$$D = \begin{vmatrix} 1 & e^{\frac{i\pi}{3}} & e^{\frac{i\pi}{4}} \\ e^{-\frac{i\pi}{3}} & 1 & e^{\frac{2i\pi}{3}} \\ e^{-\frac{i\pi}{4}} & e^{-\frac{2i\pi}{3}} & 1 \end{vmatrix}$$

d'où, en le développant au moyen de la règle de SARRUS,

$$D = 1 + e^{-\frac{i\pi}{4}} e^{\frac{i\pi}{3}} e^{\frac{2i\pi}{3}} + e^{\frac{i\pi}{4}} e^{-\frac{i\pi}{3}} e^{-\frac{2i\pi}{3}} - \left(e^{\frac{i\pi}{4}} e^{-\frac{i\pi}{4}} + e^{\frac{i\pi}{3}} e^{-\frac{i\pi}{3}} + e^{\frac{2i\pi}{3}} e^{-\frac{2i\pi}{3}}\right)$$

$$= 1 - \left(e^{-\frac{i\pi}{4}} + e^{\frac{i\pi}{4}}\right) - 3 = -2\cos\frac{\pi}{4} - 2 = -\sqrt{2} - 2 .$$

7.5 Démontrer que si a, b, c sont des nombres réels,

$$D = \begin{vmatrix} 1 & \sin a & \cos a \\ 1 & \sin b & \cos b \\ 1 & \sin c & \cos c \end{vmatrix} = \sin(b-c) + \sin(c-a) + \sin(a-b)$$

$$- 4 \sin \frac{b-c}{2} \sin \frac{c-a}{2} \sin \frac{a-b}{2}.$$

Solution Remplaçons la deuxième (resp. troisième) ligne par la différence entre la deuxième (resp. troisième) ligne et la première. Nous obtenons

$$D = \begin{vmatrix} 1 & \sin a & \cos a \\ 0 & \sin b - \sin a & \cos b - \cos a \\ 0 & \sin c - \sin a & \cos c - \cos a \end{vmatrix}$$

d'où en développant par rapport à la première colonne,

$$D = (\sin b - \sin a)(\cos c - \cos a) - (\cos b - \cos a)(\sin c - \sin a) ;$$

en développant et simplifiant on obtient

$$D = \sin(b-c) + \sin(c-a) + \sin(a-b),$$

or on a

$$\sin(b-c) + \sin(c-a) = 2 \sin \frac{b-a}{2} \cos \frac{a+b-2c}{2}$$

et

$$\sin(a-b) = 2 \sin \frac{a-b}{2} \cos \frac{a-b}{2},$$

donc

$$D = 2 \sin \frac{a-b}{2} \left(\cos \frac{a-b}{2} - \cos \frac{a+b-2c}{2} \right)$$

$$= - 4 \sin \frac{a-b}{2} \sin \frac{c-a}{2} \sin \frac{b-c}{2}.$$

7.6 Calculer

$$D = \begin{vmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{vmatrix}$$

où

$$\omega = \cos\frac{2\pi}{3} + \mathrm{i}\sin\frac{2\pi}{3}.$$

Solution Remplaçons la première ligne par la somme des trois lignes du déterminant. Sachant que $\omega^3 = 1$ et $1 + \omega + \omega^2 = 0$, on obtient

$$D = \begin{vmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{vmatrix} = \begin{vmatrix} 3 & 0 & 0 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{vmatrix} = 3\begin{vmatrix} \omega & \omega^2 \\ \omega^2 & \omega \end{vmatrix} = 3(\omega^2 - \omega).$$

Comme $\omega^2 = \overline{\omega}$:

$$D = 3(\overline{\omega} - \omega) = -6\,\mathrm{i}\,\mathrm{Im}\,\omega = -6\,\mathrm{i}\sin\frac{2\pi}{3}.$$

7.7 Démontrer que si a, b, c sont des nombres réels,

$$D = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & \cos c & \cos b \\ 1 & \cos c & 1 & \cos a \\ 1 & \cos b & \cos a & 1 \end{vmatrix} = -16\sin^2\frac{a}{2}\sin^2\frac{b}{2}\sin^2\frac{c}{2}.$$

Solution Retranchons la première colonne de chacune des trois autres, on obtient

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & \cos c & \cos b \\ 1 & \cos c & 1 & \cos a \\ 1 & \cos b & \cos a & 1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & \cos c - 1 & \cos b - 1 \\ 1 & \cos c - 1 & 0 & \cos a - 1 \\ 1 & \cos b - 1 & \cos a - 1 & 0 \end{vmatrix}$$

par suite, en développant par rapport à la première ligne,

$$D = \begin{vmatrix} 0 & \cos c - & \cos b - 1 \\ \cos c - 1 & 0 & \cos a - 1 \\ \cos b - 1 & \cos a - 1 & 0 \end{vmatrix}$$

et en utilisant la règle de SARRUS, on obtient

$$D = 2(\cos a - 1)(\cos b - 1)(\cos c - 1) = -16 \sin^2 \frac{a}{2} \sin^2 \frac{b}{2} \sin^2 \frac{c}{2}.$$

7.8 Soit n un entier supérieur à 2 et

$$a = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}.$$

On désigne par X la matrice de $\mathcal{M}_n(\mathbf{C})$ de terme général

$$x_{pq} = a^{(p-1)(q-1)} \qquad (1 \leqslant p \leqslant n, \quad 1 \leqslant q \leqslant n).$$

a) Calculer X^2 et montrer que

$$\det X^2 = (-1)^{\frac{(n-1)(n-2)}{2}} n^n.$$

b) Soient $a_0, a_1, \ldots, a_{n-1}$ des nombres complexes ; considérons les matrices

$$M = \begin{pmatrix} a_0 & a_1 & a_2 & \ldots & a_{n-1} \\ a_1 & a_2 & a_3 & \ldots & a_0 \\ \vdots & & & & \\ a_{n-1} & a_0 & a_1 & & a_{n-2} \end{pmatrix} \qquad Y = MX \quad \text{et} \quad Z = XY$$

de $\mathcal{M}_n(\mathbf{C})$; on pose $M = (m_{pq})$, $Y = (y_{pq})$, $Z = (z_{pq})$ $(1 \leqslant p \leqslant n, 1 \leqslant q \leqslant n)$. Démontrer que

$$y_{pq} = a^{-(p-1)(q-1)} \sum_{k=0}^{n-1} a^{k(q-1)} a_k$$

$$z_{pq} = 0 \quad \text{si} \quad p \neq q \quad \text{et} \quad z_{pp} = n \sum_{k=0}^{n-1} a^{k(p-1)} a_k.$$

c) Calculer $\det Z$ et en déduire que

$$\det M = (-1)^{\frac{(n-1)(n-2)}{2}} \prod_{n=0}^{n-1} \left(\sum_{k=0}^{n-1} a^{kh} a_k \right).$$

Solution *a*) Le calcul de X^2 a été fait dans l'exercice 6.7 ; rappelons que

$$X^2 = \begin{pmatrix} n & 0 & 0 & \dots & 0 \\ 0 & 0 & & & n \\ 0 & & & & 0 \\ \vdots & & & & \vdots \\ 0 & n & 0 & \dots & 0 \end{pmatrix}$$

donc $\det X^2 = \varepsilon(\sigma)\, n^n$ où $\varepsilon(\sigma)$ est la signature de permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}$$

soit

$$\varepsilon(\sigma) = (-1)^{\frac{(n-1)(n-2)}{2}} \qquad \text{d'où} \qquad \det X^2 = (-1)^{\frac{(n-1)(n-2)}{2}} n^n .$$

b) Pour chaque entier m nous désignerons par $[m]$ l'unique entier tel que $[m] \equiv m \pmod n$ et $0 \leqslant [m] < n$. Avec cette notation on a

$$m_{pq} = a_{[p+q-2]} \qquad \text{si} \qquad 1 \leqslant p \leqslant n \qquad \text{et} \qquad 1 \leqslant q \leqslant n$$

d'autre part

$$y_{pq} = \sum_{i=1}^{p} m_{pi}\, x_{iq}$$

donc

$$y_{pq} = \sum_{i=1}^{n} a_{[p+i-2]}\, a^{(q-1)(i-1)}$$

soit

$$y_{pq} = a^{-(q-1)(p-1)} \sum_{i=1}^{n} a_{[p+i-2]}\, a^{(q-1)(i-1)+(q-1)(p-1)}$$

soit encore

$$y_{pq} = a^{-(q-1)(p-1)} \sum_{i=1}^{n} a_{[p+i-2]}\, a^{(q-1)(p+i-2)} .$$

Mais a^{p+i-2} ne dépend que de la classe modulo n de $p + i - 2$ donc

$$a^{p+i-2} = a^{[p+i-2]} ;$$

quand i décrit l'ensemble $\{1, 2, \dots, n\}$, $[p + i - 2]$ décrit l'ensemble $\{0, 1, \dots, n-1\}$ donc

$$y_{pq} = a^{-(q-1)(p-1)} \sum_{k=0}^{n-1} a_k\, a^{k(q-1)} \qquad (1 \leqslant p \leqslant n,\ 1 \leqslant q \leqslant n) .$$

Par ailleurs, nous avons

$$z_{pq} = \sum_{i=1}^{n} x_{pi}\, y_{iq}$$

soit

$$z_{pq} = \sum_{i=1}^{n} a^{(p-1)(i-1)}\, a^{-(q-1)(i-1)} \left[\sum_{k=0}^{n-1} a_k\, a^{k(q-1)}\right];$$

le terme entre crochets est indépendant de i, donc

$$z_{pq} = \left[\sum_{i=1}^{n} a^{(i-1)(p-q)}\right] \cdot \left[\sum_{k=0}^{n-1} a_k\, a^{k(q-1)}\right].$$

Si $p \neq q$,

$$\sum_{i=1}^{n} a^{(i-1)(p-q)} = \frac{a^{n(p-q)} - 1}{a^{p-q} - 1} = 0 \qquad \text{donc} \qquad z_{pq} = 0.$$

Si $p = q$,

$$\sum_{i=1}^{n} a^{(i-1)(p-q)} = n \qquad \text{donc} \qquad z_{pq} = n \sum_{k=0}^{n-1} a^{k(p-1)}\, a_k .$$

c) Nous venons de voir que Z est une matrice diagonale, donc

$$\det Z = \prod_{r=1}^{n} z_{rr}$$

soit

$$\det Z = \prod_{r=1}^{n} n\left(\sum_{k=0}^{n-1} a^{k(r-1)}\, a_k\right).$$

Mais $Z = XY = XMX$ donc $\det Z = \det X.\det M.\det X$ soit

$$\det Z = (\det X)^2.\det M\,,$$

d'où la relation

$$n^n \prod_{r=1}^{n} \left(\sum_{k=0}^{n-1} a_k\, a^{k(r-1)}\right) = (-1)^{\frac{(n-1)(n-2)}{2}}\, n^n \det M\,,$$

d'où

$$\det M = (-1)^{\frac{(n-1)(n-2)}{2}} \prod_{r=1}^{n} \left(\sum_{k=0}^{n-1} a_k\, a^{k(r-1)}\right)$$

et en posant $r = h + 1$, on obtient

$$\det M = (-1)^{\frac{(n-1)(n-2)}{2}} \prod_{h=0}^{n-1} \left(\sum_{k=0}^{n-1} a_k\, a^{kh}\right).$$

7.9 Soient p, q, n trois entiers naturels tels que $p + q = n$. Soit $\mathscr{S}_{p,q}$ l'ensemble des permutations σ de $\mathscr{S}_n$ telles que $\sigma(i)$ appartienne à l'ensemble $\{1, 2, ..., p\}$ pour tout $i = 1, 2, ..., p$.

Soit (s, t) un élément de $\mathscr{S}_p \times \mathscr{S}_q$; définissons la permutation $\theta(s, t) = \sigma$ par

$$\sigma(i) = s(i) \qquad \text{si} \qquad 1 \leqslant i \leqslant p$$

$$\sigma(j) = t(j - p) + p \qquad \text{si} \qquad p + 1 \leqslant j \leqslant p + q .$$

1) Démontrer que l'application θ ainsi définie est une bijection de $\mathscr{S}_p \times \mathscr{S}_q$ sur $\mathscr{S}_{p,q}$ et que $\varepsilon(\theta(s, t)) = \varepsilon(s)\,\varepsilon(t)$.

2) Soient A, A' deux matrices carrées à coefficients réels, d'ordres respectifs p et q, C une matrice à coefficients réels de type (p, q) et B la matrice carrée d'ordre $p + q = n$ à coefficients réels définie par

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

où 0 est la matrice nulle d'ordre (q, p). Posons

$$B = (b_i^j)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} .$$

Démontrer que

$$\det B = \sum_{\sigma \in \mathscr{S}_{p,q}} \varepsilon(\sigma)\, b_1^{\sigma(1)}\, b_2^{\sigma(2)} \ldots\ldots b_n^{\sigma(n)} ;$$

en déduire que $\det B = \det A . \det A'$.

Solution 1) Démontrons que l'application θ est surjective ; soit σ un élément de $\mathscr{S}_{p,q}$; puisque $\sigma(i)$ appartient à $\{1, 2, ..., p\}$ pour tout élément i de $\{1, 2, ..., p\}$, σ induit une bijection s de $\{1, 2, ..., p\}$ sur lui-même ; comme σ est une bijection, pour tout élément j de $\{p + 1, p + 2, ..., p + q\}$ $\sigma(j)$ appartient à $\{p + 1, ..., p + q\}$ donc σ induit une bijection t' de $\{p + 1, ..., p + q\}$ sur lui-même ; posons pour $k = 1, 2, ..., q$, $t(k) = t'(k + p) - p$; il est clair que t est alors une bijection de l'ensemble $\{1, 2, ..., q\}$ sur lui-même et que l'on a $\sigma = \theta(s, t)$ donc θ est une surjection. Démontrons maintenant que l'application θ est injective. Soient (s, t), (s', t') deux éléments de $\mathscr{S}_p \times \mathscr{S}_q$ tels que $\theta(s, t) = \theta(s', t')$; par définition de θ nous avons pour $i = 1, 2, ..., p$,

$$[\theta(s, t)]\,(i) = s(i) = s'(i) = [\theta(s', t')]\,(i) \quad \text{donc} \quad s = s' ,$$

pour $j = p + 1, p + 2, ..., p + q$,

$$[\theta(s, t)]\,(j) = t(j - p) + p = t'(j - p) + p = [\theta(s', t')]\,(j) ,$$

donc $t = t'$, par suite $(s, t) = (s', t')$ donc θ est bien injective donc bijective.

Soient (s, t) un élément de $\mathscr{S}_p \times \mathscr{S}_q$ et $\sigma = \theta(s, t)$; cherchons le nombre de couples (i, j) tels que $i < j$ et $\sigma(i) > \sigma(j)$. Si i appartient à $\{ 1, 2, ..., p \}$ et si j appartient à $\{ p + 1, ..., p + q \}$ on a $i < j$ et $\sigma(i) < \sigma(j)$ donc dans ce cas il ne peut y avoir d'inversion. Les inversions seront donc les couples (i, j) tels que i et j appartiennent ou bien à $\{ 1, 2, ..., p \}$ ou bien à $\{ p + 1, ..., p + q \}$ et tels que $\sigma(i) > \sigma(j)$ et $i < j$. Si i et j appartiennent à $\{ 1, 2, ..., p \}$, on a $\sigma(i) = s(i)$ et $\sigma(j) = s(j)$ donc le nombre de couples (i, j) tels que $i < j$ et $\sigma(i) > \sigma(j)$ est le nombre d'inversions de s. Si i' et j' appartiennent à $\{ p + 1, ..., p + q \}$ et $i' < j'$ nous aurons $\sigma(i') > \sigma(j')$ si et seulement si

$$t(i' - p) + p > t(j' - p) + p$$

soit $t(i' - p) > t(j' - p)$; si on pose $i = i' - p$, $j = j' - p$, alors nous aurons $i' < j'$ et $\sigma(i') > \sigma(j')$ si et seulement si $i < j$ et $t(i) > t(j)$ c'est-à-dire si et seulement si (i, j) est une inversion de t. Dans ce cas le nombre de couples (i', j') tels que $i' < j'$ et $\sigma(i') > \sigma(j')$, est le nombre d'inversions de t ; par suite le nombre d'inversions de σ est la somme des nombres d'inversions de s et t ; soient $i(\sigma)$, $i(s)$, $i(t)$ ces trois nombres ; alors

$$\varepsilon(\sigma) = (-1)^{i(\sigma)} = (-1)^{i(s)+i(t)} = (-1)^{i(s)} (-1)^{i(t)} = \varepsilon(s).\varepsilon(t) .$$

2) D'après la définition de la matrice B,

$$b_i^j = 0 \quad \text{si} \quad 1 \leqslant i \leqslant p \quad \text{et} \quad p + 1 \leqslant j \leqslant p + q ;$$

soit σ une permutation de $\mathscr{S}_n$ qui n'appartient pas à $\mathscr{S}_{p,q}$, alors il existe au moins un entier i tel que $1 \leqslant i \leqslant p$ et $p + 1 \leqslant \sigma(i) \leqslant p + q$ donc tel que $b_i^{\sigma(i)} = 0$, par suite si σ n'appartient pas à $\mathscr{S}_{p,q}$, le produit $b_1^{\sigma(1)} b_2^{\sigma(2)} ... b_n^{\sigma(n)}$ est nul, or

$$\det B = \sum_{\sigma \in \mathscr{S}_n} \varepsilon(\sigma)\, b_1^{\sigma(1)} b_2^{\sigma(2)} ..... b_n^{\sigma(n)}$$

donc

$$\det B = \sum_{\sigma \in \mathscr{S}_{p,q}} \varepsilon(\sigma)\, b_1^{\sigma(1)} b_2^{\sigma(2)} ..... b_n^{\sigma(n)} .$$

Si (s, t) est un élément de $\mathscr{S}_p \times \mathscr{S}_q$ et $\sigma = \theta(s, t)$ on a

$$\varepsilon(\sigma)\, b_1^{\sigma(1)} b_2^{\sigma(2)} ..... b_n^{\sigma(n)} = \varepsilon(s)\, \varepsilon(t)\, b_1^{s(1)} b_2^{s(2)} ..... b_p^{s(p)} b_{p+1}^{p+t(1)} ..... b_{p+q}^{p+t(q)}$$

et comme θ est une bijection de $\mathscr{S}_p \times \mathscr{S}_q$ sur $\mathscr{S}_{p.q}$ on a

$$\det B = \sum_{(s,t) \in \mathscr{S}_p \times \mathscr{S}_q} \varepsilon(s)\, \varepsilon(t)\, b_1^{s(1)} ..... b_p^{s(p)} . b_{p+1}^{p+t(1)} ..... b_{p+q}^{p+t(q)} =$$

$$= \sum_{s \in \mathscr{S}_p} \varepsilon(s)\, b_1^{s(1)} .... b_p^{s(p)} \sum_{t \in \mathscr{S}_q} \varepsilon(t)\, b_{p+1}^{p+t(1)} .... b_{p+q}^{p+t(q)} = \det A \det A' .$$

7.10 Soit a un nombre réel ; calculer l'inverse de la matrice

$$A = \begin{pmatrix} \cos a & -\sin a \\ \sin a & \cos a \end{pmatrix}.$$

Solution On a $\det A = \cos^2 a + \sin^2 a = 1$ donc A est inversible ; sa comatrice est

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

donc

$$A^{-1} = \begin{pmatrix} \cos a & \sin a \\ -\sin a & \cos a \end{pmatrix}.$$

7.11 Calculer les inverses des matrices suivantes de $\mathcal{M}_3(\mathbf{C})$,

$$A = \begin{pmatrix} -3 & 2 & -1 \\ 2 & 0 & 1 \\ -1 & 2 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

où

$$\omega = \cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}.$$

Solution Le déterminant de A est égal à -4 et sa comatrice est

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

donc

$$A^{-1} = -\tfrac{1}{4}\begin{pmatrix} -2 & -4 & 2 \\ -3 & -4 & 1 \\ 4 & 4 & -4 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 1 & -\frac{1}{2} \\ \frac{3}{4} & 1 & -\frac{1}{4} \\ -1 & -1 & 1 \end{pmatrix}.$$

Rappelons que $\det B = 3(\omega^2 - \omega)$ (*cf.* exercice 7.6) ; la comatrice de B est

$$\begin{pmatrix} \omega^2 - \omega & \omega^2 - \omega & \omega^2 - \omega \\ \omega^2 - \omega & \omega - 1 & 1 - \omega^2 \\ \omega^2 - \omega & 1 - \omega^2 & \omega - 1 \end{pmatrix}$$

en utilisant la relation $1 + \omega + \omega^2 = 0$ on trouve

$$B^{-1} = \frac{1}{3(\omega^2 - \omega)}\begin{pmatrix} \omega^2 - \omega & \omega^2 - \omega & \omega^2 - \omega \\ \omega^2 - \omega & \omega - 1 & 1 - \omega^2 \\ \omega^2 - \omega & 1 - \omega^2 & \omega - 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3\omega} & \frac{\omega}{3} \\ \frac{1}{3} & \frac{\omega}{3} & \frac{1}{3\omega} \end{pmatrix}.$$

7.12 Soient E un espace vectoriel de dimension finie sur un corps K et $E_1, E_2, \ldots, E_k$ des sous-espaces vectoriels de E tels que $E = E_1 \oplus E_2 \oplus \cdots \oplus E_k$. Nous poserons $d(i) = \dim_K E_i$ $(1 \leqslant i \leqslant k)$ et supposerons E rapporté à une base

$$B = \{ a_{1,1}, a_{1,2}, \ldots, a_{1,d(1)}, a_{2,1}, \ldots, a_{2,d(2)}, a_{3,1}, \ldots, a_{k,1}, \ldots, a_{k,d(k)} \}$$

telle que pour $i = 1, 2, \ldots, k$, $\{ a_{i,1}, a_{i,2}, \ldots, a_{i,d(i)} \}$ soit une base de E_i.

1) Soit f un endomorphisme de E tel que $f(E_i) \subset E_i$ pour $i = 1, 2, \ldots, k$; soit f_i l'application linéaire de E_i dans E_i $(1 \leqslant i \leqslant k)$ définie par $f_i(x) = f(x)$ pour tout élément x de E_i et soit A_i^i la matrice carrée d'ordre $d(i)$ représentant l'application f_i par rapport à la base $\{ a_{i,1}, a_{i,2}, \ldots, a_{i,d(i)} \}$ de E_i. Démontrer que la matrice A de f par rapport à la base B est

$$A = M(f, (a_{ij})) = \begin{pmatrix} A_1^1 & 0 & \cdots & 0 \\ 0 & A_2^2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & A_k^k \end{pmatrix}$$

2) Démontrer que f est un automorphisme de E si et seulement si pour tout $i = 1, 2, \ldots, k$, f_i est un automorphisme de E_i. En déduire que A est inversible si et seulement si toutes les matrices A_i^i $(1 \leqslant i \leqslant k)$ sont inversibles.

3) On suppose A inversible ; calculer A^{-1}.

Solution 1) Déterminons les colonnes de la matrice A ; soit $a_{l,n}$ un élément de la base $(a_{i,j})$; le vecteur $a_{l,n}$ appartient à E_l de même que $f(a_{l,n})$; la

$$(d(1) + d(2) + \cdots + d(l-1) + n)\text{-ième}$$

colonne de la matrice A est formée des composantes de $f(a_{l,n})$ sur la base $(a_{i,j})$; comme $f(a_{l,n})$ appartient à E_l, il existe des scalaires $\lambda_1, \lambda_2, \ldots, \lambda_{d(l)}$ tels que

$$f(a_{l,n}) = \sum_{i=1}^{d(l)} \lambda_i a_{l,i} ;$$

la $(d(1) + d(2) + \cdots + d(l-1) + n)$-ième colonne de la matrice A comprend donc de haut en bas, $(d(1) + d(2) + \cdots + d(l-1))$ zéros, puis $\lambda_1, \lambda_2, \ldots, \lambda_{d(l)}$, puis rien que des zéros. Comme $f(a_{l,n}) = f_l(a_{l,n})$ les scalaires $\lambda_1, \lambda_2, \ldots, \lambda_{d(l)}$ sont les composantes sur la base $a_{l,1}, a_{l,2}, \ldots, a_{l,d(l)}$ du vecteur $f_l(a_{l,n})$ de E_l, donc ils constituent la n-ième colonne de la matrice A_l^l, par suite la matrice A a bien la forme indiquée.

2) Supposons que f soit un automorphisme ; alors, pour chaque entier $i = 1, 2, ..., k$, f_i étant la restriction de f à E_i est un endomorphisme injectif de E_i qui est de dimension finie donc f_i est un automorphisme de E_i. Réciproquement supposons que toutes les applications f_i $(1 \leqslant i \leqslant k)$ soient des automorphismes. Soit x un élément de E tel que $f(x) = 0$ et soit

$$x = x_1 + x_2 + \cdots + x_k$$

la décomposition de x sur les sous-espaces $E_1, E_2, ..., E_k$. Nous avons

$$f(x) = f(x_1) + f(x_2) + \cdots + f(x_k) = f_1(x_1) + f_2(x_2) + \cdots + f_k(x_k) = 0 .$$

Or $f_i(x_i)$ étant un élément de E_i $(1 \leqslant i \leqslant k)$ et la somme des E_i étant directe, on a pour $i = 1, 2, ..., k$, $f_i(x_i) = 0$. Mais chacune des applications f_i $(1 \leqslant i \leqslant k)$ est injective donc $x_i = 0$ $(1 \leqslant i \leqslant k)$ par suite $x = 0$ et ceci prouve que f est injective. Comme E est de dimension finie f est alors un automorphisme de E (*cf.* Q., Ch. 7, § IV, n° 143, corollaire 2). Puisqu'un endomorphisme d'un espace vectoriel de dimension finie rapporté à une base, est un automorphisme si et seulement si la matrice qui le représente est inversible, il est clair que A est inversible si et seulement si toutes les matrices A_i^i $(1 \leqslant i \leqslant k)$ le sont.

3) Puisque A est inversible, f est inversible donc toutes les applications f_i $(1 \leqslant i \leqslant k)$ le sont ; la matrice de f_i^{-1} est $[A_i^i]^{-1}$ $(1 \leqslant i \leqslant k)$. Si x est un élément de E_i, alors $y = f_i^{-1}(x)$ appartient à E_i et on a

$$f(y) = f(f_i^{-1}(x)) = f_i(f_i^{-1}(x)) = x$$

donc $y = f^{-1}(x)$ et f^{-1} et f_i^{-1} coïncident sur E_i ; il résulte alors de la première question que A^{-1} qui est la matrice de f^{-1} par rapport à la base $(a_{i,j})$ est

$$A^{-1} = \begin{pmatrix} [A_1^1]^{-1} & 0 & \cdots & 0 \\ 0 & [A_2^2]^{-1} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & [A_k^k]^{-1} \end{pmatrix}$$

7.13 Soit K un corps commutatif. On considère la matrice A de $\mathcal{M}_n(K)$ définie par

$$A = (a_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}$$

et

$$\begin{cases} a_{ij} = 1 & \text{si} \quad j \leqslant i \\ a_{ij} = 0 & \text{si} \quad j > i . \end{cases}$$

Montrer que A est inversible et calculer A^{-1}. (On pourra considérer A comme la matrice d'un endomorphisme d'un espace vectoriel de dimension n sur K, rapporté à une base.)

Solution Soit E un espace vectoriel de dimension n sur K ; rapportons E à une base $\{ a_1, a_2, ..., a_n \}$ et soit f l'endomorphisme de E dont la matrice par rapport à la base $\{ a_1, ..., a_n \}$ est A. Comme la matrice A est triangulaire on a

$$\det A = a_{11}.a_{22}.....a_{nn} = 1$$

donc A est inversible (*cf.* Q., Ch. 9, § II, n^{os} 169 et 170), par suite f est un automorphisme, or on a

$$\begin{cases} f(a_1) = a_1 \\ f(a_2) = a_1 + a_2 \\ \vdots \\ f(a_n) = a_1 + a_2 + \cdots + a_n \end{cases}$$

donc

$$f^{-1}(a_1) = a_1 ,$$

$$f^{-1}(a_2) = f^{-1}(f(a_2) - a_1) = f^{-1}(f(a_2)) - f^{-1}(a_1) = a_2 - a_1 .$$

Soit p un entier tel que $2 \leqslant p < n$; supposons que pour $i = 2, 3, ..., p$ on ait $f^{-1}(a_i) = a_i - a_{i-1}$, alors on a $f(a_{p+1}) = a_1 + a_2 + \cdots + a_{p+1}$ donc

$$a_{p+1} = f^{-1}(a_1) + f^{-1}(a_2) + \cdots + f^{-1}(a_{p+1}) =$$
$$= a_1 + (a_2 - a_1) + \cdots + (a_p - a_{p-1}) + f^{-1}(a_{p+1}) = a_p + f^{-1}(a_{p+1})$$

d'où $f^{-1}(a_{p+1}) = a_{p+1} - a_p$; par suite, pour tout entier $q = 2, 3, ..., n$ on a $f^{-1}(a_q) = a_q - a_{q-1}$ et la matrice A^{-1} qui est la matrice de f^{-1} par rapport à la base $\{ a_1, ..., a_n \}$ est

$$A^{-1} = \begin{pmatrix} 1 & -1 & 0 & \cdots & 0 \\ 0 & 1 & -1 & & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & -1 \\ 0 & \cdots & & 0 & 1 \end{pmatrix}$$

7.14 Soit K un corps commutatif de caractéristique différente de deux.

1) Calculer le déterminant de la matrice A de $\mathcal{M}_n(K)$,

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

2) Dans le cas où le déterminant de A est non nul, calculer A^{-1}. Expliciter A^{-1} pour $n = 3$ et 5.

Solution 1) Développons le déterminant de A par rapport à la première colonne ; il vient

$$\det A = \begin{vmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{vmatrix} + (-1)^{n+1} \begin{vmatrix} 1 & 0 & & & 0 \\ 1 & 1 & \ddots & & \vdots \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 & 0 \\ 0 & \cdots & 0 & 1 & 1 \end{vmatrix}$$

Chacun des déterminants d'ordre $(n-1)$ figurant dans cette somme est le déterminant d'une matrice triangulaire donc est égal au produit de ses termes diagonaux c'est-à-dire à 1, on a donc $\det A = (1) + (-1)^{n+1}$. Il en résulte que $\det A = 2$ si n est impair et $\det A = 0$ si n est pair.

2) Supposons n impair. Soient E un espace vectoriel de dimension n sur K, $\{a_1, a_2, \ldots, a_n\}$ une base de E et f l'endomorphisme de E dont la matrice par rapport à la base $\{a_1, a_2, \ldots, a_n\}$ est A. Nous avons alors les relations

$$\begin{aligned} f(a_1) &= a_1 + a_n \quad \text{soit} \quad a_1 = f^{-1}(a_1) + f^{-1}(a_n) \\ f(a_2) &= a_1 + a_2 \quad \text{soit} \quad a_2 = f^{-1}(a_1) + f^{-1}(a_2) \\ &\vdots \\ f(a_i) &= a_{i-1} + a_i \quad \text{soit} \quad a_i = f^{-1}(a_{i-1}) + f^{-1}(a_i) \\ &\vdots \\ f(a_n) &= a_{n-1} + a_n \quad \text{soit} \quad a_n = f^{-1}(a_{n-1}) + f^{-1}(a_n). \end{aligned}$$

On en tire

$$\sum_{i=1}^{n} (-1)^{i+1} a_i = 2f^{-1}(a_n)$$

donc

$$f^{-1}(a_n) = \sum_{i=1}^{n} (-1)^{i+1} \frac{a_i}{2}$$

d'où

$$f^{-1}(a_1) = a_1 - f^{-1}(a_n) = a_1 - \sum_{i=1}^{n} (-1)^{i+1} \frac{a_i}{2}$$

soit

$$f^{-1}(a_1) = \frac{a_1}{2} - \sum_{i=2}^{n} (-1)^{i+1} \frac{a_i}{2}.$$

On a ensuite $f^{-1}(a_2) = a_2 - f^{-1}(a_1)$ soit

$$f^{-1}(a_2) = a_2 - \left(\frac{a_1}{2} - \sum_{i=2}^{n} (-1)^{i+1} \frac{a_i}{2}\right) = \frac{1}{2}\left[-a_1 + a_2 + \sum_{i=3}^{n} (-1)^{i+1} a_i\right].$$

Soit k un entier tel que $1 \leqslant k < n$; supposons que

$$f^{-1}(a_k) = \frac{(-)^{k+1}}{2}[a_1 - a_2 + \cdots + (-1)^{k+1} a_k] + \frac{1}{2}(-1)^k \sum_{i=k+1}^{n} (-1)^{i+1} a_i$$

alors

$$f^{-1}(a_{k+1}) = a_{k+1} - f^{-1}(a_k) = \frac{(-1)^{k+2}}{2}[a_1 - a_2 + \cdots + (-1)^{k+1} a_k] + \\ + a_{k+1} - \frac{a_{k+1}}{2} + \frac{(-1)^{k+1}}{2} \sum_{i=k+2}^{n} (-1)^{i+1} a_i$$

donc

$$f^{-1}(a_{k+1}) = (-1)^{k+2}[a_1 - a_2 + \cdots + (-1)^{k+2} a_{k+1}] + \\ + \frac{(-1)^{k+1}}{2} \sum_{i=k+2}^{n} (-1)^{i+1} a_i .$$

Par suite, on a pour tout entier $q = 1, 2, \ldots, n$

$$f^{-1}(a_q) = \frac{(-1)^{q+1}}{2}[a_1 - a_2 + \cdots + (-1)^{q+1} a_q] + \frac{(-1)^q}{2} \sum_{i=q+1}^{n} (-1)^{i+1} a_i$$

soit encore :

$$f^{-1}(a_q) = \frac{(-1)^q}{2}\left[\sum_{i=1}^{q} (-1)^i a_i + \sum_{i=q+1}^{n} (-1)^{i+1} a_i\right].$$

Les coefficients des vecteurs $\{a_1, \ldots, a_n\}$ dans la formule ci-dessus sont les éléments que la q-ième colonne ($1 \leqslant q \leqslant n$) de la matrice A^{-1}.

Application. Si $n = 3$ on a

$$A^{-1} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

et si $n = 5$ on a

$$A^{-1} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

7.15 1) Soient $K = \mathbf{Z}/2\,\mathbf{Z}$ le corps à deux éléments et A la matrice suivante de $\mathscr{M}_4(K)$

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

Déterminer le rang de A.

2) Même question pour la même matrice lorsque $K = \mathbf{Z}/3\,\mathbf{Z}$ et $K = \mathbf{Z}/5\,\mathbf{Z}$.

Solution 1) Calculons le déterminant de A

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

développons par rapport à la première ligne ; il vient

$$\det A = \begin{vmatrix} 2 & -1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & -1 \end{vmatrix} = -2 - 1 - (1 + 2) = -6 .$$

dans $\mathbf{Z}/2\,\mathbf{Z}$ on a donc $\det A = -6 = 0$ par suite il faut chercher les mineurs non nuls de ce déterminant ; or on a

$$\begin{vmatrix} 1 & -1 & 0 \\ 1 & 1 & -1 \\ 0 & 1 & 1 \end{vmatrix} = 1 - (-1 - 1) = 3 = 1$$

donc la matrice A de $\mathscr{M}_4(\mathbf{Z}/2\,\mathbf{Z})$ est de rang 3.

2) Si $K = \mathbf{Z}/3\,\mathbf{Z}$ on a d'après le calcul précédent, $\det A = -6 = 0$ donc on doit rechercher les mineurs non nuls du déterminant de A ; on a

$$\begin{vmatrix} 1 & -1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{vmatrix} = 1 + 1 - (-1 + 1) = 2$$

ce mineur étant nul non dans $\mathbf{Z}/3\,\mathbf{Z}$, la matrice A de $\mathscr{M}_4(\mathbf{Z}/3\,\mathbf{Z})$ est de rang 3.

Si $K = \mathbf{Z}/5\,\mathbf{Z}$ on a d'après le premier calcul $\det A = -6 = +4$ donc $\det A$ est non nul dans $\mathbf{Z}/5\,\mathbf{Z}$ et A est une matrice de rang 4 de $\mathscr{M}_4(\mathbf{Z}/5\,\mathbf{Z})$.

7.16 On considère la matrice suivante de $\mathscr{M}_3(\mathbf{R})$,

$$A = \begin{pmatrix} 13 & -8 & -12 \\ 12 & -7 & -12 \\ 6 & -4 & -5 \end{pmatrix}.$$

1) Montrer que cette matrice est inversible et calculer A^{-1}.

2) En déduire l'expression de A^n en fonction de A, pour tout entier rationnel n.

Solution 1) Calculons le déterminant de A.

$$\det A = \begin{vmatrix} 13 & -8 & -12 \\ 12 & -7 & -12 \\ 6 & -4 & -5 \end{vmatrix} = \begin{vmatrix} 1 & -1 & 0 \\ 12 & -7 & -12 \\ 6 & -4 & -5 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 12 & 5 & -12 \\ 6 & 2 & -5 \end{vmatrix}$$

d'où en développant suivant la première ligne,

$$\det A = -5 \times 5 + 2 \times 12 = -1 .$$

Comme det A n'est pas nul, A est inversible ; pour calculer A^{-1} commençons par calculer la comatrice de A,

$$\operatorname{com} A = \begin{pmatrix} -13 & -12 & -6 \\ 8 & 7 & 4 \\ 12 & -12 & 5 \end{pmatrix}$$

alors

$$A^{-1} = -{}^t\operatorname{com} A = \begin{pmatrix} 13 & -8 & -12 \\ 12 & -7 & 12 \\ 6 & -4 & -5 \end{pmatrix} = A$$

2) Comme $A = A^{-1}$ si n est un entier pair on a en posant $n = 2p$.

$$A^n = A^p . A^p = A^p . (A^{-1})^p = (A . A^{-1})^p = I_3^p = I_3$$

où I_3 désigne la matrice unité de $\mathcal{M}_3(\mathbf{R})$. Si n est un entier impair on a en posant $n = 2p + 1$, $A^n = A^{2p} . A$ or $A^{2p} = I_3$ donc $A^n = I_3 . A = A$.

7.17 Résoudre, dans le corps Q le système suivant

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

Solution Multiplions les deux membres de l'équation (1) par 2 et retranchons l'équation (2) ; on obtient $-3x - 4y + 3z = 1$, par conséquent l'équation (3) est une combinaison linéaire des deux premières, donc le système proposé est indéterminé et on doit résoudre le système

$$\begin{cases} x - y = 3 - z \\ 5x + 2y = 5 + z \end{cases}$$

où z est une inconnue non principale ; on trouve

$$x = \frac{1}{7}(11 - z) \qquad \text{et} \qquad y = \frac{1}{7}(-10 + 6z).$$

7.18 Résoudre dans le corps **Q** le système suivant

$$\begin{cases} 3x + 4y + z + 2t = 3 & (1) \\ 6x + 8y + 2z + 5t = 7 & (2) \\ 9x + 12y + 3z + 10t = 13. & (3) \end{cases}$$

Solution La matrice des coefficients de ce système, soit

$$\begin{pmatrix} 3 & 4 & 1 & 2 \\ 6 & 8 & 2 & 5 \\ 9 & 12 & 3 & 10 \end{pmatrix}$$

est de rang 2 car tous les mineurs d'ordre 3 sont nuls et par exemple $\begin{vmatrix} 1 & 2 \\ 2 & 5 \end{vmatrix}$ est un mineur non nul. Il y a donc deux équations principales (les équations (1) et (2)) et deux inconnues principales (z et t), par conséquent on doit résoudre le système

$$\begin{cases} z + 2t = 3 - 3x - 4y \\ 2z + 5t = 7 - 6x - 8y \end{cases}$$

on obtient $t = 1$ et $z = 1 - 3x - 4y$.

Vérifions que x, y, z, t ainsi définis vérifient bien l'équation (3) :

$$9x + 12y + 3(1 - 3x - 4y) + 10 = 13 \qquad (3)$$

ce qui est vérifié.

La solution du système est donc : x, y quelconques, $z = 1 - 3x - 4y$ et $t = 1$.

7.19 Résoudre dans le corps **Q**, le système suivant

$$\begin{cases} 2x + y + z + t = 3 & (1) \\ x + 2y + z + t = 1 & (2) \\ x + y + 2z + t = 2 & (3) \\ x + y + z + 2t = 4 & (4) \\ x - y + z - t = 0. & (5) \end{cases}$$

Solution Ajoutons membre à membre les quatre premières équations ; nous trouvons $5x + 5y + 5z + 5t = 10$ donc $x + y + z + t = 2$. En retranchant cette égalité successivement des équations (1), (2), (3), (4) on obtient

$$x = 1\,, \quad y = -1\,, \quad z = 0\,, \quad t = 2\,.$$

Comme ces nombres vérifient l'équation (5), le système admet la solution

$$x = 1\,, \quad y = -1\,, \quad z = 0\,, \quad t = 2\,.$$

7.20 Résoudre dans le corps **R** et discuter suivant les valeurs du paramètre réel m, le système suivant

$$\begin{cases} x + y + z = m + 1 & (1) \\ mx + y + (m-1)z = m & (2) \\ x + my + z = 1\,. & (3) \end{cases}$$

Solution Le déterminant du système est

$$D = \begin{vmatrix} 1 & 1 & 1 \\ m & 1 & m-1 \\ 1 & m & 1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ m & 1-m & -1 \\ 1 & m-1 & 0 \end{vmatrix} = \begin{vmatrix} 1-m & -1 \\ m-1 & 0 \end{vmatrix} = m - 1$$

a) Si $m \neq 1$, le système est un système de CRAMER et admet la solution unique suivante

$$x = \frac{\begin{vmatrix} m+1 & 1 & 1 \\ m & 1 & m-1 \\ 1 & m & 1 \end{vmatrix}}{m-1} \qquad y = \frac{\begin{vmatrix} 1 & m+1 & 1 \\ m & m & m-1 \\ 1 & 1 & 1 \end{vmatrix}}{m-1}$$

$$z = \frac{\begin{vmatrix} 1 & 1 & m+1 \\ m & 1 & m \\ 1 & m & 1 \end{vmatrix}}{m-1}$$

soit :

$$x = \frac{-m^3 + m^2 + 2m - 1}{m-1}\,, \quad y = \frac{-m}{m-1}\,, \quad z = \frac{m^3 - m}{m-1} = m(m+1)\,.$$

b) Si $m = 1$ le système devient

$$\begin{cases} x + y + z = 2 \\ x + y \quad\;\; = 1 \\ x + y + z = 1 \end{cases}$$

il est donc impossible.

7.21 Résoudre dans le corps **R**, et discuter suivant les valeurs des paramètres réels a, b, c, d le système suivant

$$\begin{cases} x + \quad y + \quad z = 1 \\ ax + \; by + \; cz = d \\ a^2 x + b^2 y + c^2 z = d^2 . \end{cases}$$

Solution Calculons le déterminant du système

$$D = \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ a & b-a & c-a \\ a^2 & b^2-a^2 & c^2-a^2 \end{vmatrix} = \begin{vmatrix} b-a & c-a \\ b^2-a^2 & c^2-a^2 \end{vmatrix}$$

d'où $D = (b - a)(c - a)(c - b)$.

Si $a \neq b$, $b \neq c$ et $c \neq a$, le système est de CRAMER et admet la solution unique suivante

$$x = \frac{\begin{vmatrix} 1 & 1 & 1 \\ d & b & c \\ d^2 & b^2 & c^2 \end{vmatrix}}{(b-c)(c-a)(a-b)}, \quad y = \frac{\begin{vmatrix} 1 & 1 & 1 \\ a & d & c \\ a^2 & d^2 & c^2 \end{vmatrix}}{(b-c)(c-a)(a-b)},$$

$$z = \frac{\begin{vmatrix} 1 & 1 & 1 \\ a & b & d \\ a^2 & b^2 & d^2 \end{vmatrix}}{(b-c)(c-a)(a-b)}$$

soit

$$x = \frac{(c-d)(d-b)}{(c-a)(a-b)}, \quad y = \frac{(d-c)(a-d)}{(b-c)(a-b)}, \quad z = \frac{(b-d)(d-a)}{(b-c)(c-a)}.$$

Si $a = b$, posons $x + y = t$; le système devient

$$\begin{cases} t + z = 1 \\ at + cz = d \\ a^2 t + c^2 z = d^2 . \end{cases}$$

Si $a \neq c$, il est de rang 2 et il admet une solution unique si et seulement si son déterminant caractéristique est nul soit

$$\begin{vmatrix} 1 & 1 & 1 \\ a & c & d \\ a^2 & c^2 & d^2 \end{vmatrix} = (c - a)(d - a)(d - c) = 0 .$$

Comme $c \neq a$, il y a une solution si et seulement si $d = a$ ou $d = c$.

Si $d = a$, le système devient

$$\begin{cases} t + z = 1 \\ at + cz = a \\ a^2 t + c^2 z = a^2 \end{cases}$$

d'où l'on tire $z = 0$ et $t = 1$.

Si $d = c$, le système devient

$$\begin{cases} t + z = 1 \\ at + dz = d \\ a^2 t + d^2 z = d^2 \end{cases}$$

et admet la solution $t = 0$, $z = 1$.

Si $a = c$ le système devient

$$\begin{cases} t + z = 1 \\ a(t + z) = d \\ a^2(t + z) = d^2 . \end{cases}$$

Si $a = d$ il admet la solution $z = 1 - t = 1 - x - y$.

Si $a \neq d$ le système est impossible.

Dans le cas où le système n'est pas un système de CRAMER, les résultats que nous avons obtenus se résument dans le tableau suivant

$$a = b \begin{cases} c \neq a \begin{cases} d \neq a \text{ et } d \neq c, & \text{système impossible} \\ d = a, & \text{système indéterminé } (z = 1, x = 1 - y) \\ d \neq a \text{ et } d = c, & \text{système indéterminé } (z = 1 \text{ et } y = -x) \end{cases} \\ c = a \begin{cases} a \neq d, & \text{système impossible} \\ a = d, & \text{système indéterminé } (z = 1 - x - y) . \end{cases} \end{cases}$$

On a des discussions analogues pour les cas $b = c$ et $a = c$.

7.22 Soient K un corps commutatif de caractéristique p et $a_1, a_2, \ldots, a_n, s$ des éléments de K. Résoudre et discuter dans K le système suivant

$$\begin{cases} x_0 + x_1 = a_1 \\ x_0 + x_2 = a_2 \\ \cdots\cdots\cdots\cdots \\ x_0 + x_n = a_n \\ x_0 + x_1 + x_2 + \cdots + x_n = s\,. \end{cases}$$

Solution Additionnons membre à membre les n premières équations ; nous obtenons

$$nx_0 + x_1 + x_2 + \cdots + x_n = a_1 + a_2 + \cdots + a_n\,,$$

soit

$$(n-1)\,x_0 + (x_0 + x_1 + \cdots + x_n) = a_1 + a_2 + \cdots + a_n$$

et en tenant compte de la dernière équation

$$(n-1)\,x_0 = a_1 + a_2 + \cdots + a_n - s\,.$$

Supposons que $(n-1)$ soit un multiple de p ; alors :

— si $a_1 + a_2 + \cdots + a_n = s$, x_0 est arbitraire et on a $x_i = a_i - x_0$ pour $i = 1, 2, \ldots, n$;

— si $a_1 + a_2 + \cdots + a_n \neq s$, le système est impossible.

Supposons maintenant que $(n-1)$ ne soit pas un multiple de p ; alors $(n-1)$ est inversible dans K et

$$x_0 = \frac{a_1 + a_2 + \cdots + a_n - s}{n-1}\,,$$

d'où l'on déduit

$$x_i = \frac{a_1 + a_2 + \cdots + a_{i-1} + na_i + a_{i+1} + \cdots + a_n - s}{n-1} \text{ pour } i = 1, 2, \ldots, n\,.$$

7.23 Soient a, b, c, d quatre nombres réels strictement positifs. Démontrer que le système suivant ne possède aucune solution dans R.

$$\begin{cases} x + y + z + t = a \\ x - y - z + t = b \\ -x - y + z + t = c \\ -3x + y - 3z - 7t = d\,. \end{cases}$$

Solution Calculons le déterminant de ce système

$$D = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -3 & 1 & -3 & -7 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & -2 & -2 & 0 \\ -1 & 0 & 2 & 2 \\ -3 & 4 & 0 & -4 \end{vmatrix}$$

$$= \begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 \\ -1 & 0 & 2 & 2 \\ 3 & 4 & -4 & -4 \end{vmatrix}.$$

Ce déterminant a deux colonnes égales, il est donc nul. Cherchons un mineur non nul ; on a

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

Donc le système est de rang 3. Prenons t comme inconnue non principale et résolvons le système

$$\begin{cases} x + y + z = a - t & (1) \\ x - y - z = b - t & (2) \\ -x - y + z = c - t. & (3) \end{cases}$$

En ajoutant membre à membre les équations (1) et (2) nous trouvons

$$2x = a + b - 2t \quad \text{soit} \quad x = \frac{a + b - 2t}{2} = \frac{a + b}{2} - t.$$

En ajoutant membre à membre les équations (2) et (3) nous trouvons

$$-2y = c + b - 2t \quad \text{soit} \quad y = \frac{-b - c + 2t}{2} = t - \frac{b + c}{2}.$$

En ajoutant membre à membre les équations (1) et (3) nous trouvons

$$2z = a + c - 2t \quad \text{soit} \quad z = \frac{a + c - 2t}{2} = \frac{a + c}{2} - t.$$

Remplaçons x, y, z par les valeurs que nous venons de trouver, dans la dernière équation du système proposé ; on obtient

$$-3\left(\frac{a + b}{2} - t\right) + \left(t - \frac{b + c}{2}\right) - 3\left(\frac{a + c}{2} - t\right) - 7t = d$$

soit $-(3a + 2b + 2c) = d$. Comme a, b, c, d sont des nombres réels strictement positifs il est impossible que $d = -(3a + 2b + 2c)$, donc le système proposé est impossible.

8

POLYNÔMES ET FRACTIONS RATIONNELLES

8.1 Dans $K[X]$ on considère les polynômes suivants

$$f(X) = X^2 + 2X + 3\,,\, g(X) = 2X^2 + 3X + 1\,,\, h(X) = 3X^2 + X + 2.$$

Calculer $P = f^3 + g^3 + h^3 - 3fgh$.

a) pour $K = \mathbf{Z}$,

b) pour $K = \mathbf{Z}/3\,\mathbf{Z}$.

Solution L'expression d'un polynôme symétrique en fonction des polynômes symétriques élémentaires (*cf.* Q., Ch. 11, § III, n° 199) permet d'écrire

$$f^3 + g^3 + h^3 = (f + g + h)^3 - 3(f + g + h)(fg + gh + hf) + 3fgh\,.$$

Le polynôme P à calculer est donc

$$P = (f + g + h)^3 - 3(f + g + h)(fg + gh + hf)$$

soit encore

$$P = (f + g + h)\left[(f + g + h)^2 - 3(fg + gh + hf)\right]$$

a) $K = \mathbf{Z}$. On a

$$f(X) + g(X) + h(X) = 6(X^2 + X + 1)$$
$$f(X).g(X) = 2X^4 + 7X^3 + 13X^2 + 11X + 3$$
$$g(X).h(X) = 6X^4 + 11X^3 + 10X^2 + 7X + 2$$
$$h(X).f(X) = 3X^4 + 7X^3 + 13X^2 + 7X + 6$$

donc

$$(fg + gh + hf)(X) = 11X^4 + 25X^3 + 36X^2 + 25X + 11$$

par ailleurs

$$(f + g + h)^2(X) = 36[X^4 + 2X^3 + 3X^2 + 2X + 1]$$

donc

$$P(X) = 6[X^2 + X + 1][36[X^4 + 2X^3 + 3X^2 + 2X + 1] - 33X^4 - 75X^3 - 108X^2 - 75X - 33]$$

soit

$$P(X) = 6[X^2 + X + 1][3X^4 - 3X^3 - 3X + 3] = 18[X^6 - 2X^3 + 1] = 18[X^3 + 1]^2.$$

b) $K = \mathbf{Z}/3\,\mathbf{Z}$. 18 est multiple de 3 donc $P = 0$ dans $\mathbf{Z}/3\,\mathbf{Z}$.

8.2

Dans $\mathbf{C}[X]$ on considère les polynômes

$$f(X) = aX^2 + bX + c, \quad \varphi(X) = \alpha X^2 + \beta X + \gamma.$$

Peut-on trouver des nombres complexes $a, b, c, \alpha, \beta, \gamma$ tels que $f[\varphi] = \varphi[f]$.

Solution On a

$$\varphi^2(X) = \alpha^2 X^4 + 2\alpha\beta X^3 + (\beta^2 + 2\alpha\gamma)X^2 + 2\beta\gamma X + \gamma^2,$$

donc

$$f[\varphi](X) = f[\varphi(X)] = a\varphi^2(X) + b\varphi(X) + c$$

soit

$$f[\varphi](X) = a\alpha^2 X^4 + 2a\alpha\beta X^3 + (a\beta^2 + 2a\alpha\beta + b\alpha)X^2 + (2a\beta\gamma + \beta b)X + a\gamma^2 + b\gamma + c.$$

Pour obtenir $\varphi[f](X)$ il suffit d'intervertir les rôles joués par (a, b, c) et (α, β, γ) ; les deux polynômes $f[\varphi]$ et $\varphi[f]$ sont égaux si et seulement si tous leurs coefficients sont égaux ; $a, b, c, \alpha, \beta, \gamma$ doivent alors vérifier les égalités :

$$\begin{cases} a\alpha^2 = \alpha a^2 \\ 2a\alpha\beta = 2\alpha ab \\ a\beta^2 + 2a\alpha\beta + b\alpha = \alpha b^2 + 2\alpha ab + \beta a \\ 2a\beta\gamma + \beta b = 2\alpha bc + \beta b \\ a\gamma^2 + b\gamma + c = \alpha c^2 + \beta c + \gamma. \end{cases}$$

1er *cas.* a et α sont non nuls.

Le système précédent se ramène à $a = \alpha$, $b = \beta$, $c = \gamma$ c'est-à-dire que $f[\varphi] = \varphi[f]$ si et seulement si $f = \varphi$.

2e *cas.* a et α sont nuls.

b, c, β, γ doivent alors vérifier la condition

$$b\gamma + c = \beta c + \gamma.$$

3e *cas.* a est nul, α est non nul.

Le système se ramène à

$$\begin{cases} b = b^2 \\ 2\alpha bc = 0 \\ b\gamma + c = \alpha c^2 + \beta c + \gamma\,. \end{cases}$$

Si $b = 0$ (c, α, β, γ) doivent vérifier la condition $c = \alpha c^2 + \beta c + \gamma$, autrement dit c doit être racine de l'équation $\alpha X^2 + (\beta - 1)X + \gamma = 0$. Si $b \neq 0$, alors nécessairement $b = 1$ et $\alpha c = 0$, $c = \alpha c^2 + \beta c$. Comme α est non nul on a $c = 0$ et $\varphi[f] = f[\varphi]$ quels que soient α, β, γ, avec $\alpha \neq 0$.

4e *cas.* a est non nul, α est nul.

Ce cas se déduit du précédent en intervertissant les rôles joués par les lettres grecques et latines.

Dans les cas 2, 3, 4 le problème admet donc des solutions autres que la solution triviale $f = \varphi$.

8.3 Effectuer dans $\mathbf{R}[X]$ les divisions euclidiennes de

a) $X^n \sin\varphi - X\sin\varphi + \sin(n-1)\varphi$.

b) $X^{n+1}\cos(n-1)\varphi - X^n\cos n\varphi - X\cos\varphi + 1$ par $X^2 - 2X\cos\varphi + 1$.

Dans les deux cas on trouve que le reste est nul. Peut-on démontrer plus rapidement ce résultat en se plaçant dans $\mathbf{C}[X]$.

Solution *a*) Effectuons la division euclidienne du polynôme

$$f(X) = X^n \sin\varphi - X\sin n\varphi + \sin(n-1)\varphi\,,$$

par le polynôme $g(X) = X^2 - 2X\cos\varphi + 1$, dans $\mathbf{R}[X]$.

Le quotient du monôme dominant de f par le monôme dominant de g est $m_0 = X^{n-2}\sin\varphi$ (*cf.* Q. Ch. 11, § II, n° 189) ; posons $f_1 = f - m_0.g$, alors

$$f_1(X) = X^{n-1}\sin 2\varphi - X^{n-2}\sin\varphi - X\sin n\varphi + \sin(n-1)\varphi\,;$$

le quotient du monôme dominant de f_1 par le monôme dominant de g est $m_1 = X^{n-3} \sin 2\varphi$; posons $f_2 = f_1 - m_1 g$, alors

$$f_2(X) = X^{n-2} \sin 3\varphi - X^{n-3} \sin 2\varphi - X \sin n\varphi + \sin (n-1)\varphi .$$

Nous pouvons recommencer h fois ($1 \leqslant h \leqslant n-2$). Supposons que par ce procédé on ait trouvé $m_{h-1} = X^{n-h-1} \sin h\varphi$ et

$$f_h(X) = X^{n-h} \sin (h+1)\varphi - X^{n-h-1} \sin h\varphi - X \sin n\varphi + \sin (n-1)\varphi$$

alors m_h quotient du monôme dominant de f_h par g est $m_h = X^{n-h-2} \sin (h+1)\varphi$ et on a en posant $f_{h+1} = f_h - m_h g$,

$$f_{h+1}(X) = X^{n-h-1} \sin (h+2)\varphi - X^{n-h-2} \sin (h+1)\varphi - X \sin n\varphi + \sin (n-1)\varphi .$$

En recommençant $(n-2)$ fois l'opération on obtiendra donc

$$f_{n-2}(X) = X^2 \sin (n-1)\varphi - X \sin (n-2)\varphi - X \sin n\varphi + \sin (n-1)\varphi,$$

soit

$$f_{n-2}(X) = \sin (n-1)\varphi [X^2 - 2X \cos \varphi + 1] = \sin (n-1)\varphi . g(X) ;$$

par suite le quotient de f par g est

$$q = m_0 + m_1 + \cdots + m_{n-3} + \sin (n-1)\varphi$$

soit

$$q(X) = X^{n-2} \sin \varphi + X^{n-3} \sin 2\varphi + \cdots + X \sin (n-2)\varphi + \sin (n-1)\varphi ,$$

et le reste est nul.

Si nous nous plaçons dans $\mathbf{C}[X]$, le polynôme g s'écrit

$$g(X) = (X - e^{i\varphi})(X - e^{-i\varphi}),$$

or

$$f(e^{i\varphi}) = e^{in\varphi} \sin \varphi - e^{i\varphi} \sin n\varphi + \sin (n-1)\varphi$$

soit

$$f(e^{i\varphi}) = \cos n\varphi \sin \varphi - \cos \varphi \sin n\varphi + \sin (n-1)\varphi + i[\sin n\varphi \sin \varphi - \sin \varphi \sin n\varphi]$$

par suite $f(e^{i\varphi}) = 0$; de même on a $f(e^{-i\varphi}) = 0$ donc g divise f.

b) En effectuant la division euclidienne dans $\mathbf{R}[X]$ de

$$h(X) = X^{n+1} \cos (n-1)\varphi - X^n \cos n\varphi - X \cos \varphi + 1$$

par $g(X) = X^2 - 2X \cos \varphi + 1$ on trouve le quotient

$$q(X) = X^{n-1} \cos (n-1)\varphi + X^{n-2} \cos (n-2)\varphi + \cdots + 1$$

et le reste nul.

D'autre part, en se plaçant dans $\mathbf{C}[X]$ on vérifie que $h(e^{i\varphi}) = h(e^{-i\varphi}) = 0$ et comme $g(X) = (X - e^{i\varphi})(X - e^{-i\varphi})$, g divise h.

8.4 Démontrer que les deux polynômes $X^2 + 1$ et $2X$ de $\mathbf{Z}[X]$ sont premiers entre eux. En déduire que l'anneau $\mathbf{Z}[X]$ n'est pas principal. Que peut-on dire dans $\mathbf{Z}[X]$ de l'idéal engendré par $(X^2 + 1)$ et X ?

Solution Dans $\mathbf{Z}[X]$ les diviseurs de $2X$ sont 1, 2, X, $2X$ et leurs opposés ; or 2, X et par suite $2X$ ne divisent pas $X^2 + 1$, donc $X^2 + 1$ et $2X$ sont premiers entre eux dans $\mathbf{Z}[X]$. Supposons que $\mathbf{Z}[X]$ soit principal ; alors, l'idéal I engendré par $X^2 + 1$ et $2X$ est principal ; il est engendré par un de ses éléments qui ne peut être que 1 car 1 est le seul diviseur commun à $X^2 + 1$ et $2X$, or 1 ne peut appartenir à I ; en effet, les polynômes de I sont de la forme

$$(X^2 + 1)A + (2X)B,$$

A et B étant deux polynômes de $\mathbf{Z}[X]$. $\mathbf{Z}[X]$ est un sous-anneau de $\mathbf{R}[X]$. Cherchons les polynômes A et B de $\mathbf{R}[X]$ tels que $(X^2 + 1)A + (2X)B = 1$; d'après le théorème de BEZOUT (*cf.* Q., Ch. 11, § II, n° 190) les polynômes A et B de degré minimum vérifiant ces identités sont $A_0 = 1$, $B_0 = -\frac{X}{2}$ et tous les autres sont de la forme $A = 1 + (2X)Q$ et $B = -\frac{X}{2} - (X^2 + 1)Q$ où Q est un polynôme de $\mathbf{R}[X]$. Or aucun polynôme B ne peut appartenir à $\mathbf{Z}[X]$ par suite 1 ne peut appartenir à I ; $\mathbf{Z}[X]$ n'est donc pas principal.

Par contre $(X^2 + 1) - X(X) = 1$ donc 1 appartient à l'idéal J de $\mathbf{Z}[X]$ engendré par $X^2 + 1$ et X, donc $J = \mathbf{Z}[X]$.

8.5 Dans l'anneau $\mathbf{Z}[X]$ démontrer que l'idéal engendré par $(X^2 + 1)$ est premier et non maximal.

Solution Soit I l'idéal engendré par $X^2 + 1$ dans $\mathbf{Z}[X]$. Soient P et Q deux polynômes de $\mathbf{Z}[X]$ dont le produit $P.Q$ appartient à I ; alors $X^2 + 1$ divise $P.Q$ et $X^2 + 1$ n'admet pas de diviseur autre que les constantes et lui-même ; donc $X^2 + 1$ divise soit P, soit Q et par suite P ou Q appartient à I. I est donc un idéal premier ; or il n'est pas maximal ; en effet l'idéal engendré par $X^2 + 1$ et $2X$ est strictement contenu dans $\mathbf{Z}[X]$ (*cf.* exercice 8.4) et contient I.

8.6 Calculer dans $\mathbf{R}[X]$ le p. g. c. d.

1) de $X^4 + X^3 - 3X^2 - 4X - 1$ et de $X^3 + X^2 - X - 1$,

2) des polynômes f, g, h avec

$$f(X) = 2X^6 - 5X^5 - 14X^4 + 36X^3 + 86X^2 + 12X - 31$$
$$g(X) = 2X^5 - 9X^4 + 2X^3 + 37X^2 + 10X - 14$$
$$h(X) = X^3 - 2X - 1\,.$$

Solution 1) Remarquons que

$$X^3 + X^2 - X - 1 = (X + 1)(X^2 - 1) = (X - 1)(X + 1)^2\,.$$

Posons $P(X) = X^4 + X^3 - 3X^2 - 4X - 1$. Alors 1 n'est pas racine de $P(X)$ et -1 est racine de $P(X)$; on a $P'(X) = 4X^3 + 3X^2 - 6X - 4$, donc -1 n'est pas racine de $P'(X)$; par suite, -1 est racine simple de $P(X)$. Le p. g. c. d. de $P(X)$ et de $X^3 + X^2 - X - 1$ est donc $(X + 1)$.

2) Observons que -1 est racine de $f(X)$, $g(X)$ et $h(X)$ et que

$$h(X) = (X + 1)(X^2 - X - 1)$$

et

$$g(X) = (X + 1)(2X^4 - 11X^3 + 13X^2 + 24X - 14)\,.$$

Calculons le p. g. c. d. de $X^2 - X - 1$ et de

$$2X^4 - 11X^3 + 13X^2 + 24X - 14\,;$$

l'algorithme d'EUCLIDE (*cf.* Q., Ch. 11, § II, n° 190) fournit les résultats suivants:

	$2X^2 - 9X + 6$	$\frac{X}{21} - \frac{13}{441}$	$-\frac{9\,261}{545}X + \frac{3\,528}{545}$
$2X^4 - 11X^3 + 13X^2 + 24X - 14$	$X^2 - X - 1$	$21X - 8$	$-\frac{545}{441}$
$21X - 8$	$-\frac{545}{441}$	0	

par suite $2X^4 - 11X^3 + 13X^2 + 24X - 14$ et $X^2 - X - 1$ sont premiers entre eux, donc $(X + 1)$ est le p. g. c. d. de f, g et h.

8.7 Soient a un nombre réel et m, n deux entiers naturels. Calculer dans $\mathbf{R}[X]$ le p. g. c. d. de $X^n - a^n$ et de $X^m - a^m$.

Solution Supposons a non nul (sinon le problème serait trivial) et $n > m$. Comme

$$X^n - a^n = a^n\left[\left(\frac{X}{a}\right)^n - 1\right] \quad \text{et} \quad X^m - a^m = a^m\left[\left(\frac{X}{a}\right)^m - 1\right]$$

nous sommes ramenés à calculer le p. g c. d. de $(Z^n - 1)$ et de $(Z^m - 1)$. Effectuons la division euclidienne de $(Z^n - 1)$ par $(Z^m - 1)$. Pour cela nous sommes conduits à diviser n par m. Soient q_1 et r_1 le quotient et le reste de cette division. On vérifie aisément que

$$Z^n - 1 = (Z^m - 1)(Z^{n-m} + Z^{n-2m} + \cdots + Z^{n-q_1 m}) + (Z^{r_1} - 1).$$

Le reste de la division de $(Z^n - 1)$ par $(Z^m - 1)$ est donc $(Z^{r_1} - 1)$, par suite le p. g. c. d. de $(Z^n - 1)$ et $(Z^m - 1)$ est celui de $(Z^m - 1)$ et $(Z^{r_1} - 1)$.

Ecrivons l'algorithme d'EUCLIDE pour la recherche du p. g. c. d. de n et m,

	q_1	q_2	.....	q_{p-1}	q_p
n	m	r_1	.....	r_{p-2}	r_{p-1}
r_1	r_2	r_3	.....	r_p	

r_p étant le dernier reste non nul de cette suite de divisions, c'est-à-dire le p. g. c. d. de m et n. En recommençant p fois le raisonnement précédent, nous voyons que le p. g. c. d. de $(Z^n - 1)$ et de $(Z^m - 1)$ est celui de $(Z^{r_{p-1}} - 1)$ et de $(Z^{r_p} - 1)$ c'est-à-dire $(Z^{r_p} - 1)$ car r_{p-1} est un multiple de r_p.

En conclusion, le p. g. c. d. de $(X^n - a^n)$ et de $(X^m - a^m)$ est $(X^r - a^r)$ où r désigne le p. g. c. d de m et n. En particulier si m et n sont premiers entre eux, le p. g. c. d. de $(X^n - a^n)$ et de $(X^m - a^m)$ est $(X - a)$.

8.8 Trouver le p. g. c. d. des deux polynômes $3X^3 + X + 1$ et $3X^2 + 2X - 1$

a) dans $\mathbf{Q}[X]$,

b) dans $\mathbf{Z}/3\,\mathbf{Z}[X]$,

c) dans $\mathbf{Z}[X]$.

Solution *a*) En remarquant que -1 est racine de $3X^2 + 2X - 1$ on décompose aisément ce polynôme

$$3X^2 + 2X - 1 = (X + 1)(3X - 1).$$

Or -1 et $\frac{1}{3}$ ne sont pas racines de $3X^3 + X + 1$, donc $3X^3 + X + 1$ et $3X^2 + 2X - 1$ sont premiers entre eux dans $\mathbf{Q}[X]$ et n'ont d'autres diviseurs communs que les éléments de $\mathbf{Q}$.

b) Dans $\mathbf{Z}/3\,\mathbf{Z}[X]$, $3X^3 + 2X + 1 = 2X + 1$ et

$$3X^2 + 2X - 1 = 2X - 1,$$

d'autre part $(X + 1) + (2X - 1) = 3X = 0$ donc $(X + 1) = -(2X - 1)$ et $(X + 1)$ est le p. g. c. d. des deux polynômes proposés.

c) Dans $\mathbf{Z}[X]$ les deux polynômes considérés n'ont d'autres diviseurs que les éléments de $\mathbf{Z}$ (car $\mathbf{Z}[X]$ est un sous-anneau de $\mathbf{Q}[X]$) ; par suite ces polynômes sont premiers entre eux.

8.9 Trouver tous les polynômes f de $\mathbf{R}[X]$ tels que $f(X) + 1$ soit divisible par $(X - 1)^4$ et $f(X) - 1$ par $(X + 1)^4$:

a) en utilisant la relation de BEZOUT,

b) en considérant le polynôme dérivé de f.

On montrera qu'il existe un polynôme f_0 et un seul, répondant à la question, qui soit de degré inférieur à 7.

Solution *a*) La recherche du polynôme f est un problème équivalent à celui de la recherche de deux polynômes U et V définis par $f(X) + 1 = (X - 1)^4 . U(X)$ et $f(X) - 1 = (X + 1)^4 . V(X)$ et donc liés par la relation

$$2 = (X - 1)^4 . U(X) - (X + 1)^4 . V(X),$$

dite relation (α). Comme $(X + 1)^4$ et $(X - 1)^4$ sont premiers entre eux, d'après le théorème de BEZOUT il existe des couples (U, V) de polynômes vérifiant (α) et parmi ces couples, un couple unique (U_0, V_0) de polynômes de degrés strictement inférieurs à 4. Cherchons (U_0, V_0).

Première méthode. On trouve (U_0, V_0) en effectuant la suite de divisions de l'algorithme d'EUCLIDE pour la recherche du p. g. c. d. de $(X + 1)^4$ et de $(X - 1)^4$. On a les résultats suivants :

	1	$\frac{1}{8}X - \frac{1}{2}$	$\frac{8}{5}X$	$\frac{25}{32}X$
$X^4 + 4X^3 + 6X^2 + 4X + 1$	$X^4 - 4X^3 + 6X^2 - 4X + 1$	$8X^3 + 8X$	$5X^2 + 1$	$\frac{32}{5}X$
$8X^3 + 8X$	$5X^2 + 1$	$\frac{32}{5}X$	1	

La dernière division nous permet d'écrire

$$1 = (5X^2 + 1) - \left(\frac{25}{32}X\right)\left(\frac{32}{5}X\right).$$

La division précédente donne une expression de $\frac{32}{5}X$ que l'on porte dans l'égalité ci-dessus, il vient

$$1 = (5X^2 + 1) - \left(\frac{25}{32}X\right)\left[(8X^3 + 8X) - (5X^2 + 1)\left(\frac{8}{5}X\right)\right]$$

soit

$$1 = -\left(\frac{25}{32}X\right)(8X^3 + 8X) + (5X^2 + 1)\left(1 + \frac{5}{4}X^2\right).$$

On recommence en utilisant les divisions précédentes ;

$$1 = -\left(\frac{25}{32}X\right)(8X^3 + 8X) + \\ + \left(1 + \frac{5}{4}X^2\right)\left[(X - 1)^4 - (8X^3 + 8X)\left(\frac{1}{8}X - \frac{1}{2}\right)\right],$$

d'où

$$1 = \left(1 + \frac{5}{4}X^2\right)(X - 1)^4 + \left[-\frac{25}{32}X - \left(1 + \frac{5}{4}X^2\right)\left(\frac{1}{8}X - \frac{1}{2}\right)\right](8X^3 + 8X)$$

soit

$$1 = \left(1 + \frac{5}{4}X^2\right)(X - 1)^4 + \left[-\frac{5}{32}X^3 + \frac{5}{8}X^2 - \frac{29}{32}X + \frac{1}{2}\right] \times \\ \times [(X + 1)^4 - (X - 1)^4]$$

soit encore

$$1 = \left[\frac{1}{2} + \frac{29}{32}X + \frac{5}{8}X^2 + \frac{5}{32}X^3\right](X - 1)^4 + \\ + \left[\frac{1}{2} - \frac{29}{32}X + \frac{5}{8}X^2 - \frac{5}{32}X^3\right](X + 1)^4$$

donc

$$U_0(X) = 1 + \frac{29}{16}X + \frac{5}{4}X^2 + \frac{5}{16}X^3$$

et

$$V_0(X) = -1 + \frac{29}{16}X - \frac{5}{4}X^2 + \frac{5}{16}X^3.$$

Deuxième méthode. Ecrivons la relation (α) pour $-X$,

$$2 = (X+1)^4 . U_0(X) - (X-1)^4 . V_0(-X) .$$

En raison de l'unicité des polynômes U_0 et V_0, on a $U_0(X) = -V_0(-X)$. $U_0(X)$ étant de degré inférieur ou égal à 3 est de la forme

$$U_0(X) = a + bX + cX^2 + dX^3 ,$$

donc

$$\begin{aligned} U_0(X).(X-1)^4 = {} & dX^7 + (c-4d)X^6 + (6d-4c+b)X^5 \\ & + (a-4b+6c-4d)X^4 \\ & + (d-4c+6b-4a)X^3 \\ & + (6a-4b+c)X^2 + (b-4a)X + a , \end{aligned}$$

et $V_0(X)(X+1)^4 = -[U_0(-X).(-X-1)^4]$; a, b, c, d vérifient donc (en raison de (α))

$$\begin{cases} 2a = 2 \\ 6a - 4b + c = 0 \\ a - 4b + 6c - 4d = 0 \\ c - 4d = 0 . \end{cases}$$

La solution de ce système est

$$a = 1 , \quad b = \frac{29}{16} , \quad c = \frac{5}{4} , \quad d = \frac{5}{16} .$$

Tous les polynômes (U, V) vérifiant (α) sont de la forme

$$U(X) = U_0(X) + P(X)(X+1)^4 , \; V(X) = V_0(X) - P(X)(X-1)^4$$

$P(X)$ étant un polynôme quelconque de $\mathbf{R}[X]$.

Le seul polynôme f_0 de degré 7 répondant à la question est donc

$$\begin{aligned} f_0(X) &= 1 + (X+1)^4 \left(-1 + \frac{29}{16}X - \frac{5}{4}X^2 + \frac{5}{16}X^3 \right) \\ &= \frac{35}{16}\left[-X + X^3 - \frac{3}{5}X^5 + \frac{1}{7}X^7 \right] . \end{aligned}$$

Tous les polynômes f solutions du problème sont de la forme

$$f(X) = f_0(X) - P(X)(X^2-1)^4$$

où $P(X)$ est un polynôme quelconque de $\mathbf{R}[X]$.

b) Les notations étant celles de la question précédente, le polynôme dérivé f' de f vérifie les deux relations

$$\begin{aligned} f'(X) &= 4(X-1)^3 . U(X) + (X-1)^4 . U'(X) , \\ f'(X) &= 4(X+1)^3 . V(X) + (X+1)^4 . V'(X) . \end{aligned}$$

Les polynômes U, V et leurs dérivées vérifient donc l'égalité

$$(X-1)^3[4U(X)+(X-1)U'(X)] = (X+1)^3[4V(X)+(X+1)V'(X)],$$

or $(X+1)^3$ est premier avec $(X-1)^3$ donc $(X+1)^3$ divise $4U(X)+(X-1)U'(X)$, il existe donc un polynôme $Q(X)$ de $\mathbf{R}[X]$ tel que

$$4U(X)+(X-1)U'(X) = Q(X).(X+1)^3$$
$$4V(X)+(X+1)V'(X) = Q(X)(X-1)^3$$

et par suite, tel que $f'(X) = Q(X)(X^2-1)^3$.

Cherchons d'abord les solutions du problème correspondant à un polynôme $Q(X)$ constant c'est-à-dire cherchons les polynômes $f_0(X)$ tels que $f_0'(X) = \lambda(X^2-1)^3$ où λ est un nombre réel. Il existe une constante réelle k telle que

$$f_0(X) = \lambda\left[\frac{X^7}{7} - \frac{3}{5}X^5 + \frac{3X^3}{3} - X + k\right].$$

Le polynôme $f_0(X)+1$ admet 1 comme racine d'ordre 4 si et seulement si 1 est racine de ce polynôme et racine triple de sa dérivée $f_0'(X)$. La deuxième condition est réalisée s'il a la forme précédente, λ et k vérifient donc la relation

$$\lambda\left[\frac{1}{7} - \frac{3}{5} + k\right] + 1 = 0;$$

de même $f_0(X) - 1$ admet -1 comme racine quatrième si et seulement si

$$\lambda\left[-\frac{1}{7} + \frac{3}{5} + k\right] - 1 = 0$$

donc nécessairement $k = 0$ et $\lambda = \frac{35}{16}$.

On retrouve bien l'existence d'une solution unique f_0 de degré inférieur ou égal à 7.

Si f est une solution quelconque du problème, $f - f_0$ est un multiple de $(X+1)^4$ et de $(X-1)^4$ donc de $(X^2-1)^4$. Les solutions du problème sont donc les polynômes f de $\mathbf{R}[X]$ de la forme $f(X) = f_0(X) - P(X)(X^2-1)^4$ où $P(X)$ est un élément de $\mathbf{R}[X]$.

8.10 Soient K un corps commutatif et E l'espace vectoriel des polynômes à une indéterminée X sur K, de degré inférieur ou égal à n. Si a est un élément de K, à tout polynôme P de E, on fait correspondre le polynôme $f(P)$ défini par

$$f(P)(X) = (X-a)[P'(X) + P'(a)] - 2[P(X) - P(a)].$$

a) Montrer que f est un endomorphisme de E.

b) Trouver l'image et le noyau de f.

Solution *a*) La dérivation est un endomorphisme de E. Soient P et Q deux polynômes de E, λ et μ deux éléments de K, alors $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$. D'autre part $(\lambda P + \mu Q)(X) = \lambda P(X) + \mu Q(X)$; la formule définissant $f(P)$ faisant intervenir P et P' de manière linéaire, on a

$$f(\lambda P + \mu Q) = \lambda f(P) + \mu f(Q) ;$$

f est donc un endomorphisme de E.

b) Les polynômes $(e_k)_{0 \leqslant k \leqslant n}$ définis par $e_k(X) = (X - a)^k$ forment une base de E. On a $f(e_0) = 0, f(e_1) = 0$ et $f(e_k) = (k - 2)\, e_k$ pour $2 \leqslant k \leqslant n$. $\operatorname{Im} f$ est engendré par les polynômes $(f(e_k))_{0 \leqslant k \leqslant n}$; or $f(e_0) = f(e_1) = f(e_2) = 0$ et pour $2 < k \leqslant n, f(e_k)$ est de degré k, donc les polynômes $f(e_3), f(e_4), \ldots, f(e_n)$ forment une partie libre (*cf.* Q. Ch. 11, § II, n° 187, th. 6) maximale extraite d'une partie génératrice de $\operatorname{Im} f$, donc forment une base de $\operatorname{Im} f$. Tout polynôme P de $\operatorname{Im} f$ s'écrit donc de manière unique sous la forme

$$P(X) = \lambda_1(X - a)^3 + 2\,\lambda_2(X - a)^4 + \cdots + (n - 2)\,\lambda_{n-2}(X - a)^n$$

où $\lambda_1, \lambda_2, \ldots, \lambda_{n-2}$ sont des éléments de K.

On observe aussi que a est une racine triple de tout polynôme de $\operatorname{Im} f$; réciproquement tout polynôme Q de E admettant a pour racine triple s'écrit (d'après la formule de TAYLOR)

$$Q(X) = (X - a)^3 \frac{Q'''(a)}{3!} + \cdots + (X - a)^n \frac{Q^{(n)}(a)}{n!}$$

car $Q(a) = Q'(a) = Q''(a) = 0$; il appartient donc à $\operatorname{Im} f$. $\operatorname{Im} f$ est donc le sous-espace de dimension $n - 2$ formé par les polynômes de E qui admettent a pour racine triple. E étant de dimension $n + 1$ et $\operatorname{Im} f$ de dimension $n - 2$, on a

$$\dim \operatorname{Ker} f = \dim E - \dim \operatorname{Im} f = 3$$

(*cf.* Q., Ch. 7, § IV, n° 143) ; or e_0, e_1, e_2 sont trois vecteurs libres qui appartiennent à $\operatorname{Ker} f$, donc ils forment une base de $\operatorname{Ker} f$ et $\operatorname{Ker} f$ est l'ensemble des polynômes de E de degré inférieur ou égal à 2.

8.11 Soient a, b deux entiers rationnels et n un entier naturel. Montrer que le polynôme

$$P(X) = \frac{X^n(a - bX)^n}{n!}$$

de $\mathbf{R}[X]$ ainsi que toutes ses dérivées, prend des valeurs entières pour

$$X = 0 \quad \text{et} \quad X = \frac{a}{b}.$$

Solution Les $(n-1)$ premières dérivées de $P(X)$ sont nulles pour $X = 0$ et $X = \frac{a}{b}$ car $P(X)$ contient X^n et $\left(X - \frac{a}{b}\right)^n$ en facteur. Ecrivons la formule de TAYLOR pour ce polynôme ;

$$P(X) = P^n(0)\frac{X^n}{n!} + P^{(n+1)}(0)\frac{X^{n+1}}{(n+1)!} + \cdots + P^{(2n)}(0)\frac{X^{2n}}{(2n)!}.$$

On en déduit que

$$(a - bX)^n = P^n(0) + P^{(n+1)}(0)\frac{n!}{(n+1)!}X + \cdots + P^{(2n)}(0)\frac{n!}{(2n)!}X^n.$$

En développant le premier membre de cette égalité au moyen de la formule du binôme et en identifiant les coefficients de $1, X, X^2, \ldots, X^n$, on obtient alors, pour tout entier p tel que $0 \leqslant p \leqslant n$,

$$P^{(n+p)}(0) = \frac{(n+p)!}{n!} C_n^p a^{n-p}(-b)^p$$

donc toutes les dérivées du polynôme $P(X)$ prennent des valeurs entières pour $X = 0$ puisque les dérivées d'ordre supérieur à $2n$ sont identiquement nulles.

De même la formule de TAYLOR en $\frac{a}{b}$ nous permet d'écrire

$$\frac{(-1)^n X^n b^n}{n!} = \frac{1}{n!}P^{(n)}\left(\frac{a}{b}\right) + \frac{1}{(n+1)!}P^{(n+1)}\left(\frac{a}{b}\right)\left(X - \frac{a}{b}\right) + \cdots + \frac{1}{(2n)!}P^{(2n)}\left(\frac{a}{b}\right)\left(X - \frac{a}{b}\right)^n.$$

Posons $X - \frac{a}{b} = Y$; il vient

$$\frac{(-1)^n(bY + a)^n}{n!} = \frac{1}{n!}P^n\left(\frac{a}{b}\right) + \frac{1}{(n+1)!}P^{(n+1)}\left(\frac{a}{b}\right)Y + \cdots + \frac{1}{(2n)!}P^{(2n)}\left(\frac{a}{b}\right)Y^n.$$

Nous obtenons donc pour tout entier p compris entre 0 et n,

$$P^{(n+p)}\left(\frac{a}{b}\right) = C_n^p \frac{(n+p)!}{n!}(-1)^n b^p a^{n-p}$$

par suite, toutes les dérivées de $P(X)$ prennent des valeurs entières pour $X = \frac{a}{b}$.

8.12 On dit qu'un anneau A est *factoriel* s'il est intègre, unitaire et s'il possède les propriétés F_1 et F_2 suivantes :

(F_1) Tout élément non inversible de A est produit d'un nombre fini d'éléments extrémaux de A.

(F_2) Si a et b sont deux éléments de A, tout élément extrémal p de A qui divise le produit $a.b$, divise soit a, soit b.

Soient x, y, p des éléments de A ; on écrit $x \equiv y(p)$ si et seulement s'il existe un élément k de A tel que $x - y = k.p$.

A étant un anneau factoriel et p un élément extrémal de A, on considère le polynôme

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n$$

de $A[X]$. On désigne par K le corps des fractions de l'anneau A.

a) Démontrer que si $a_i \equiv 0(p)$ pour $i = 0, 1, ..., n-1$, $a_n \not\equiv 0(p)$ et $a_0 \not\equiv 0(p^2)$, alors le polynôme f est irréductible sur $K[X]$. (Ce résultat est connu sous le nom de *critère d'irréductibilité d'Eisenstein.*)

b) En déduire que si n est un entier naturel premier, le polynôme

$$\Phi_n(X) = 1 + X + X^2 + \cdots + X^{n-1}$$

est irréductible sur $\mathbf{Q}[X]$.

Solution *a*) Supposons que f soit le produit de deux polynômes g et h de degrés strictement positifs, à coefficients dans A. Posons

$$g(X) = b_0 + b_1 X + \cdots + b_l X^l$$
$$h(X) = c_0 + c_1 X + \cdots + c_m X^m \quad \text{avec} \quad l + m = n .$$

Les coefficients de f s'expriment en fonction des coefficients de g et h de la manière suivante

$$a_i = \sum_{\substack{r+s=i \\ 0 \leqslant r \leqslant l \\ 0 \leqslant s \leqslant m}} b_r c_s \qquad \text{pour} \qquad i = 0, 1, ..., n .$$

En particulier, $a_0 = b_0 c_0$ donc p divise $b_0 c_0$ par suite p divise b_0 ou c_0, en raison de (F_2). Supposons par exemple que p divise b_0 ; comme p^2 ne divise pas a_0, p ne divise pas c_0. Pour $0 \leqslant i \leqslant l$ on peut écrire

$$a_i = b_i c_0 + \sum_{\substack{r+s=i \\ 0 \leqslant r \leqslant i-1 \\ 0 \leqslant s \leqslant m}} b_r c_s .$$

Supposons démontré que p divise b_r pour r compris entre 0 et $i-1$; comme p divise a_i, p divise $b_i c_0$ et par suite b_i. Nous avons ainsi démontré par récurrence que p divise $b_0, b_1, \ldots, b_l$, or ceci est impossible car p ne divise pas a_n et $a_n = b_l c_m$; f est donc irréductible sur $K[X]$.

b) On a $X^n - 1 = (X-1)\,\Phi_n(X)$; posons $g(Y) = \Phi_n(Y+1)$, alors

$$g(Y) = \frac{(Y+1)^n - 1}{Y};$$

en utilisant la formule du binôme on obtient

$$g(Y) = C_n^1 + C_n^2 Y + \cdots + C_n^{p+1} Y^p + \cdots + Y^{n-1}.$$

$g(Y)$ est un polynôme de degré $n-1$ à coefficients dans $\mathbf{Z}$; $\mathbf{Z}$ est un anneau intègre, unitaire dont le corps des fractions est $\mathbf{Q}$ et dont les éléments extrémaux sont les nombres premiers ; de plus $\mathbf{Z}$ satisfait aux conditions (F_1) et (F_2) ; en effet, tout entier rationnel se décompose en produit d'un nombre fini de facteurs premiers et tout nombre premier p qui divise le produit $a.b$ de deux entiers rationnels, divise soit a soit b. $\mathbf{Z}$ est donc un anneau factoriel. Soit a_p le coefficient de Y^p dans $g(Y)$; comme $a_0 = n$, on a $a_0 \equiv 0(n)$ et $a_0 \not\equiv 0(n^2)$; n étant premier, il divise C_n^p pour $1 \leqslant p \leqslant n-1$, donc $a_p \equiv 0(n)$ pour $1 \leqslant p \leqslant n-2$; on a $a_{n-1} = 1$ donc $a_{n-1} \not\equiv 0(n)$. $g(Y)$ satisfait donc au critère de la question précédente. Le polynôme $g(Y)$ et par suite le polynôme $\Phi_n(X)$ sont donc irréductibles sur $\mathbf{Q}[X]$.

8.13 Soient n un entier naturel non nul et E l'espace vectoriel des polynômes à une indéterminée X, à coefficients réels, de degré strictement inférieur à n. Soient $x_1, x_2, \ldots, x_n$ des nombres réels distincts deux à deux ; on pose

$$H(X) = (X - x_1)(X - x_2) \ldots (X - x_n).$$

1) Calculer $H'(x_i)$ $(1 \leqslant i \leqslant n)$ et les n polynômes

$$E_i(X) = \frac{1}{H'(x_i)} \frac{H(X)}{(X - x_i)} \quad (1 \leqslant i \leqslant n).$$

2) Calculer $E_j(x_i)$ $(1 \leqslant j \leqslant n,\ 1 \leqslant i \leqslant n)$; en déduire que les polynômes $E_1, E_2, \ldots, E_n$ sont linéairement indépendants et qu'ils forment une base de E.

3) *a*) Montrer que l'application φ_i $(1 \leqslant i \leqslant n)$ de E dans $\mathbf{R}$, définie en posant pour chaque élément P de E, $\varphi_i(P) = P(x_i)$ est une forme linéaire.

b) Montrer que $(\varphi_1, \varphi_2, \ldots, \varphi_n)$ est la base du dual E^* de E, duale de la base $(E_1, E_2, \ldots, E_n)$ de E.

c) En déduire le résultat suivant : étant donnés n nombres réels $y_1, y_2, \ldots, y_n$, il existe un polynôme P de E et un seul, tel que $P(x_i) = y_i$ pour $1 \leqslant i \leqslant n$.

4) Soit f une fonction définie continue sur l'intervalle $[a, b]$ de **R**, à valeurs réelles. On considère l'application g de E dans **R**, définie en posant pour chaque élément P de E,

$$g(P) = \int_a^b f(t)\, P(t)\, \mathrm{d}t\,.$$

Montrer que g est une forme linéaire ; donner ses coordonnées sur la base $(\varphi_1, \varphi_2, ..., \varphi_n)$ de E^*, sous forme d'intégrales définies.

5) Soient $b_1, b_2, ..., b_{n+1}$ des nombres réels tels que $b_1 < b_2 < \cdots < b_n < b_{n+1}$. Pour chaque entier i compris entre 1 et n on définit une application ψ_i de E dans **R** en posant pour chaque élément P de E,

$$\psi_i(P) = \int_{b_i}^{b_{i+1}} P(t)\, \mathrm{d}t\,.$$

Montrer que ψ_i $(1 \leqslant i \leqslant n)$ est une forme linéaire. Démontrer qu'il existe n polynômes $F_1, F_2, ..., F_n$ de E tels que

$$\psi_i(F_j) = \begin{cases} 0 & \text{si} \quad i \neq j \\ 1 & \text{si} \quad i = j\,. \end{cases}$$

En déduire que $(\psi_1, \psi_2, ..., \psi_n)$ est une base de E^*.

6) Exprimer (sous forme d'intégrales définies et en fonction des E_i et des F_j $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$) les coordonnées des formes ψ_i $(1 \leqslant i \leqslant n)$ sur la base $(\varphi_1, \varphi_2, ..., \varphi_n)$ et les coordonnées des formes φ_i $(1 \leqslant i \leqslant n)$ sur la base $(\psi_1, \psi_2, ..., \psi_n)$.

7) Trouver la base duale de la base de E formée par les n polynômes 1, X, $X^2, ..., X^{n-1}$.

Solution 1) On trouve facilement

$$H'(X) = \sum_{j=1}^{n} (X - x_1) ... (X - x_{j-1})(X - x_{j+1}) ... (X - x_n)\,,$$

donc

$$H'(x_i) = (x_i - x_1) ... (x_i - x_{i-1})(x_i - x_{i+1}) ... (x_i - x_n) \quad (1 \leqslant i \leqslant n)\,;$$

on en déduit que

$$E_i(X) = \frac{(X - x_1) ... (X - x_{i-1})(X - x_{i+1}) ... (X - x_n)}{(x_i - x_1) ... (x_i - x_{i-1})(x_i - x_{i+1}) ... (x_i - x_n)} \qquad (1 \leqslant i \leqslant n)\,.$$

2) En remplaçant X par x_i dans E_j on trouve $E_j(x_i) = \delta_{ij}$ (où $\delta_{ij} = 1$ si $i = j$ et $\delta_{ij} = 0$ si $i \neq j$). Montrons que la famille $(E_1, E_2, ..., E_n)$ est libre ; soient $\lambda_1, \lambda_2, ..., \lambda_n$ des nombres réels tels que $\lambda_1 E_1 + \lambda_2 E_2 + \cdots + \lambda_n E_n = 0$.

Nous avons en particulier $(\lambda_1 E_1 + \lambda_2 E_2 + \cdots + \lambda_n E_n)\ (x_i) = 0$ pour $1 \leqslant i \leqslant n$, soit $\lambda_i = 0$ pour $1 \leqslant i \leqslant n$.

La dimension de l'espace vectoriel E étant n, la famille libre $(E_1, E_2, \ldots, E_n)$ est une base de E.

3) *a*) φ_i $(1 \leqslant i \leqslant n)$ est une forme linéaire car si P, Q sont deux éléments de E et λ un nombre réel, on a

$$\varphi_i(P + Q) = (P + Q)(x_i) = P(x_i) + Q(x_i) = \varphi_i(P) + \varphi_i(Q)$$

et

$$\varphi_i(\lambda P) = (\lambda P)(x_i) = \lambda(P(x_i)) = \lambda\varphi_i(P)\,.$$

b) Pour montrer que $(\varphi_1, \varphi_2, \ldots, \varphi_n)$ est la base duale de $(E_1, E_2, \ldots, E_n)$ il suffit de vérifier que $\varphi_i(E_j) = \delta_{ij}$ pour $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant n$ (*cf.* Q., Ch. 7, § VI, n° 150) ; or on a précisément $\varphi_i(E_j) = E_j(x_i) = \delta_{ij}$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$.

c) Soient $y_1, y_2, \ldots, y_n$ des nombres réels et Q un polynôme de E ; comme $E_1, E_2, \ldots, E_n$ forment une base de E, il existe un élément $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ de $\mathbf{R}^n$ et un seul, tel que $Q = \alpha_1 E_1 + \alpha_2 E_2 + \cdots + \alpha_n E_n$. Alors on a pour $1 \leqslant i \leqslant n$, $\varphi_i(Q) = \alpha_1 E_1(x_i) + \alpha_2 E_2(x_i) + \cdots + \alpha_n E_n(x_i) = \alpha_i$; par suite, le polynôme $P = y_1 E_1 + y_2 E_2 + \cdots + y_n E_n$ est le seul polynôme de E tel que l'on ait $\varphi_i(P) = P(x_i) = y_i$ pour $1 \leqslant i \leqslant n$.

4) g est une forme linéaire car on a quels que soient les éléments P, Q de E et le nombre réel λ,

$$g(P + Q) = \int_a^b f(t)\,(P + Q)\,(t)\,\mathrm{d}t = \int_a^b f(t)\,\big(P(t) + Q(t)\big)\,\mathrm{d}t$$

$$= \int_a^b f(t)\,P(t)\,\mathrm{d}t + \int_a^b f(t)\,Q(t)\,\mathrm{d}t$$

$$= g(P) + g(Q)$$

$$\text{et}\quad g(\lambda P) = \int_a^b f(t)\,\lambda P(t)\,\mathrm{d}t$$

$$= \lambda \int_a^b f(t)\,P(t)\,\mathrm{d}t = \lambda g(P)\,.$$

Cherchons des nombres réels $\alpha_1, \alpha_2, \ldots, \alpha_n$ tels que

$$g = \alpha_1 \varphi_1 + \alpha_2 \varphi_2 + \cdots + \alpha_n \varphi_n\,.$$

On doit avoir

$$g(E_j) = \alpha_1 \varphi_1(E_j) + \alpha_2 \varphi_2(E_j) + \cdots + \alpha_n \varphi_n(E_j) = \alpha_j \quad (1 \leqslant j \leqslant n)$$

donc la j-ième coordonnée de g sur la base $(\varphi_1, \varphi_2, \ldots, \varphi_n)$ est égale à

$$g(E_j) = \int_a^b f(t)\,E_j(t)\,\mathrm{d}t\,.$$

5) Nous savons déjà que ψ_i $(1 \leqslant i \leqslant n)$ est une forme linéaire puisqu'il suffit de remplacer dans la question précédente l'intervalle $[a, b]$ par l'intervalle $[b_i, b_{i+1}]$ et de prendre pour fonction f la fonction constante de valeur 1.

Cherchons un polynôme F_j $(1 \leqslant j \leqslant n)$ tel que

$$\int_{b_i}^{b_{i+1}} F_j(t)\,\mathrm{d}t = \delta_{ij}$$

pour $1 \leqslant i \leqslant n$. Soit G_j la primitive de F_j nulle en b_1 ; Comme

$$\int_{b_i}^{b_{i+1}} F_j(t)\,\mathrm{d}t = G_j(b_{i+1}) - G_j(b_i) = \delta_{ij}\,,$$

nous devons imposer à G_j de vérifier les égalités :

$$G_j(b_1) = 0\,,\ G_j(b_2) = 0\,,\ \ldots\,,\ G_j(b_j) = 0\,,\ G_j(b_{j+1}) = 1\,,\ \ldots\,,\ G_j(b_{n+1}) = 1\,.$$

Mais d'après la question 3 *c* nous savons qu'il existe un polynôme G_j de degré n au plus, vérifiant les égalités précédentes ; le polynôme $F_j = G_j'$ est de degré strictement inférieur à n donc il appartient à E.

Pour montrer que les n éléments $\psi_1, \psi_2, \ldots, \psi_n$ forment une base de l'espace vectoriel E^* dont la dimension est n, il suffit de montrer qu'ils sont linéairement indépendants. Soient $\lambda_1, \lambda_2, \ldots, \lambda_n$ des nombres réels tels que

$$\lambda_1 \psi_1 + \lambda_2 \psi_2 + \cdots + \lambda_n \psi_n = 0\,;$$

nous avons en particulier

$$\lambda_1 \psi_1(F_j) + \lambda_2 \psi_2(F_j) + \cdots + \lambda_n \psi_n(F_j) = \lambda_j = 0 \quad (1 \leqslant j \leqslant n)\,,$$

donc $(\psi_1, \psi_2, \ldots, \psi_n)$ est une base de E^*.

6) D'après la question 4 on sait déjà que ψ_i s'écrit dans la base $(\varphi_1, \varphi_2, \ldots, \varphi_n)$

$$\psi_i = \sum_{j=1}^{n} \psi_i(E_j)\,\varphi_j = \sum_{j=1}^{n} \left(\int_{b_i}^{b_{i+1}} E_j(t)\,\mathrm{d}t \right) \varphi_j\,.$$

Cherchons les coordonnées $\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,n}$ de φ_i sur la base $(\psi_1, \psi_2, \ldots, \psi_n)$; on a

$$\varphi_i = \sum_{k=1}^{n} \alpha_{i,k}\,\psi_k\,,$$

donc on a pour $1 \leqslant j \leqslant n$,

$$\varphi_i(F_j) = \sum_{k=1}^{n} \alpha_{i,k}\,\psi_k(F_j) = \alpha_{i,j}$$

donc

$$\varphi_i = \sum_{j=1}^{n} \varphi_i(F_j)\,\psi_j = \sum_{j=1}^{n} F_j(x_i)\,\psi_j\,.$$

7) Nous savons (*cf.* Q., Ch. 7, § VI, n° 150) que les n éléments de E^* qui constituent la base duale de la base $(1, X, X^2, ..., X^{n-1})$, sont les n projections déterminées par cette base. Nous devons donc trouver les coordonnées d'un polynôme P de E sur cette base ; or, la formule de TAYLOR appliquée à un polynôme de degré $n - 1$ au plus, définit ces coordonnées :

$$P(X) = P(0) + P'(0)\,X + \frac{P''(0)}{2\,!}X^2 + \cdots + \frac{P^{(n-1)}(0)}{(n-1)\,!}X^{n-1}\,.$$

Donc les éléments de la base $(\theta_1, \theta_2, ..., \theta_n)$ duale de la base $(1, X, X^2, ..., X^{n-1})$ sont définis en posant pour tout élément P de E,

$$\theta_k(P) = \frac{P^{(k-1)}(0)}{(k-1)\,!} \qquad (1 \leqslant k \leqslant n)\,.$$

8.14 Dans **C** résoudre l'équation $x^3 + 12\,x = 12$. (On peut poser $x = u + v$ et se ramener à une équation du second degré.)

Solution Posons $x = u + v$; il vient $(u + v)^3 + 12(u + v) = 12$ soit

$$u^3 + v^3 + (3\,uv + 12)\,(u + v) = 12\,,$$

donc si l'on pose $uv = -4$, on a $u^3 + v^3 = 12$ et par suite u^3 et v^3 sont les solutions de l'équation du second degré

$$X^2 - 12\,X - 64 = 0\,.$$

On a donc $u^3 = 16$ et $v^3 = -4$. Si l'on note j la racine cubique de l'unité d'argument $\frac{2\,\pi}{3}$, les solutions de l'équation $u^3 = 16$ sont

$$u_1 = \sqrt[3]{16}\,, \quad u_2 = j\sqrt[3]{16} \qquad \text{et} \qquad u_3 = j^2\sqrt[3]{16}\,.$$

De même, les solutions de l'équation $v^3 = -4$ sont $-\sqrt[3]{4}$, $-j\sqrt[3]{4}$ et $-j^2\sqrt[3]{4}$; les racines de l'équation proposée sont données par $x = u + v$ avec $u^3 = 16$, $v^3 = -4$ et $uv = -4$ donc par

$$x_1 = \sqrt[3]{16} - \sqrt[3]{4}\,, \quad x_2 = j\sqrt[3]{16} - j^2\sqrt[3]{4}\,,$$

$$x_3 = j^2\sqrt[3]{16} - j\sqrt[3]{4}\,.$$

Il n'y a pas d'autre racine car l'équation est de degré 3.

8.15 Résoudre dans **C** les équations suivantes

$$x^4 - 2x^2 - 15 = 0 \qquad (1)$$

$$x^4 - x^2 + 4 = 0. \qquad (2)$$

Solution 1) Si x vérifie l'équation (1), x^2 est solution de l'équation du second degré $X^2 - 2X - 15 = 0$ qui a pour racines 5 et -3. Les quatre solutions de l'équation (1) sont donc $\sqrt{5}$, $-\sqrt{5}$, $i\sqrt{3}$, $-i\sqrt{3}$.

2) L'équation du second degré associée à l'équation (2) en posant $X = x^2$ n'a pas de solution réelle ; pour résoudre (2) nous emploierons une méthode différente de la précédente. On a

$$x^4 - x^2 + 4 = (x^2 + 2)^2 - 5x^2 = (x^2 + \sqrt{5}x + 2)(x^2 - \sqrt{5}x + 2)$$

par suite, les solutions de l'équation (2) sont les solutions des équations du second degré

$$x^2 + \sqrt{5}x + 2 = 0 \quad \text{et} \quad x^2 - \sqrt{5}x + 2 = 0,$$

soit

$$\frac{-\sqrt{5} + i\sqrt{3}}{2}, \frac{-\sqrt{5} - i\sqrt{3}}{2}, \frac{\sqrt{5} + i\sqrt{3}}{2}, \frac{\sqrt{5} - i\sqrt{3}}{2}.$$

8.16 Soit n un entier positif. Décomposer en éléments simples sur **C** puis sur **R** les fractions rationnelles $\frac{1}{X^{2n} - 1}$ et $\frac{1}{X^{2n+1} - 1}$.

Solution Pour chaque entier positif p, posons

$$f_p(X) = \frac{1}{X^p - 1};$$

dans **C** le polynôme $X^p - 1$ a p racines distinctes $(\omega_k)_{0 \leq k \leq p-1}$ données par

$$\omega_k = e^{\frac{2k\pi i}{p}}.$$

La décomposition en éléments simples de $f_p(X)$ est donc de la forme

$$f_p(X) = \sum_{k=0}^{p-1} \frac{a_k}{X - \omega_k}$$

$a_0, a_1, \ldots, a_{p-1}$ étant des nombres complexes. Si ω est un nombre complexe, on a l'identité

$$X^p - \omega^p = (X - \omega)(X^{p-1} + \omega X^{p-2} + \cdots + \omega^{p-2} X + \omega^{p-1})$$

donc on a

$$\frac{X - \omega_k}{X^p - 1} = \frac{1}{X^{p-1} + \omega_k X^{p-2} + \cdots + \omega_k^{p-1}}$$

et par suite

$$a_k = \frac{1}{p\omega_k^{p-1}} = \frac{\omega_k}{p}$$

(*cf.* Q., Ch. 12, § II, n° 206). La décomposition de la fraction rationnelle $f_p(X)$ dans $\mathbf{C}(X)$ est donc

$$f_p(X) = \frac{1}{p} \sum_{k=0}^{p-1} \frac{\omega_k}{X - \omega_k} \qquad \text{avec} \qquad \omega_k = \mathrm{e}^{\frac{2k\pi i}{p}}.$$

Cette décomposition de $f_p(X)$ est indépendante de la parité de p ; elle résout donc le problème posé dans $\mathbf{C}(X)$. La décomposition de $f_p(X)$ sur $\mathbf{R}$ s'obtient en regroupant deux à deux les éléments simples de la décomposition sur $\mathbf{C}$ correspondant à deux pôles complexes conjugués. On a

$$\frac{\omega_k}{X - \omega_k} + \frac{\bar{\omega}_k}{X - \bar{\omega}_k} = \frac{X(\omega_k + \bar{\omega}_k) - 2}{X^2 - (\omega_k + \bar{\omega}_k) X + 1} = \frac{2\left(X \cos \frac{2k\pi}{p} - 1\right)}{X^2 - 2\left(\cos \frac{2k\pi}{p}\right) X + 1}.$$

Si p est pair, $f_p(X)$ a deux pôles réels 1 et -1 ; la décomposition dans $\mathbf{R}(X)$ de $f_{2n}(X)$ est donc

$$f_{2n}(X) = \frac{1}{2n}\left[\frac{1}{X - 1} + \frac{-1}{X + 1} + 2 \sum_{k=1}^{n-1} \frac{\left(X \cos \frac{k\pi}{n} - 1\right)}{X^2 - 2X \cos \frac{k\pi}{n} + 1}\right].$$

Si p est impair, $f_p(X)$ a un seul pôle réel 1, par suite la décomposition dans $\mathbf{R}(X)$ de $f_{2n+1}(X)$ est

$$f_{2n+1}(X) = \frac{1}{2n+1}\left[\frac{1}{X - 1} + 2 \sum_{k=1}^{n} \frac{\left(X \cos \frac{2k\pi}{2n+1} - 1\right)}{X^2 - 2X \cos \frac{2k\pi}{2n+1} + 1}\right].$$

8.17 Soient n un entier positif et a, b deux nombres complexes ; décomposer en éléments simples sur **C**, les fractions rationnelles

$$\frac{1}{(X^2-1)^n} \quad \text{et} \quad \frac{1}{(X-a)^n(X-b)^n}$$

Solution On remarque que la première fraction à décomposer est un cas particulier de la seconde obtenu en posant $a = 1$ et $b = -1$. Traitons donc directement la décomposition de $\dfrac{1}{(X-a)^n(X-b)^n}$. Posons

$$F(X) = \frac{1}{(X-b)^n};$$

en appliquant la formule de TAYLOR à l'ordre $(n-1)$, pour $X = a$ à la fraction $F(X)$, on obtient

$$F(X) = F(a) + (X-a)\frac{F'(a)}{1!} + \cdots + (X-a)^{n-1}\frac{F^{(n-1)}(a)}{(n-1)!} + (X-a)^n G(X)$$

où $G(X)$ est une fraction rationnelle dépourvue de pôle en a (*cf.* Q., Ch. 12, § II, n° 206). Or la décomposition en éléments simples de $\dfrac{1}{(X-a)^n(X-b)^n}$ sur **C** est de la forme

$$\frac{1}{(X-a)^n(X-b)^n} = \sum_{p=1}^{n}\frac{A_p}{(X-a)^p} + \sum_{p=1}^{n}\frac{B_p}{(X-b)^p}$$

où A_p et B_p $(1 \leqslant p \leqslant n)$ sont des nombres complexes. Le calcul précédent montre que

$$\frac{1}{(X-a)^n(X-b)^n} = \frac{F(a)}{(X-a)^n} + \frac{F'(a)}{1!(X-a)^{n-1}} + \cdots + \frac{F^{(n-1)}(a)}{(n-1)!(X-a)} + G(X).$$

En raison de l'unicité des coefficients A_p et B_p on a

$$A_p = \frac{F^{(n-p)}(a)}{(n-p)!};$$

or $$F^{(p)}(X) = (-n)(-n-1)\ldots(-n-p+1)(X-b)^{-n-p}$$

donc

$$F^{(p)}(a) = (-1)^p n(n+1)\dots(n+p-1)(a-b)^{n-p}$$

$$= \frac{(-1)^p (n+p-1)!}{(n-1)!} \frac{1}{(a-b)^{n+p}}$$

et par suite

$$A_p = \frac{(-1)^{n-p}(2n-p-1)!}{(n-1)!\,(n-p)!} \frac{1}{(a-b)^{2n-p}}$$

soit encore

$$A_p = (-1)^{n-p} C_{2n-p-1}^{n-1} \frac{1}{(a-b)^{2n-p}}$$

Les coefficients B_p s'obtiennent en changeant les rôles joués par a et b ; on a donc

$$B_p = (-1)^{n-p} C_{2n-p-1}^{n-1} \frac{1}{(b-a)^{2n-p}}$$

En particulier

$$\frac{1}{(X^2-1)^n} = \sum_{p=1}^{n} \frac{(-1)^n}{2^{2n-p}} C_{2n-p-1}^{n-1} \left[\frac{(-1)^p}{(X-1)^p} + \frac{1}{(X+1)^p}\right].$$

8.18 Décomposer en éléments simples dans $\mathbf{C}(X)$ et dans $\mathbf{R}(X)$ les fractions rationnelles suivantes

$$F_1(X) = \frac{1}{(X-1)^5(X^2+2X+4)}. \tag{1}$$

$$F_2(X) = \frac{1}{X^4 - 2X^3(\cos a + \cos b) + 2X^2(1 + 2\cos a \cos b) - 2X(\cos a + \cos b) + 1} \tag{2}$$

où a et b sont des nombres réels tels que $\cos a \neq \cos b$, $a \notin \mathbf{Z}\pi$ et $b \notin \mathbf{Z}\pi$.

$$F_3(X) = \frac{3X^5 + 2X^4 + X^2 + 3X + 2}{X^4 + 1}. \tag{3}$$

Solution 1) Décomposition de $F_1(X)$ dans $\mathbf{C}(X)$ est de la forme

$$F_1(X) = \sum_{p=1}^{5} \frac{A_p}{(X-1)^p} + \frac{B}{(X+1-i\sqrt{3})} + \frac{C}{(X+1+i\sqrt{3})},$$

où A_1, A_2, A_3, A_4, A_5, B et C sont des nombres complexes. B est la valeur prise par la fraction $\dfrac{1}{(X-1)^5(X+1+i\sqrt{3})}$ pour $X = -1 + i\sqrt{3}$ donc $B = \dfrac{1}{(-2+i\sqrt{3})^5(2i\sqrt{3})}$; de même $C = \dfrac{1}{(2+i\sqrt{3})^5(2i\sqrt{3})}$.
Pour calculer les coefficients A_1, A_2, A_3, A_4, A_5, posons $Y = X - 1$; alors $X^2 + 2X + 4 = 7 + 4Y + Y^2$ et en faisant la division suivant les puissances croissantes de 1 par $7 + 4Y + Y^2$ (*cf.* Q. Ch. 12, § II, n° 206) on obtient

$$\begin{array}{l|l}
1 & 7 + 4Y + Y^2 \\
\cline{2-2}
-\frac{4}{7}Y - \frac{1}{7}Y^2 & \frac{1}{7} - \frac{4}{7^2}Y + \frac{9}{7^3}Y^2 - \\
\frac{9}{7^2}Y^2 + \frac{4}{7^2}Y^3 & -\frac{8}{7^4}Y^3 - \frac{31}{7^5}Y^4 \\
-\frac{8}{7^3}Y^3 - \frac{9}{7^3}Y^4 & \\
-\frac{31}{7^4}Y^4 + \frac{8}{7^4}Y^5 & \\
\frac{180}{7^5}Y^5 + \frac{31}{7^5}Y^6 &
\end{array}$$

Ecrivons alors l'égalité que nous fournit cette division

$$1 = (7 + 4Y + Y^2)\left(\frac{1}{7} - \frac{4}{7^2}Y + \frac{9}{7^3}Y^2 - \frac{8}{7^4}Y^3 - \frac{31}{7^5}Y^4\right) + \frac{180}{7^5}Y^5 + \frac{31}{7^5}Y^6$$

d'où l'on déduit

$$\frac{1}{Y^5(7+4Y+Y^2)} = \frac{1}{7Y^5} - \frac{4}{7^2Y^4} + \frac{9}{7^3Y^3} - \frac{8}{7^4Y^2} - \frac{31}{7^5Y} + \frac{180+31Y}{7^5(7+4Y+Y^2)}$$

soit en revenant à l'indéterminée X

$$\frac{1}{(X-1)^5(X^2+2X+4)} = \frac{1}{7(X-1)^5} - \frac{4}{7^2(X-1)^4} + \frac{9}{7^3(X-1)^3} - \frac{8}{7^4(X-1)^2} - \frac{31}{7^5(X-1)} + \frac{31X+149}{7^5(X^2+2X+4)}$$

ce qui nous donne à la fois les coefficients A_p $(1 \leqslant p \leqslant 5)$ et la décomposition dans $\mathbf{R}(X)$.

2) Commençons par décomposer en facteurs le dénominateur $D(X)$ de la fraction $F_2(X)$; on a

$$D(X) = X^2\left[\left(X^2 + \frac{1}{X^2}\right) - 2(\cos a + \cos b)\left(X + \frac{1}{X}\right) + 2(1 + 2\cos a \cos b)\right].$$

Posons $Y = X + \dfrac{1}{X}$; il vient

$$D(X) = X^2[Y^2 - 2(\cos a + \cos b)\, Y + 4\cos a \cos b],$$

soit encore

$$D(X) = X^2[Y - 2\cos a]\,[Y - 2\cos b] = (X^2 - 2X\cos a + 1)(X^2 - 2X\cos b + 1)$$

par suite, la décomposition de $D(X)$ dans $\mathbf{C}[X]$ est

$$D(X) = (X - e^{ia})(X - e^{-ia})(X - e^{ib})(X - e^{-ib}).$$

Compte tenu des hypothèses faites sur a et b, les quatre facteurs de $D(X)$ sont distincts deux à deux donc la décomposition en éléments simples de $F_2(X)$ dans $\mathbf{C}[X]$ est de la forme

$$F_2(X) = \frac{A}{X - e^{ia}} + \frac{\bar{A}}{X - e^{-ia}} + \frac{B}{X - e^{ib}} + \frac{\bar{B}}{X - e^{-ib}},$$

la fraction $F_2(X)$ étant à coefficients réels, $\bar{A}$ et $\bar{B}$ sont les conjugués des nombres complexes A et B ; A est la valeur prise par la fraction

$$\frac{1}{(X - e^{-ia})(X^2 - 2X\cos b + 1)}$$

pour $X = e^{ia}$, donc

$$A = \frac{1}{(e^{ia} - e^{-ia})(e^{2ia} - 2e^{ia}\cos b + 1)} = \frac{1}{(e^{ia} - e^{-ia})e^{ia}(e^{ia} - 2\cos b + e^{-ia})},$$

soit aussi

$$A = \frac{1}{4i\sin a(\cos a - \cos b)e^{ia}} = \frac{-ie^{-ia}}{4\sin a(\cos a - \cos b)},$$

par suite

$$A = \frac{ie^{ia}}{4 \sin a(\cos a - \cos b)}.$$

a et b jouant des rôles symétriques dans l'expression de $F_2(X)$, on a

$$B = \frac{-ie^{-ib}}{4 \sin b(\cos b - \cos a)} \quad \text{et} \quad B = \frac{ie^{ib}}{4 \sin b(\cos b - \cos a)}.$$

En regroupant deux par deux les fractions obtenues dans la décomposition de $F_2(X)$ dans $\mathbf{C}(X)$, on obtient la décomposition de $F_2(X)$ dans $\mathbf{R}(X)$; on a donc

$$F_2(X) = \frac{-X + 2\cos a}{2(\cos a - \cos b)(X^2 - 2X\cos a + 1)} + \frac{-X + 2\cos b}{2(\cos b - \cos a)(X^2 - 2X\cos b + 1)}.$$

3) La fraction $F_3(X)$ admet une partie entière ; en effet on a

$$F_3(X) = 3X + 2 + \frac{X^2}{X^4 + 1}.$$

Nous sommes donc ramenés à décomposer la fraction $\frac{X^2}{X^4 + 1}$ Effectuons directement la décomposition de $\frac{X^2}{X^4 + 1}$ dans $\mathbf{R}(X)$ (ce procédé ayant un intérêt pour le calcul des intégrales en analyse).

$X^4 + 1$ est un trinôme bicarré et on a

$$X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 + 1 + \sqrt{2}X)(X^2 + 1 - \sqrt{2}X)$$

La décomposition de $\frac{X^2}{X^4 + 1}$ dans $\mathbf{R}(X)$ est donc de la forme

$$\frac{X^2}{X^4 + 1} = \frac{AX + B}{X^2 + X\sqrt{2} + 1} + \frac{CX + D}{X^2 - X\sqrt{2} + 1}$$

ou A, B, C, D sont des nombres réels tels que $A = -C$ et $B = D$ car le premier membre est une fraction paire.

Après réduction au même dénominateur du second membre et identification des numérateurs on obtient $B = D = 0$ et $A = -C = \frac{-1}{2\sqrt{2}}$ d'où la décomposition dans $\mathbf{R}(X)$

$$F_3(X) = 3X + 2 + \frac{1}{2\sqrt{2}}\left[\frac{1}{X^2 - \sqrt{2}X + 1} - \frac{1}{X^2 + \sqrt{2}X + 1}\right].$$

Les racines de $X^2 - X\sqrt{2} + 1$ dans C sont $e^{i\frac{\pi}{4}}$ et $e^{-i\frac{\pi}{4}}$; dans $C(X)$ la décomposition de $\dfrac{1}{X^2 - X\sqrt{2} + 1}$ est

$$\frac{1}{X^2 - \sqrt{2}\,X + 1} = \frac{A}{X - e^{i\frac{\pi}{4}}} + \frac{\bar{A}}{X - e^{-i\frac{\pi}{4}}},$$

où A désigne le nombre complexe

$$\frac{1}{e^{i\frac{\pi}{4}} - e^{-i\frac{\pi}{4}}} = -\frac{i}{\sqrt{2}} \qquad \text{et} \qquad \bar{A} = \frac{i}{\sqrt{2}};$$

de même on voit que

$$\frac{1}{X^2 + X\sqrt{2} + 1} = \frac{i}{\sqrt{2}(X - e^{-\frac{3i\pi}{4}})} - \frac{i}{\sqrt{2}(X - e^{\frac{3i\pi}{4}})},$$

par suite la décomposition de $F_3(X)$ dans $C(X)$ est

$$F_3(X) = 3X + 2 + \frac{i}{4}\left[\frac{-1}{X - e^{i\frac{\pi}{4}}} + \frac{1}{X - e^{-i\frac{\pi}{4}}} + \frac{1}{X - e^{3i\frac{\pi}{4}}} + \frac{-1}{X - e^{-3i\frac{\pi}{4}}}\right].$$

9

PROBLÈMES DE SYNTHÈSE

9.1

Soient K, K', K'' des corps commutatifs, E, E', E'' des espaces vectoriels sur K, K', K'' respectivement, φ un homomorphisme de corps de K dans K' et ψ un homomorphisme de corps de K' dans K''.

Une application f de E dans E' sera dite *φ-semi-linéaire* si elle vérifie quels que soient les éléments x, y de E et λ de K

$$f(x + y) = f(x) + f(y)$$
$$f(\lambda x) = \varphi(\lambda) f(x) .$$

1) *a*) Montrer que si E_1 et E_2 sont deux espaces vectoriels sur le corps K et h une application linéaire de E_1 dans E_2, alors h est Id K-semi-linéaire.

b) Soient f une application φ-semi-linéaire de E dans E' et g une application ψ-semi-linéaire de E' dans E'' ; montrer que $g \circ f$ est une application $(\psi \circ \varphi)$ semi-linéaire de E dans E''.

c) Supposons E de dimension finie et soient $(a_1, a_2, ..., a_n)$ une base de E et $b_1, b_2, ..., b_n$, n vecteurs de E'. Montrer qu'il existe une application φ-semi-linéaire f de E dans E' et une seule, telle que $f(a_i) = b_i$ pour $1 \leqslant i \leqslant n$.

d) Supposons que φ soit un isomorphisme de corps et que E soit de dimension finie sur K. Démontrer qu'une application φ-semi-linéaire f de E dans E' est bijective si et seulement si l'image par f d'une base de E est une base de E'.

2) *a*) Posons $E = K[X]$ et $E' = K'[X]$. Soit f l'application de E dans E' qui à chaque polynôme

$$P(X) = \sum_{i=0}^{n} \lambda_i X^i$$

de $K[X]$ fait correspondre le polynôme

$$(f(P))(X) = \sum_{i=0}^{n} \varphi(\lambda_i) X^i$$

de $K'[X]$. Montrer que f est une application φ-semi-linéaire de $K[X]$ dans $K'[X]$.

b) Démontrer que f est un homomorphisme d'anneaux de $K[X]$ dans $K'[X]$.

c) Si α est un élément de K qui est racine du polynôme P de $K[X]$, montrer que $\varphi(\alpha)$ est racine du polynôme $f(P)$ de $K'[X]$.

3) Posons $F = \mathscr{M}_n(K)$ (espace vectoriel et anneau des matrices carrées d'ordre n à coefficients dans K) et de la même manière $F' = \mathscr{M}_n(K')$.

a) Soit g l'application de F dans F' qui, à la matrice

$$A = (a_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}$$

de F fait correspondre la matrice

$$g(A) = (\varphi(a_{ij}))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}$$

de F'. Montrer que g est une application φ-semi-linéaire.

b) Démontrer que g est un homomorphisme d'anneaux de F dans F'.

Solution 1) *a*) Si h est linéaire, on a quels que soient les éléments x, y de E et λ de K, $h(x + y) = h(x) + h(y)$ et $h(\lambda x) = \lambda h(x) = (\mathrm{Id}\ K)(\lambda)\, h(x)$, donc h est Id K-semi-linéaire.

b) Si x, y sont des éléments de E et λ un élément de K, on a

$$g \circ f(x + y) = g(f(x) + f(y)) = g(f(x)) + g(f(y)) = g \circ f(x) + g \circ f(y)$$

et

$$g \circ f(\lambda x) = g(f(\lambda x)) = g(\varphi(\lambda) f(x)) = \\ = \psi(\varphi(\lambda))\, g(f(x)) = (\psi \circ \varphi)(\lambda)\, (g \circ f)(x)$$

donc $g \circ f$ est $(\psi \circ \varphi)$-semi-linéaire.

c) Soit f l'application de E dans E' définie comme suit : si x est un élément de E, x se met d'une manière et d'une seule sous la forme

$$x = \sum_{i=1}^{n} \lambda_i a_i$$

où $\lambda_1, \lambda_2, \ldots, \lambda_n$ sont des éléments de K et on pose

$$f(x) = \sum_{i=1}^{n} \varphi(\lambda_i) b_i .$$

Alors, f et φ-semi-linéaire ; en effet si x, y sont des éléments de E et λ un élément de K, si de plus x, y s'écrivent

$$x = \sum_{i=1}^{n} \lambda_i a_i , \quad y = \sum_{i=1}^{n} \mu_i a_i ,$$

on a

$$f(x + y) = \sum_{i=1}^{n} \varphi(\lambda_i + \mu_i) b_i = \sum_{i=1}^{n} (\varphi(\lambda_i) + \varphi(\mu_i)) b_i$$

$$= \sum_{i=1}^{n} \varphi(\lambda_i) b_i + \sum_{i=1}^{n} \varphi(\mu_i) b_i = f(x) + f(y)$$

et

$$f(\lambda x) = \sum_{i=1}^{n} \varphi(\lambda\lambda_i) b_i = \sum_{i=1}^{n} \varphi(\lambda) \varphi(\lambda_i) b_i = \varphi(\lambda) \sum_{i=1}^{n} \varphi(\lambda_i) b_i = \varphi(\lambda) f(x) .$$

Par ailleurs on a $f(a_i) = b_i$ pour $1 \leqslant i \leqslant n$. Je dis que f est la seule application φ-semi-linéaire de E dans E' qui possède cette propriété ; en effet, si f' est une application φ-semi-linéaire de E dans E' telle que $f'(a_i) = b_i$ pour $1 \leqslant i \leqslant n$, et si $x = \sum_{i=1}^{n} \lambda_i a_i$ est un élément de E, on a

$$f'(x) = f'\left(\sum_{i=1}^{n} \lambda_i a_i\right) = \sum_{i=1}^{n} f'(\lambda_i a_i) = \sum_{i=1}^{n} \varphi(\lambda_i) f'(a_i)$$

$$= \sum_{i=1}^{n} \varphi(\lambda_i) b_i = f(x) , \qquad \text{donc} \qquad f' = f .$$

d) Soit $(a_1, a_2, ..., a_n)$ une base de E. Supposons que f soit bijective et montrons que $(f(a_1), f(a_2), ..., f(a_n))$ est une base de E'. Soient $\lambda'_1, \lambda'_2, ..., \lambda'_n$ des éléments de K' tels que $\sum_{i=1}^{n} \lambda'_i f(a_i) = 0$; comme φ est surjective, il existe des éléments $\lambda_1, \lambda_2, ..., \lambda_n$ de K tels que $\varphi(\lambda_i) = \lambda'_i$ pour $1 \leqslant i \leqslant n$, et on a

$$\sum_{i=1}^{n} \varphi(\lambda_i) f(a_i) = 0$$

or

$$\sum_{i=1}^{n} \varphi(\lambda_i) f(a_i) = \sum_{i=1}^{n} f(\lambda_i a_i) = f\left(\sum_{i=1}^{n} \lambda_i a_i\right)$$

donc

$$f\left(\sum_{i=1}^{n} \lambda_i a_i\right) = 0$$

et comme f est bijective

$$\sum_{i=1}^{n} \lambda_i a_i = 0 ,$$

or $(a_1, a_2, ..., a_n)$ est une base de E donc $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$ et comme φ est un homomorphisme de corps $\lambda'_1 = \lambda'_2 = \cdots = \lambda'_n = 0$ donc les vecteurs $(a_1), f(a_2), ..., f(a_n)$ sont linéairement indépendants. Montrons que

$$(f(a_1), f(a_2), ..., f(a_n))$$

est un système générateur de E' ; soit y un élément de E', comme f est surjective il existe un élément x de E tel que $y = f(x)$, donc il existe des éléments $\lambda_1, \lambda_2, ..., \lambda_n$ de K tels que

$$x = \sum_{i=1}^{n} \lambda_i a_i ;$$

alors

$$y = f(x) = \sum_{i=1}^{n} \varphi(\lambda_i) f(a_i) ,$$

donc $(f(a_1), f(a_2), ..., f(a_n))$ est un système générateur donc une base de E'.

Réciproquement, supposons que $(f(a_1), f(a_2), ..., f(a_n))$ soit une base de E' ; montrons que f est surjective. Soit y un élément de E', alors il existe des éléments $\lambda'_1, \lambda'_2, ..., \lambda'_n$ de K' tels que

$$y = \sum_{i=1}^{n} \lambda'_i f(a_i) ;$$

comme φ est surjective, il existe des éléments $\lambda_1, \lambda_2, ..., \lambda_n$ de K tels que $\varphi(\lambda_i) = \lambda'_i$ pour $1 \leqslant i \leqslant n$ et on a

$$y = \sum_{i=1}^{n} \varphi(\lambda_i) f(a_i) = \sum_{i=1}^{n} f(\lambda_i a_i) = f\left(\sum_{i=1}^{n} \lambda_i a_i\right),$$

donc f est surjective.

Cherchons maintenant le noyau de f (considéré comme homomorphisme de groupes). Soit $x = \sum_{i=1}^{n} \lambda_i a_i$ un élément de E tel que $f(x) = 0$, alors on a

$$\sum_{i=1}^{n} \varphi(\lambda_i) f(a_i) = 0$$

et $(f(a_1), f(a_2), ..., f(a_n))$ est une base de E' donc $\varphi(\lambda_i) = 0$ pour $1 \leqslant i \leqslant n$, or φ est injectif, donc $\lambda_i = 0$ pour $1 \leqslant i \leqslant n$ par suite $x = 0$, $\operatorname{Ker} f = \{0\}$ et f est injective donc bijective.

2) *a*) Soient

$$P(X) = \sum_{i=1}^{n} \lambda_i X^i \qquad \text{et} \qquad Q(X) = \sum_{j=1}^{m} \mu_j X^j$$

deux éléments de $K[X]$ et λ un élément de K ; supposons par exemple que $m \leqslant n$, alors on a

$$P(X) + Q(X) = \sum_{i=0}^{m} (\lambda_i + \mu_i) X^i + \sum_{i=m+1}^{n} \lambda_i X^i$$

donc

$$f(P(X) + Q(X)) = \sum_{i=0}^{m} \varphi(\lambda_i + \mu_i) X^i + \sum_{i=m+1}^{n} \varphi(\lambda_i) X^i$$

$$= \sum_{i=0}^{m} (\varphi(\lambda_i) X^i + \varphi(\mu_i) X^i) + \sum_{i=m+1}^{n} \varphi(\lambda_i) X^i$$

$$= \sum_{i=0}^{n} \varphi(\lambda_i) X^i + \sum_{j=0}^{n} \varphi(\mu_j) X^j = f(P(X)) + f(Q(X))$$

et

$$f(\lambda . P(X)) = \sum_{i=0}^{n} \varphi(\lambda\lambda_i) X^i = \sum_{i=0}^{n} \varphi(\lambda) \varphi(\lambda_i) X^i$$

$$= \varphi(\lambda) \sum_{i=0}^{n} \varphi(\lambda_i) X^i = \varphi(\lambda) f(P(X)),$$

donc f est une application φ-semi-linéaire.

b) $P(X)$ et $Q(X)$ étant comme en (*a*), on a

$$P(X) . Q(X) = \sum_{i=0}^{m+n} v_i X^i \qquad \text{avec} \qquad v_i = \sum_{\substack{l+k=i \\ 1 \leqslant l \leqslant n \\ 1 \leqslant k \leqslant m}} \lambda_l \mu_k ,$$

donc

$$f(P(X) . Q(X)) = \sum_{i=0}^{m+n} \varphi(v_i) X^i , \qquad \text{or} \qquad \varphi(v_i) = \sum_{\substack{l+k=i \\ 1 \leqslant l \leqslant n \\ 1 \leqslant k \leqslant m}} \varphi(\lambda_l) \varphi(\mu_k)$$

donc

$$f(P(X) . Q(X)) = \left(\sum_{i=0}^{n} \varphi(\lambda_i) X^i \right) \left(\sum_{j=0}^{m} \varphi(\mu_j) X^j \right) = f(P(X)) f(Q(X)),$$

par suite f est un homomorphisme d'anneaux.

c) Si α est racine du polynôme $P(X) = \sum_{i=0}^{n} \lambda_i X^i$, on a

$$\sum_{i=0}^{n} \lambda_i \alpha^i = 0 \qquad \text{donc} \qquad \varphi \left(\sum_{i=0}^{n} \lambda_i \alpha^i \right) = 0$$

et comme φ est un homomorphisme de corps

$$\sum_{i=0}^{n} \varphi(\lambda_i) [\varphi(\alpha)]^i = 0$$

donc $\varphi(\alpha)$ est racine de $f(P(X))$.

3) *a*) Si

$$A = (a_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}, \quad B = (b_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}$$

sont deux éléments de F et λ un élément de K, on a

$$g(A + B) = (\varphi(a_{ij} + b_{ij}))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} = (\varphi(a_{ij}) + \varphi(b_{ij}))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}$$

$$= (\varphi(a_{ij}))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} + (\varphi(b_{ij}))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} = g(A) + g(B),$$

et

$$g(\lambda.A) = (\varphi(\lambda a_{ij}))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} = (\varphi(\lambda).\varphi(a_{ij}))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}$$

$$= \varphi(\lambda).(\varphi(a_{ij}))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} = \varphi(\lambda).g(A),$$

donc g est une application φ-semi-linéaire.

b) A et B étant comme en (*a*), on a

$$A.B = (c_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} \qquad \text{avec} \qquad c_{ij} = \sum_{k=1}^{n} a_{ik}\, b_{kj},$$

donc

$$g(A.B) = (\varphi(c_{ij}))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} = \left(\sum_{i=1}^{n} \varphi(a_{ik})\, \varphi(b_{kj})\right)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}$$

$$= \left[(\varphi(a_{ij}))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}\right] \cdot \left[\varphi(b_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}\right] = g(A).g(B),$$

donc g est un homomorphisme d'anneaux.

9.2 On note $\mathbf{Z}$ l'ensemble des entiers rationnels, $\mathbf{R}$ l'ensemble des nombres réels, $(e_1, e_2, ..., e_n)$ la base canonique de $\mathbf{R}^n$ $(n \geqslant 2)$. Soient $x = (x_1, x_2, ..., x_n)$ et $y = (y_1, y_2, ..., y_n)$ deux éléments de $\mathbf{R}^n$. On pose

$$f(x, y) = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n .$$

On considère $\mathbf{Z}^n$ comme sous-groupe du groupe additif $\mathbf{R}^n$.

1) Soit Φ l'homomorphisme canonique de $\mathbf{Z}$ sur $\mathbf{Z}/2\,\mathbf{Z}$.
Si $x = (x_1, x_2, ..., x_n)$ est un élément de $\mathbf{Z}^n$, on pose

$$\theta(x) = \Phi(x_1 + x_2 + \cdots + x_n).$$

Montrer que θ est un homomorphisme de $\mathbf{Z}^n$ sur $\mathbf{Z}/2\,\mathbf{Z}$. Déterminer son noyau K et son image. Quel est le nombre d'éléments du groupe $\mathbf{Z}^n/K$?

2) Montrer que K est l'ensemble des éléments x de $\mathbf{Z}^n$ tels que $f(x, x)$ soit pair, et aussi le sous-groupe de $\mathbf{Z}^n$ engendré par les vecteurs

$$e_i - e_n,\ e_i + e_n \qquad (1 \leqslant i \leqslant n - 1).$$

3) Soit S l'ensemble des éléments x de $\mathbf{Z}^n$ tels que $f(x, x) = 1$ ou $f(x, x) = 2$. Déterminer les éléments de S et leur nombre.

4) On pose

$$a_1 = e_1 - e_2\,,\ a_2 = e_2 - e_3,\ \ldots,\ a_{n-1} = e_{n-1} - e_n\,,\ a_n = e_n\,.$$

Montrer que les vecteurs a_i $(1 \leqslant i \leqslant n)$ forment une base de $\mathbf{R}^n$. Etant donné un élément $(x_1, x_2, \ldots, x_n)$ de $\mathbf{R}^n$, calculer ses coordonnées par rapport à la base $(a_1, a_2, \ldots, a_n)$. Exprimer les éléments de S comme combinaison linéaire des vecteurs a_i $(1 \leqslant i \leqslant n)$.

5) Soit V le sous-espace vectoriel de $\mathbf{R}^n$ de base $(a_1, a_2, \ldots, a_{n-1})$. Quelle relation vérifient les coordonnées d'un vecteur x de V par rapport à la base $(e_1, e_2, \ldots, e_n)$?

On pose $T = S \cap V$. Déterminer les éléments de T et leur nombre. Calculer $f(x, x)$ pour un élément de T. On pose $a'_n = e_1 + e_2 + \cdots + e_n$, montrer que V est l'ensemble des éléments x de $\mathbf{R}^n$ tels que $f(x, a'_n) = 0$.

Montrer que $(a_1, a_2, \ldots, a_{n-1}, a'_n)$ est une base de $\mathbf{R}^n$.

6) Soit i un entier tel que $1 \leqslant i \leqslant n - 1$. Montrer qu'il existe un vecteur b_i de $\mathbf{R}^n$, et un seul, tel que

(1) $f(b_i, a_j) = \delta_{ij}$ pour $1 \leqslant j \leqslant n - 1$, et

(2) $f(b_i, a'_n) = 0$.

On déterminera b_i par ses coordonnées relativement à la base $(e_1, e_2, \ldots, e_n)$.

7) Montrer en utilisant (1) et (2) que $b_1, b_2, \ldots, b_{n-1}$ sont linéairement indépendants et forment une base de V. Exprimer les b_i comme combinaisons linéaires des a_j. Pour $n = 4$, calculer la matrice de passage M de la base $(a_1, a_2, \ldots, a_{n-1})$ à la base $(b_1, b_2, \ldots, b_{n-1})$.

Solution 1) Soient $x = (x_1, x_2, \ldots, x_n)$ et $y = (y_1, y_2, \ldots, y_n)$ deux éléments de $\mathbf{Z}^n$; alors

$$x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)\,,$$

par suite

$$\theta(x + y) = \Phi\big((x_1 + y_1) + (x_2 + y_2) + \cdots + (x_n + y_n)\big)\,;$$

l'addition dans $\mathbf{Z}$ est commutative, associative et Φ est un homomorphisme, donc on a

$$\theta(x + y) = \Phi(x_1 + x_2 + \cdots + x_n) + \Phi(y_1 + y_2 + \cdots + y_n) = \theta(x) + \theta(y)\,.$$

$\mathbf{Z}/2\,\mathbf{Z}$ a deux éléments $\bar{0}$ et $\bar{1}$ qui sont images d'au moins deux éléments de $\mathbf{Z}^n$; en effet $\theta(0, 0, \ldots, 0) = \bar{0}$ et $\theta(1, 0, 0, \ldots, 0) = \bar{1}$, par suite θ est un homomor-

phisme surjectif de $\mathbf{Z}^n$ sur $\mathbf{Z}/2\,\mathbf{Z}$. Son noyau K est l'ensemble des éléments $(x_1, x_2, ..., x_n)$ de $\mathbf{Z}^n$ tels que $x_1 + x_2 + \cdots + x_n$ soit pair. La décomposition canonique de θ prouve que $\mathbf{Z}^n/K$ est isomorphe à $\mathbf{Z}/2\,\mathbf{Z}$ donc a deux éléments.

2) Soit $x = (x_1, x_2, ..., x_n)$ un élément de $\mathbf{Z}^n$; alors

$$f(x, x) = x_1^2 + x_2^2 + \cdots + x_n^2 .$$

Si a est un élément de $\mathbf{Z}$, le nombre $a^2 - a = a(a-1)$ est pair donc a^2 et a sont de même parité. Or on sait (1) qu'un élément $x = (x_1, x_2, ..., x_n)$ de $\mathbf{Z}^n$ est dans K si et seulement si $x_1 + x_2 + \cdots + x_n$ est pair ; en vertu de la remarque précédente cela revient à dire que $f(x, x)$ est pair.

Soit K' le sous-groupe de $\mathbf{Z}^n$ engendré par les vecteurs

$$e_i - e_n\,,\ e_i + e_n\ (1 \leqslant i \leqslant n-1)\,.$$

On a $f(e_i - e_n, e_i - e_n) = 2$ et $f(e_i + e_n, e_i + e_n) = 2$ $(1 \leqslant i \leqslant n-1)$ donc les vecteurs $e_i - e_n$, $e_i + e_n$ $(1 \leqslant i \leqslant n-1)$ appartiennent à K et il s'ensuit que $K' \subset K$. Soit $x = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n$ un élément de K ; on a

$$x_1 + x_2 + \cdots + x_n = 2s$$

ou s est un élément de $\mathbf{Z}$ et

$$x = x_1(e_1 - e_n) + x_2(e_2 - e_n) + \cdots + x_{n-1}(e_{n-1} - e_n) + 2se_n =$$
$$= x_1(e_1 - e_n) + x_2(e_2 - e_n) + \cdots + x_{n-1}(e_{n-1} - e_n) + s(e_1 + e_n) - s(e_1 - e_n)\,,$$

donc x appartient à K' et $K' = K$.

3) Si $x = (x_1, x_2, ..., x_n)$ est un élément de $\mathbf{Z}^n$, on a

$$f(x, x) = x_1^2 + x_2^2 + \cdots + x_n^2\ ;$$

$x_i\,(1 \leqslant i \leqslant n)$ étant un élément de $\mathbf{Z}$, x_i^2 est supérieur ou égal à 1 s'il n'est pas nul ; donc, pour que $f(x, x) = 1$ il faut et suffit qu'un des x_i et un seul soit égal à $+1$ ou -1, les autres étant nuls. Les éléments x de $\mathbf{Z}^n$ tels que $f(x, x) = 1$ sont donc les vecteurs $e_i\,(1 \leqslant i \leqslant n)$ et les vecteurs $(-e_i)\,(1 \leqslant i \leqslant n)$. Leur nombre est $2n$. Pour que $f(x, x) = 2$ il faut et suffit que deux coordonnées distinctes de x soient égales à 1 ou -1, les autres étant nulles. Les vecteurs x de $\mathbf{Z}^n$ tels que $f(x, x) = 2$ sont donc les vecteurs $e_i + e_j$, $e_i - e_j$, $-e_i + e_j$, $-e_i - e_j$ avec $1 \leqslant i < j \leqslant n$. Leur nombre est donc

$$4\,C_n^2 = 2\,n(n-1) = 2\,n^2 - 2\,n\,.$$

Par suite le nombre d'éléments de S est $2n^2$.

4) On a $e_n = a_n$, $e_{n-1} = a_{n-1} + a_n$, ..., $e_1 = a_1 + a_2 + \cdots + a_n$. Par suite $(a_1, a_2, ..., a_n)$ est un système générateur de $\mathbf{R}^n$. Comme il est minimal, $(a_1, a_2, ..., a_n)$ est une base de $\mathbf{R}^n$. Si $x = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n$ est un élément de $\mathbf{R}^n$, on a

$$x = x_1(a_1 + a_2 + \cdots + a_n) + x_2(a_2 + a_3 + \cdots + a_n) + \cdots +$$
$$+ x_{n-1}(a_{n-1} + a_n) + x_n a_n$$

donc

$$x = x_1 a_1 + (x_1 + x_2) a_2 + \cdots + (x_1 + x_2 + \cdots + x_{n-1}) a_{n-1} + \\ + (x_1 + x_2 + \cdots + x_n) a_n .$$

Les coordonnées $\alpha_1, \alpha_2, \ldots, \alpha_n$ de x par rapport à la base $(a_1, a_2, \ldots, a_n)$ sont donc

$$\alpha_1 = x_1 , \alpha_2 = x_1 + x_2, \ldots, \alpha_{n-1} = x_1 + x_2 + \cdots + x_{n-1} , \\ \alpha_n = x_1 + x_2 + \cdots + x_n .$$

Les vecteurs de S sont les vecteurs

$$e_i (1 \leqslant i \leqslant n) , \quad - e_i (1 \leqslant i \leqslant n) , \quad \varepsilon_i e_i - \varepsilon_j e_j \\ (1 \leqslant i < j \leqslant n, \quad \varepsilon_i^2 = 1, \quad \varepsilon_j^2 = 1) .$$

Nous avons déjà exprimé les vecteurs $e_i (1 \leqslant i \leqslant n)$ comme combinaison linéaire des $a_i (1 \leqslant i \leqslant n)$ donc aussi les vecteurs $(- e_i)$ $(1 \leqslant i \leqslant n)$. On a

$$\varepsilon_i e_i - \varepsilon_j e_j = \varepsilon_i (a_i + a_{i+1} + \cdots + a_{j-1}) + (\varepsilon_i - \varepsilon_j) (a_j + \cdots + a_n) .$$

5) V est le sous-ensemble des vecteurs $(x_1, x_2, \ldots, x_n)$ de $\mathbf{R}^n$ tels que

$$\alpha_n = x_1 + x_2 + \cdots + x_n = 0 .$$

Parmi les vecteurs de S, ceux qui appartiennent à V sont ceux dont deux coordonnées sont opposées, les autres étant nulles. Ce sont donc les vecteurs $e_i - e_j$ et $e_j - e_i$ avec $1 \leqslant i < j \leqslant n$. Leur nombre est $2\, C_n^2 = n^2 - n$. Si x est un élément de T on a $f(x, x) = 2$. Soit $x = (x_1, x_2, \ldots, x_n)$ un élément de $\mathbf{R}^n$; on a $f(x, a_n') = x_1 + x_2 + \cdots + x_n$; V est donc l'ensemble des éléments x de $\mathbf{R}^n$ tels que $f(x, a_n') = 0$. Comme $f(a_n', a_n') = n$, a_n' n'appartient pas à V $(a_1, a_2, \ldots, a_{n-1}, a_n')$ est un système libre, il est maximal, c'est donc une base de $\mathbf{R}^n$.

6) Posons $b_i = (x_1, x_2, \ldots, x_n)$. Les conditions (1) et (2) se traduisent par

$$x_1 - x_2 = x_2 - x_3 = \cdots = x_{i-1} - x_i = 0 , x_i - x_{i+1} = 1 , \\ x_{i+1} - x_{i+2} = x_{i+2} - x_{i+3} = \cdots = x_{n-1} - x_n = 0$$

et

$$x_1 + x_2 + \cdots + x_n = 0 .$$

Soit encore par

$$x_1 = x_2 = x_3 = \cdots = x_i = 1 + x_{i+1} , x_{i+1} = x_{i+2} = \cdots = x_n ,$$

avec $i x_1 + (n - i) (x_1 - 1) = 0$, par suite

$$x_1 = \frac{n - i}{n} = 1 - \frac{i}{n}$$

et finalement

$$b_i = \left(1 - \frac{i}{n}\right)(e_1 + e_2 + \cdots + e_i) - \frac{i}{n}(e_{i+1} + \cdots + e_n).$$

7) Soient $\lambda_1, \lambda_2, \ldots, \lambda_{n-1}$ des éléments de $\mathbf{R}$ tels que

$$\lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_{n-1} b_{n-1} = 0 ;$$

alors on a pour $1 \leqslant j \leqslant n-1$, $f(\lambda_1 b_1 + \cdots + \lambda_{n-1} b_{n-1}, a_j) = 0$ car le vecteur $\lambda_1 b_1 + \cdots + \lambda_{n-1} b_{n-1}$ est nul ; par ailleurs,

$$f(\lambda_1 b_1 + \cdots + \lambda_{n-1} b_{n-1}, a_j) = \lambda_j$$

d'après les formules (1) et (2), donc les éléments $\lambda_j (1 \leqslant j \leqslant n-1)$ de $\mathbf{R}$ sont tous nuls et les vecteurs $b_1, b_2, \ldots, b_{n-1}$ sont linéairement indépendants. D'après (2) ils appartiennent à V ; comme V est de dimension $n-1$, ils forment une base de V. D'après les formules de (4) on a

$$e_1 + e_2 + \cdots + e_i = a_1 + 2a_2 + 3a_3 + \cdots + ia_i + i(a_{i+1} + \cdots + a_n)$$
$$e_{i+1} + \cdots + e_n = a_{i+1} + 2a_{i+2} + \cdots + (n-i)a_i ,$$

et par suite en utilisant (5) on obtient

$$b_i = \left(1 - \frac{i}{n}\right)a_1 + 2\left(1 - \frac{i}{n}\right)a_2 + \cdots + i\left(1 - \frac{i}{n}\right)a_i + i\left(1 - \frac{i+1}{n}\right)a_{i+1} +$$
$$+ i\left(1 - \frac{i+2}{n}\right)a_{i+2} + \cdots + i\left(1 - \frac{n-1}{n}\right)a_{n-1} .$$

Pour $n = 4$ on obtient

$$b_1 = \tfrac{3}{4}a_1 + \tfrac{1}{2}a_2 + \tfrac{1}{4}a_3$$
$$b_2 = \tfrac{1}{2}a_1 + a_2 + \tfrac{1}{2}a_3$$
$$b_3 = \tfrac{1}{4}a_1 + \tfrac{1}{2}a_2 + \tfrac{3}{4}a_3$$

et par suite, la matrice M est

$$M = \begin{pmatrix} \frac{3}{4} & \frac{1}{2} & \frac{1}{4} \\ \frac{1}{2} & 1 & \frac{1}{2} \\ \frac{1}{4} & \frac{1}{2} & \frac{3}{4} \end{pmatrix}.$$

9.3

Soient K un corps commutatif et n un entier tel que $n > 2$. Soit P_n l'espace vectoriel des polynômes à une indéterminée X, à coefficients dans K, de degré strictement inférieur à n. Soient α et β deux éléments distincts de K.

1) Quelle est la dimension de P_n ?

2) *a*) Montrer que les trois sous-ensembles suivants constituent des sous-espaces vectoriels de P_n :

E_α : ensemble des polynômes de P_n possédant la racine α,
E_β : ensemble des polynômes de P_n possédant la racine β,
E : ensemble des polynômes de P_n possédant les racines α et β.

b) Démontrer que les polynômes

$$(X - \alpha),\ X(X - \alpha),\ X^2(X - \alpha),\ \ldots,\ X^{n-2}(X - \alpha)\,,$$

forment une base de E_α.

c) Démontrer que les polynômes

$$(X - \alpha)(X - \beta)\,;\ X(X - \alpha)(X - \beta)\,;\ \ldots\,;\ X^{n-3}(X - \alpha)(X - \beta)$$

forment une base de E.

3) Soit u l'application de P_n dans lui-même définie en posant pour chaque polynôme P de P_n,

$$[u(P)](X) = P(\alpha)\,X + P(\beta)\,.$$

a) Montrer que u est linéaire.

b) Déterminer le noyau de u.

c) Démontrer que $u(P_n)$ est le sous-espace de P_n formé par les polynômes de degré inférieur ou égal à 1.

4) Démontrer qu'il existe des éléments λ, μ de K tels que

$$\lambda(X - \alpha) + \mu(X - \beta) = 1\,.$$

En déduire que $E_\alpha + E_\beta = P_n$.

Vérifier la relation

$$\dim E_\alpha + \dim E_\beta = \dim (E_\alpha + E_\beta) + \dim (E_\alpha \cap E_\beta).$$

Solution 1) La famille $(1, X, X^2, \ldots, X^{n-1})$ est une famille libre de P_n (*cf.* Q. Ch. 11, § II, n° 187) et engendre P_n ; c'est donc une base de P_n, par suite P_n est de dimension n sur K.

2) *a*) Soient P, Q deux éléments de E_α et λ, μ deux éléments de K ; alors on a $P(\alpha) = Q(\alpha) = 0$ donc $(\lambda P + \mu Q)(\alpha) = \lambda P(\alpha) + \mu Q(\alpha) = 0$ par suite $\lambda P + \mu Q$ appartient à E_α donc E_α est un sous-espace vectoriel de P_n. On démontre de la même manière que E_β est un sous-espace vectoriel de P_n ; de plus, il est clair que $E = E_\alpha \cap E_\beta$ donc E est aussi un sous-espace vectoriel de P_n.

b) Il est clair que les polynômes $(X - \alpha)$; $X(X - \alpha)$; ... ; $X^{n-2}(X - \alpha)$, sont des éléments de E_α. Comme ces polynômes ont des degrés distincts deux à deux, ils forment une famille libre de E_α (*cf.* Q., Ch. 11, § II, n° 187). Le sous-espace E_α est contenu strictement dans P_n donc $\dim E_\alpha \leqslant n - 1$; comme nous venons de trouver $n - 1$ éléments de E_α linéairement indépendants,

$$\dim E_\alpha \geqslant n - 1 ,$$

donc $\dim E_\alpha = n - 1$ et la famille donnée est une base de E_α.

c) Les degrés des polynômes

$$(X - \alpha)(X - \beta) ; X(X - \alpha)(X - \beta) ; \ldots ; X^{n-3}(X - \alpha)(X - \beta)$$

sont deux à deux distincts donc (*cf.* Q., Ch. 11, § II, n° 187) ces polynômes forment une famille libre. Il est clair qu'ils appartiennent tous à E, donc $\dim E \geqslant n - 2$. Or E est un sous-espace strictement contenu dans E_α (par exemple $(X - \alpha)$ appartient à E_α et non à E) donc $\dim E \leqslant n - 2$ par suite $\dim E = n - 2$ et la famille de polynômes ci-dessus est une base de E.

3) *a*) Soient P, Q deux éléments de P_n et λ, μ deux éléments de K ; alors on a

$$\begin{aligned}[u(\lambda P + \mu Q)](X) &= (\lambda P + \mu Q)(\alpha) X + (\lambda P + \mu Q)(\beta) \\ &= (\lambda P)(\alpha) X + (\mu Q)(\alpha) X + \lambda P(\beta) + \mu Q(\beta) \\ &= \lambda[P(\alpha) X + P(\beta)] + \mu[Q(\alpha) X + Q(\beta)] \\ &= \lambda[u(P)](X) + \mu[u(Q)](X)\end{aligned}$$

donc u est linéaire.

b) Un polynôme P de P_n appartient au noyau $\operatorname{Ker} u$ de u si et seulement si $[u(P)](X) = P(\alpha) X + P(\beta) = 0$ c'est-à-dire si et seulement si

$$P(\alpha) = P(\beta) = 0 ;$$

donc $\operatorname{Ker} u = E$.

c) Il est clair que tout élément de $u(P_n)$ est de degré inférieur ou égal à 1. Réciproquement, soit $\lambda X + \mu$ un polynôme de P_n de degré inférieur ou égal à 1, cherchons un polynôme P de P_n tel que $[u(P)](X) = \lambda X + \mu$; il suffit de déterminer P tel que $P(\alpha) = \lambda$ et $P(\beta) = \mu$; le polynôme

$$P(X) = \lambda \frac{(X - \beta)}{\alpha - \beta} + \mu \frac{(X - \alpha)}{\beta - \alpha} ,$$

par exemple, satisfait à la question, donc $u(P_n)$ est formé de tous les polynômes de P_n dont le degré est inférieur ou égal à 1.

4) Les polynômes $(X - \alpha)$ et $(X - \beta)$ de P_n sont évidemment premiers entre eux, donc le théorème de BEZOUT permet d'affirmer qu'il existe deux éléments λ, μ de K tels que $\lambda(X - \alpha) + \mu(X - \beta) = 1$. Par ailleurs, on peut aisément calculer λ et μ ; il suffit pour cela de résoudre le système

$$\begin{cases} \lambda + \mu = 0 \\ \lambda\alpha + \mu\beta = -1 \end{cases}$$

et on trouve

$$\lambda = \frac{1}{\beta - \alpha}, \quad \mu = \frac{1}{\alpha - \beta}.$$

L'égalité que nous venons de démontrer, prouve que 1 appartient à

$$E_\alpha + E_\beta ;$$

il en est donc de même de tous les éléments de K. Par ailleurs si $0 < k \leqslant n - 1$, on vérifie facilement l'égalité

$$X^k = (X - \alpha)(X^{k-1} + \alpha X^{k-2} + \cdots + \alpha^{k-2} X + \alpha^{k-1}) + \alpha^k .$$

Or α^k est un élément de $E_\alpha + E_\beta$ et $(X - \alpha)(X^{k-1} + \alpha X^{k-2} + \cdots + \alpha^{k-1})$ appartient à E_α donc à $E_\alpha + E_\beta$, par suite X^k appartient à $E_\alpha + E_\beta$, donc $E_\alpha + E_\beta$ contient la base $(1, X, X^2, ..., X^{n-1})$ de P_n, par suite $E_\alpha + E_\beta = P_n$.

On a

$$\dim E_\alpha = \dim E_\beta = n - 1 \; ; E_\alpha \cap E_\beta = E, \dim E = n - 2$$

et

$$E_\alpha + E_\beta = P_n \quad \text{donc} \quad \dim (E_\alpha + E_\beta) = n ,$$

par suite on a bien

$$\dim E_\alpha + \dim E_\beta = \dim (E_\alpha + E_\beta) + \dim (E_\alpha \cap E_\beta) .$$

9.4 Dans ce qui suit nous désignerons par $\mathscr{F}(\mathbf{N}, \mathbf{C})$ l'espace vectoriel (sur $\mathbf{C}$) des fonctions définies sur $\mathbf{N}$ à valeurs dans $\mathbf{C}$; par $\mathbf{C}[X]$ l'espace vectoriel (sur $\mathbf{C}$) des polynômes à une indéterminée X et à coefficients complexes ; pour chaque entier $n \geqslant 0$, nous noterons $\mathbf{C}_n[X]$ le sous-espace vectoriel de $\mathbf{C}[X]$ formé des polynômes de degré inférieur ou égal à n, et du polynôme nul.

I. 1) Pour chaque entier $k \geqslant 1$, on pose

$$\{ X \}^k = X(X - 1). .... (X - k + 1)$$

et $\{ X \}^0 = 1$. Montrer que pour chaque entier $n \geqslant 1$, les polynômes

$$\{ X \}^0, \{ X \}^1, ..., \{ X \}^n$$

forment une base de $\mathbf{C}_n[X]$.

2) Soit Δ l'application définie sur $\mathbf{C}[X]$ à valeurs dans $\mathbf{C}[X]$ qui associe à chaque polynôme P de $\mathbf{C}[X]$ le polynôme ΔP défini par

$$(\Delta P)(X) = P(X + 1) - P(X) .$$

a) Montrer que Δ est un endomorphisme de $\mathbf{C}[X]$.

b) Montrer que pour tout entier $k > 0$, on a

$$\Delta \{ X \}^k = k \{ X \}^{k-1} .$$

c) Montrer que pour tout entier $n > 0$, on a

$$\Delta(\mathbf{C}_n[X]) = \mathbf{C}_{n-1}[X] .$$

d) Déterminer le noyau de Δ.

3) On pose $\Delta^2 = \Delta \circ \Delta$, $\Delta^3 = \Delta \circ \Delta^2$, et pour tout entier $h \geqslant 1$,

$$\Delta^{h+1} = \Delta \circ \Delta^h .$$

Montrer que si P est un polynôme de degré n, alors : $\Delta^n P \neq 0$, $\Delta^{n+1} P = 0$ et

$$P(X) = P(0) + \frac{(\Delta P)(0)}{1!} \{ X \} + \frac{(\Delta^2 P)(0)}{2!} \{ X \}^2 + \cdots + \frac{(\Delta^n P)(0)}{n!} \{ X \}^n .$$

II. 1) On désigne par D l'application définie sur $\mathscr{F}(\mathbf{N}, \mathbf{C})$ à valeurs dans $\mathscr{F}(\mathbf{N}, \mathbf{C})$ qui associe à chaque fonction f de $\mathscr{F}(\mathbf{N}, \mathbf{C})$ la fonction Df définie en posant pour tout entier n, $(Df)(n) = f(n + 1) - f(n)$.

a) Montrer que D est un endomorphisme de $\mathscr{F}(\mathbf{N}, \mathbf{C})$.

b) Déterminer le noyau de D.

2) *a*) On pose $D^2 = D \circ D$, $D^3 = D \circ D^2$ et pour tout entier $h \geqslant 1$, $D^{h+1} = D \circ D^h$. Montrer que si la fonction f est une fonction polynôme de N dans C, de degré r (c'est-à-dire, s'il existe des nombres complexes $a_0, a_1, \ldots, a_r$ tels que $a_r \neq 0$, et $f(n) = a_0 + a_1 n + \cdots + a_r n^r$ pour tout élément n de N) alors on a $D^r f \neq 0$, $D^{r+1} f = 0$.

b) Réciproquement montrer que si f est un élément de $\mathscr{F}(\mathbf{N}, \mathbf{C})$ tel que $D^r f \neq 0$ et $D^{r+1} f = 0$, alors f est une fonction polynôme de degré r, de N dans C.

III. Les notations étant celles de II, soit f une fonction polynôme de N dans C, de degré $(r - 1)$. Montrer qu'il existe une fonction polynôme g de N dans C et une seule, de degré r, telle que l'on ait $Dg = f$ et $g(0) = 0$. En déduire une expression simple de la somme $f(0) + f(1) + \cdots + f(n)$.

Application. Calculer les sommes suivantes :

$$A = 1^2 + 2^2 + \cdots + n^2$$
$$B = 1^3 + 2^3 + \cdots + n^3$$
$$C = 1^2 + 3^2 + \cdots + (2n - 1)^2$$
$$D = 1.2 + 2.3 + \cdots + n(n + 1) .$$

Solution I. 1) Pour chaque entier $k \geqslant 0$, $\{X\}^k$ est un polynôme de degré k donc $\{X\}^0, \{X\}^1, \ldots, \{X\}^n$ forment une famille libre de $\mathbf{C}_n[X]$ (*cf.* Q., Ch. 12, § II, n° 187) qui est de dimension $n+1$, donc ces polynômes forment une base de $\mathbf{C}_n[X]$.

2) *a*) Si P, Q sont deux polynômes de $\mathbf{C}[X]$ et λ, μ deux nombres complexes, on a

$$[\Delta(\lambda P + \mu Q)](X) = (\lambda P + \mu Q)(X+1) - (\lambda P + \mu Q)(X) =$$
$$= \lambda[P(X+1) - P(X)] + \mu[Q(X+1) - Q(X)] = \lambda(\Delta P)(X) + \mu(\Delta Q)(X)$$

par suite Δ est bien un endomorphisme de $\mathbf{C}[X]$.

b) Si $k \geqslant 1$, on a $\{X\}^k = X(X-1).\ldots.(X-k+1)$ donc

$$\begin{aligned}\Delta\{X\}^k &= \{X+1\}^k - \{X\}^k \\ &= (X+1)(X)(X-1).\ldots.(X-k+2) - X(X-1).\ldots.(X-k+1) \\ &= X(X-1).\ldots.(X-k+2)[(X+1) - (X-k+1)] \\ &= kX(X-1).\ldots.(X-k+2) = k\{X\}^{k-1}.\end{aligned}$$

c) Si P est un élément de $\mathbf{C}_n[X]$, d'après (1) il existe une famille $a_0, a_1, \ldots, a_n$ d'éléments de $\mathbf{C}$ tels que

$$P(X) = a_n\{X\}^n + a_{n-1}\{X\}^{n-1} + \cdots + a_1\{X\} + a_0\{X\}^0.$$

D'après (*a*) on a

$$(\Delta P)(X) = \Delta(a_n\{X\}^n + \cdots + a_1\{X\} + a_0\{X\}^0) =$$
$$= a_n\Delta\{X\}^n + a_{n-1}\Delta\{X\}^{n-1} + \cdots + a_1\Delta\{X\} + a_0\Delta\{X\}^0 :$$

or d'après (*b*) on a

$$\Delta\{X\}^k = k\{X\}^{k-1} \quad \text{si} \quad k \geqslant 1$$

et il est clair que

$$\Delta\{X\}^0 = 0, \quad \text{donc} \quad (\Delta P)(X) = na_n\{X\}^{n-1} + \cdots + 2a_2\{X\} + a_1$$

donc ΔP appartient à $\mathbf{C}_{n-1}[X]$ et par suite $\Delta(\mathbf{C}_n[X]) \subset \mathbf{C}_{n-1}[X]$. D'autre part, observons que si $k \geqslant 1$, on a

$$\{X\}^{k-1} = \frac{\Delta\{X\}^k}{k}$$

donc si

$$Q(X) = b_{n-1}\{X\}^{n-1} + \cdots + b_1\{X\}^1 + b_0$$

est un polynôme de $\mathbf{C}_{n-1}[X]$ on a $Q = \Delta P$ avec

$$P(X) = \frac{b_{n-1}}{n}\{X\}^n + \frac{b_{n-2}}{n-1}\{X\}^{n-1} + \cdots + b_0\{X\}$$

donc $\mathbf{C}_{n-1}[X] \subset \Delta(\mathbf{C}_n[X])$ par suite $\Delta(\mathbf{C}_n[X]) = \mathbf{C}_{n-1}[X]$.

d) Remarquons que si P est un polynôme de degré n ($n \geqslant 1$) et si

$$P(X) = a_n \{ X \}^n + \cdots + a_1 \{ X \} + a_0 ,$$

avec $a_n \neq 0$, alors $(\Delta P)(X) = n a_n \{ X \}^{n-1} + \cdots + a_1$ est de degré $(n-1)$ exactement ; par suite le noyau de Δ ne peut contenir aucun polynôme de degré supérieur ou égal à 1. Les polynômes de degré 0 sont les éléments de

$$\mathbf{C} = \mathbf{C}_0[X]$$

et il est clair que si P appartient à $\mathbf{C}_0[X]$ on a $\Delta P = 0$ donc

$$\operatorname{Ker} \Delta = \mathbf{C}_0[X] = \mathbf{C} .$$

3) Posons $P(X) = a_n \{ X \}^n + a_{n-1} \{ X \}^{n-1} + \cdots + a_1 \{ X \} + a_0$ ($a_n \neq 0$). Alors on a

$$(\Delta P)(X) = n a_n \{ X \}^{n-1} + (n-1) a_{n-1} \{ X \}^{n-2} + \cdots + a_1 ;$$
$$(\Delta^2 P)(X) = n(n-1) a_n \{ X \}^{n-2} + (n-1)(n-2) a_{n-1} \{ X \}^{n-3} + \cdots + 2a_2 ,$$

et par récurrence sur k on voit que pour tout entier k tel que $1 \leqslant k \leqslant n$, on a

$$(\Delta^k P)(X) = n(n-1), \ldots, (n-k+1) a_n \{ X \}^{n-k} + \cdots + k ! \, a_k .$$

En particulier on a $(\Delta^n P)(X) = n ! \, a_n$ donc $\Delta^n P \neq 0$ et

$$\Delta^{n+1} P = \Delta(\Delta^n P) = 0$$

d'après (2, *d*). De plus on a $(\Delta^k P)(0) = k ! \, a_k$ pour $1 \leqslant k \leqslant n$ donc

$$P(X) = P(0) + \frac{(\Delta P)(0)}{1 !} \{ X \} + \frac{(\Delta^2 P)(0)}{2 !} \{ X \}^2 + \cdots + \frac{(\Delta^n P)(0)}{n !} \{ X \}^n .$$

Cette identité, connue sous le nom d'identité de GRÉGORY, permet de calculer les coordonnées d'un polynôme P de $\mathbf{C}_n[X]$ par rapport à la base $\{ X \}^0, \{ X \}, \ldots, \{ X \}^n$, de la même manière que la formule de TAYLOR permet de calculer ses coordonnées par rapport à la base $1, X, X^2, \ldots, X^n$.

II. 1) *a*) Si f et g appartiennent à $\mathscr{F}(\mathbf{N}, \mathbf{C})$ et si λ, μ sont deux nombres complexes, on a pour tout entier naturel n,

$$D(\lambda f + \mu g)(n) = (\lambda f + \mu g)(n+1) - (\lambda f + \mu g)(n) =$$
$$= \lambda [f(n+1) - f(n)] + \mu [g(n+1) - g(n)] = \lambda Df(n) + \mu Dg(n),$$

donc

$$D(\lambda f + \mu g) = \lambda Df + \mu Dg ,$$

par suite D est un endomorphisme de $\mathscr{F}(\mathbf{N}, \mathbf{C})$.

b) Une fonction f de $\mathscr{F}(\mathbf{N}, \mathbf{C})$ appartient au noyau de D si et seulement si l'on a $Df = 0$ c'est-à-dire si et seulement si l'on a pour tout entier naturel n, $Df(n) = f(n+1) - f(n) = 0$. $\operatorname{Ker} D$ est donc l'ensemble des fonctions constantes de N dans C.

2) *a*) Soit f un élément de $\mathscr{F}(\mathbf{N}, \mathbf{C})$. Supposons que f soit une fonction polynôme de degré r, de N dans C ; alors, il existe des nombres complexes $a_0, a_1, \ldots, a_r$ tels que $a_r \neq 0$ et

$$f(n) = a_0 + a_1 n + a_2 n^2 + \cdots + a_r n^r$$

pour tout entier naturel n. Soit P le polynôme de $\mathbf{C}_r[X]$ défini par

$$P(X) = a_r X^r + a_{r-1} X^{r-1} + \cdots + a_1 X + a_0 ;$$

alors on a, d'après (I.3), $\Delta^r P \neq 0$ et $\Delta^{r+1} P = 0$. Or, f est la restriction à N de la fonction polynôme $\widetilde{P}$ de C dans C, associée à P (*cf.* Q., Ch. 11, § I, n° 185) et on a $\Delta P(X) = P(X + 1) - P(X)$, donc $(\widetilde{\Delta P})(z) = \widetilde{P}(z + 1) - \widetilde{P}(z)$ pour tout nombre complexe z et en particulier $(\widetilde{\Delta P})(n) = (Df)(n)$ pour tout entier naturel n. Df est donc la restriction à N de $\widetilde{\Delta P}$ et on voit par récurrence sur k que $D^k f$ est la restriction à N de $\widetilde{\Delta^k P}$. Mais nous savons que $\Delta^r P \neq 0$ et $\Delta^{r+1} P = 0$ donc $D^{r+1} f = 0$ et comme N est infini la restriction de la fonction polynôme $\Delta^r P$ à N ne peut être identiquement nulle, donc $D^r f \neq 0$.

b) Nous procéderons par récurrence sur r. Si f appartient à $\mathscr{F}(\mathbf{N}, \mathbf{C})$ et si l'on a $Df \neq 0$ et $D^2 f = 0$, alors d'après (1, *b*), Df est une fonction constante : soit a sa valeur ; alors on a pour tout entier naturel n, $f(n + 1) - f(n) = a$ donc $\big(f(n) - f(n-1)\big) + \big(f(n-1) - f(n-2)\big) + \cdots + \big(f(1) - f(0)\big) = na$ soit $f(n) = na + f(0)$, si bien que f est une fonction polynôme de degré 1 de N dans C. Supposons à présent le résultat démontré pour $r - 1$ et soit f un élément de $\mathscr{F}(\mathbf{N}, \mathbf{C})$ tel que $D^r f \neq 0$ et $D^{r+1} f = 0$. Alors on a

$$D^{r-1}(Df) \neq 0 \quad \text{et} \quad D^r(Df) = 0 ,$$

donc d'après l'hypothèse de récurrence Df est une fonction polynôme de degré $(r - 1)$, de N dans C. Soit

$$P(X) = a_{r-1} \{ X \}^{r-1} + a_{r-2} \{ X \}^{r-2} + \cdots + a_1 \{ X \} + a_0$$

le polynôme de $\mathbf{C}_{r-1}[X]$ tel que Df soit la restriction à N de la fonction polynôme $\widetilde{P}$ associée à P. Alors on a

$$P = \Delta Q \quad \text{avec} \quad Q = \frac{a_{r-1}}{r} \{ X \}^r + \cdots + a_0 \{ X \} \qquad (cf.\ \text{I, 1, } c) .$$

Désignant par g la restriction à N de la fonction polynôme $\widetilde{Q}$ associée à Q, nous savons (2, *a*) que Dg est la restriction à N de $\widetilde{\Delta Q}$, or $P = \Delta Q$, donc $Dg = Df$, par suite $D(g - f) = 0$ et $g - f$ est une fonction constante (II, 1, *b*) donc f est une fonction polynôme de degré r, de N dans C.

III. Si f est une fonction polynôme de degré $r - 1$, nous venons de montrer qu'il existe une fonction g de degré r, telle que $f = Dg$ (remplacer Df par f à la fin de la démonstration de II, 2, *b*) de plus cette fonction g est telle que

$g(0) = 0$. Supposons que g' soit une fonction polynôme de N dans C, de degré r, telle que $Dg' = f$ et $g'(0) = 0$; alors on aurait $Dg = Dg'$ soit

$$D(g - g') = 0,$$

par suite $g - g'$ serait une fonction constante, or

$$(g - g')(0) = g(0) - g'(0) = 0 \quad \text{donc} \quad g = g'.$$

Si g est la fonction telle que $Df = g$ et $g(0) = 0$, on a pour tout entier naturel n,

$$\begin{aligned} f(0) + f(1) + \cdots + f(n) &= Dg(0) + \cdots + Dg(n) = \\ &= (g(1) - g(0)) + (g(2) - g(1)) + \cdots + (g(n+1) - g(n)) \\ &= g(n+1) - g(0) = g(n+1). \end{aligned}$$

Applications.

a) *Calcul de A.* Soit f la fonction polynôme de N dans C associée au polynôme $P(X) = X^2$. On a $\{X\}^2 = X(X-1) = X^2 - X$, donc

$$X^2 = \{X\}^2 + \{X\},$$

par suite (III) la fonction polynôme g associée au polynôme

$$\tfrac{1}{3}\{X\}^3 + \tfrac{1}{2}\{X\}^2 = Q(X)$$

est telle que $Dg = f$ et $g(0) = 0$. Or

$$Q(X) = \frac{X(X-1)(2X-1)}{6}$$

donc

$$A = 1^2 + 2^2 + \cdots + n^2 = f(0) + f(1) + f(2) + \cdots + f(n) = g(n+1)$$

donc

$$A = \frac{n(n+1)(2n+1)}{6}.$$

b) *Calcul de B.* Même procédé que pour A avec f associée au polynôme $P(X) = X^3$. On a $\{X\}^3 = X^3 - 3X^2 + 2X$ d'où

$$P(X) = \{X\}^3 + 3X^2 - 2X = \{X\}^3 + 3\{X\}^2 + \{X\}$$

et

$$Q(X) = \frac{1}{4}\{X\}^4 + \{X\}^3 + \frac{1}{2}\{X\}^2 = \frac{X^2(X-1)^2}{4},$$

d'où

$$B = 1^3 + 2^3 + \cdots + n^3 = f(0) + f(1) + \cdots + f(n) = g(n+1) = \frac{n^2(n+1)^2}{4}.$$

c) *Calcul de C.* Le procédé précédent fournit ici :

$$P(X) = (2X + 1)^2 = 4\{X\}^2 + 8\{X\} + 1,$$

d'où

$$Q\{X\} = \frac{4}{3}\{X\}^3 + 4\{X\}^2 + \{X\} = \frac{X(2X - 1)(2X + 1)}{3},$$

ce qui donne

$$C = \frac{n(2n - 1)(2n + 1)}{3}.$$

d) *Calcul de D.* Même procédé

$$P(X) = X(X + 1) = \{X\}^2 + 2\{X\};$$

$$Q(X) = \frac{\{X\}^3}{3} + \{X\}^2 = \frac{X(X - 1)(X + 1)}{3} \quad \text{et} \quad D = \frac{n(n + 1)(n + 2)}{3}.$$

9.5 Soit E l'espace vectoriel complexe $\mathbf{C}^3$ rapporté à la base canonique (e_1, e_2, e_3). A tout élément a de coordonnées (a_1, a_2, a_3) de E, on associe l'application linéaire f_a de E dans E définie par

$$\begin{aligned} f_a(e_1) &= a_1 e_1 + a_2 e_2 + a_3 e_3 \\ f_a(e_2) &= \quad\; \bar{a}_1 e_2 + \bar{a}_2 e_3 \\ f_a(e_3) &= \quad\quad\quad\; a_1 e_3 \end{aligned}$$

($\bar{a}_i$ désignant le conjugué de a_i dans C).

1) *a*) Exprimer les coordonnées (y_1, y_2, y_3) de $y = f_a(x)$ en fonction des coordonnées (x_1, x_2, x_3) de x.

b) Caractériser les éléments a de E pour lesquels f_a est un automorphisme de E.

c) Lorsque f_a n'est pas un automorphisme de E, déterminer le rang de f_a en fonction du plus grand indice p ($1 \leqslant p \leqslant 3$) pour lequel a_i est nul pour $1 \leqslant i \leqslant p$.

2) *a*) Montrer que pour deux éléments a et b de E, on a $f_a + f_b = f_{a+b}$.

b) On définit dans E la loi de composition $\top$ par $x \top y = f_x(y)$ pour tout x et tout y de E. Démontrer que pour deux éléments a et b de E, on a

$$f_a \circ f_b = f_{a \top b}.$$

c) Montrer que l'addition de l'espace vectoriel E et la loi de composition $\top$ munissent E d'une structure d'anneau unitaire. Cet anneau A est-il commutatif ? Quels sont les éléments inversibles de cet anneau ?

3) λ étant un élément de C, comparer $f_{\lambda a}$ et λf_a.

Solution Dans toute la suite nous désignerons par M_a la matrice de l'endomorphisme f_a de E, relativement à la base canonique. On a donc

$$M_a = \begin{pmatrix} a_1 & 0 & 0 \\ a_2 & \bar{a}_1 & 0 \\ a_3 & \bar{a}_2 & a_1 \end{pmatrix}.$$

1) *a*) L'égalité vectorielle $y = f_a(x)$ s'écrit sous forme matricielle

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} a_1 & 0 & 0 \\ a_2 & \bar{a}_1 & 0 \\ a_3 & \bar{a}_2 & a_1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

On a donc

$$\begin{cases} y_1 = a_1 x_1 \\ y_2 = a_2 x_1 + \bar{a}_1 x_2 \\ y_3 = a_3 x_1 + \bar{a}_2 x_2 + a_1 x_3 . \end{cases}$$

b) Le déterminant de la matrice M_a est $a_1^2 \bar{a}_1$. Ce déterminant est nul si et seulement si a_1 est nul ; par suite, f_a est un automorphisme si et seulement si a_1 n'est pas nul.

c) Supposons a_1 nul ; la matrice $\begin{pmatrix} a_2 & 0 \\ a_3 & \bar{a}_2 \end{pmatrix}$ extraite de M_a a pour déterminant $a_2 \bar{a}_2$; par suite, M_a est de rang 2 ainsi que f_a si a_2 n'est pas nul, et on a dans ce cas $p = 1$. Si a_2 est nul et a_3 non nul, f_a et M_a sont de rang 1 et on a $p = 2$; enfin si $a_1 = a_2 = a_3 = 0$, f_a est de rang 0 et p est égal à 3. Ainsi, lorsque f_a n'est pas un automorphisme de E, le rang de f_a est égal à $3 - p$.

2) *a*) Les coordonnées de $a + b$ sont $(a_1 + b_1,\ a_2 + b_2,\ a_3 + b_3)$ si $a = (a_1, a_2, a_3)$ et $b = (b_1, b_2, b_3)$; on a

$$\overline{a_i + b_i} = \bar{a}_i + \bar{b}_i \qquad (1 \leqslant i \leqslant 3)$$

donc $M_{a+b} = M_a + M_b$ et par suite $f_{a+b} = f_a + f_b$.

b) Effectuons le produit des matrices M_a et M_b ;

$$M_a . M_b = \begin{pmatrix} a_1 & 0 & 0 \\ a_2 & \bar{a}_1 & 0 \\ a_3 & \bar{a}_2 & a_1 \end{pmatrix} \begin{pmatrix} b_1 & 0 & 0 \\ b_2 & \bar{b}_1 & 0 \\ b_3 & \bar{b}_2 & b_1 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 b_1 & 0 & 0 \\ a_2 b_1 + \bar{a}_1 b_2 & \bar{a}_1 \bar{b}_1 & 0 \\ a_3 b_1 + \bar{a}_2 b_2 + a_1 b_3 & \bar{a}_2 \bar{b}_1 + a_1 \bar{b}_2 & a_1 b_1 \end{pmatrix}.$$

On remarque que $M_a . M_b = M_c$, c étant l'élément de E de coordonnées $(a_1 b_1,\ a_2 b_1 + \bar{a}_1 b_2,\ a_3 b_1 + \bar{a}_2 b_2 + a_1 b_3)$. D'autre part les formules de (1, *a*) montrent que $c = f_a(b)$ et par suite $c = a \top b$. On a donc $f_a \circ f_b = f_{a \top b}$.

c) Soient x, y, z trois éléments quelconques de E ; on a les égalités suivantes

$$(x \top y) \top z = f_{x \top y}(z) = f_x \circ f_y(z) = f_x[f_y(z)] = f_x(y \top z) = x \top (y \top z) \quad (\alpha)$$

$$x \top (y + z) = f_x(y + z) = f_x(y) + f_x(z) = (x \top y) + (x \top z) \quad (\beta)$$

$$(x + y) \top z = f_{x+y}(z) = f_x(z) + f_y(z) = (x \top z) + (y \top z)\,. \quad (\gamma)$$

La loi $\top$ est donc associative (α), distributive par rapport à l'addition de E ((β) et (γ)). Il en résulte que l'addition et la loi $\top$ munissent E d'une structure d'anneau. Les formules de (1, *a*) appliquées à x de coordonnées $(0, x_2, 0)$ et y de coordonnées $(0, y_2, 0)$ montrent que

$$x \top y = (0, 0, \bar{x}_2\, y_2) \qquad \text{et} \qquad y \top x = (0, 0, x_2\, \bar{y}_2)\,;$$

donc si x_2 est réel non nul et y_2 imaginaire pur, non nul, $x \top y$ est différent de $y \top x$, et par suite l'anneau obtenu n'est pas commutatif. f_{e_1} est l'application identique de E ; pour tout élément a de E, on a donc

$$f_a = f_a \circ f_{e_1} = f_{e_1} \circ f_a = f_{a \top e_1} = f_{e_1 \top a}\,.$$

D'autre part, on voit facilement que si a, b sont deux éléments de E, alors $f_a = f_b$ si et seulement si $a = b$. Il en résulte que pour tout élément a de E on a

$$a = a \top e_1 = e_1 \top a\,.$$

e_1 est donc élément neutre pour la loi $\top$, et par suite l'anneau A est unitaire.

Les formules (2, *a*) et (2, *b*) montrent que l'application Φ qui à un élément a de E associe l'endomorphisme f_a, est un homomorphisme de l'anneau A dans l'anneau des endomorphismes de E. Cet homomorphisme est injectif puisque $f_a = f_b$ si et seulement si $a = b$. Donc, pour que a soit inversible dans E il faut et suffit que f_a soit un automorphisme de E. Les éléments inversibles de A sont donc les éléments a de coordonnées (a_1, a_2, a_3) avec a_1 non nul.

3) On a

$$M_{\lambda a} = \begin{pmatrix} \lambda a_1 & 0 & 0 \\ \lambda a_2 & \bar{\lambda}\bar{a}_1 & 0 \\ \lambda a_3 & \bar{\lambda}\bar{a}_2 & \lambda a_1 \end{pmatrix} \quad \text{et} \quad \lambda . M_a = \begin{pmatrix} \lambda a_1 & 0 & 0 \\ \lambda a_2 & \lambda\bar{a}_1 & 0 \\ \lambda a_3 & \lambda\bar{a}_2 & \lambda a_1 \end{pmatrix}.$$

Par suite $M_{\lambda a} = \lambda M_a$ si λ est réel ou si $a_2 = a_3 = 0$. Dans le cas contraire $M_{\lambda a} \neq \lambda M_a$ et par suite $f_{\lambda a} \neq \lambda f_a$. Φ n'est donc pas une application linéaire de l'espace vectoriel E dans l'espace vectoriel des applications linéaires de E dans E.

9.6

Soit $\mathcal{M}$ l'algèbre sur $\mathbf{R}$ des matrices carrées d'ordre 2 à coefficients réels, et soit $\mathcal{A}$ le groupe multiplicatif des matrices inversibles de $\mathcal{M}$.

Pour tout élément $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathcal{M}$, on pose $D(X) = ad - bc$. On désigne par $\mathbf{R}^*$ le groupe multiplicatif des nombres réels non nuls, par $\mathbf{R}_+^*$ le groupe

multiplicatif des nombres réels strictement positifs et par $\mathbf{T} = \mathbf{R}/2\pi\mathbf{Z}$, le groupe additif des nombres réels modulo 2π.

1) Montrer que les matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad K = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad L = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

constituent une base de $\mathscr{M}$. En déduire que toute matrice $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathscr{M}$ s'écrit de façon unique sous la forme $X = x_0 I + x_1 J + x_2 K + x_3 L$. Calculer x_0, x_1, x_2, x_3 en fonction de a, b, c, d et calculer $D(X)$ en fonction de x_0, x_1, x_2, x_3.

Démontrer les relations $J^2 = -I$, $K^2 = L^2 = I$; $J.K = -K.J = L$; $L.J = I$ et $J.L = -K$.

2) Démontrer que l'application R de $\mathbf{T}$ dans $\mathscr{A}$ définie par

$$R(\theta) = \cos\theta . I + \sin\theta . J ,$$

pour chaque élément θ de $\mathbf{T}$, est un homomorphisme injectif de $\mathbf{T}$ dans $\mathscr{A}$. Démontrer les relations

$$R\left(-\frac{\theta}{2}\right).J.R\left(\frac{\theta}{2}\right) = J ; \quad R\left(-\frac{\theta}{2}\right).K.R\left(\frac{\theta}{2}\right) = K.R(\theta) ;$$

$$R\left(-\frac{\theta}{2}\right).L.R\left(\frac{\theta}{2}\right) = L.R(\theta) .$$

Démontrer que l'application U de $\mathbf{R}_+^* \times \mathbf{T}$ dans $\mathscr{A}$ définie par $U(s, \theta) = s.R(\theta)$ vérifie la relation

$$U(s, \theta).U(s', \theta') = U(ss', \theta + \theta') .$$

En déduire que U est un homomorphisme injectif du groupe produit $\mathbf{R}_+^* \times \mathbf{T}$ dans $\mathscr{A}$.

Démontrer la relation $K.U(s, \theta).K = U(s, -\theta)$.

3) Calculer $J.X$ et $X.J$. En déduire que l'équation

$$J.X = X.J \tag{1}$$

est équivalente au système d'équations $x_2 = 0$ et $x_3 = 0$. Pour une solution X de (1) quelle est l'expression de $D(X)$ en fonction de x_0 et x_1.

Montrer que U établit une bijection entre l'ensemble $\mathbf{R}_+^* \times \mathbf{T}$ et l'ensemble des solutions de l'équation en X

$$X^{-1} JX = J . \tag{2}$$

4) Démontrer que l'application S de $\mathbf{R}$ dans $\mathscr{A}$ définie par

$$S(t) = \operatorname{ch} t . I + \operatorname{sh} t . K$$

pour chaque nombre réel t, est un homomorphisme injectif de $\mathbf{R}$ dans $\mathscr{A}$.

Démontrer que l'application T de $\mathbf{R}^*$ dans $\mathscr{A}$ définie par

$$T(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & \sigma \end{pmatrix}$$

pour chaque élément σ de $\mathbf{R}^*$, est un homomorphisme injectif de $\mathbf{R}^*$ dans $\mathscr{A}$.

En posant $V(t, \sigma) = S(t)\,T(\sigma)$ démontrer la relation

$$[V(t, \sigma)]^{-1} = T\left(\frac{1}{\sigma}\right) S(-t)$$

et calculer la matrice $J_{t,\sigma} = [V(t, \sigma)]^{-1}.J.V(t, \sigma)$.

5) Calculer les coefficients de la matrice X^2 en fonction de ceux de X. Montrer que toute solution de l'équation

$$X^2 = -I \tag{3}$$

peut s'écrire de façon unique sous la forme

$$\begin{pmatrix} \operatorname{sh} 2t & \sigma \operatorname{ch} 2t \\ -\frac{1}{\sigma} \operatorname{ch} 2t & -\operatorname{sh} 2t \end{pmatrix}.$$

En déduire que l'application ω de $\mathbf{R} \times \mathbf{R}^*$ dans $\mathscr{A}$ définie par $\omega(t, \sigma) = J_{t,\sigma}$ établit une bijection entre l'ensemble $\mathbf{R} \times \mathbf{R}^*$ et l'ensemble $\mathscr{S}$ des solutions de l'équation (3).

6) Démontrer que pour tout élément A de $\mathscr{A}$, la matrice $A^{-1}.J.A$ est un élément de $\mathscr{S}$. Montrer qu'il existe un élément unique (t, σ) de $\mathbf{R} \times \mathbf{R}^*$ tel que la matrice $B = A.[V(t, \sigma)]^{-1}$ soit une solution de l'équation (2).

En déduire que toute matrice A de $\mathscr{A}$ s'écrit de façon unique sous la forme

$$A = U(s, \theta)\,V(t, \sigma).$$

Quelles sont les valeurs des paramètres s et θ relatifs à la matrice $-A$ opposée de A.

Solution 1) Comme $\mathscr{M}$ est de dimension 4, il suffira de montrer de I, J, K, L forment une famille libre. Soient x_0, x_1, x_2, x_3 des nombres réels tels que

$$x_0 I + x_1 J + x_2 K + x_3 L = 0$$

alors

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = x_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + x_1 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + x_3 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} x_0 + x_3, x_1 + x_2 \\ x_2 - x_1, x_0 - x_3 \end{pmatrix}$$

donc

$$x_0 + x_3 = x_1 + x_2 = x_2 - x_1 = x_0 - x_3 = 0$$

d'où $x_0 = x_1 = x_2 = x_3 = 0$. Les matrices I, J, K, L forment donc une base de $\mathscr{M}$, par suite toute matrice

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

de $\mathscr{M}$ s'écrit de manière unique sous la forme $X = x_0 I + x_1 J + x_2 K + x_3 L$ et on a

$$x_0 + x_3 = a\,, \quad x_1 + x_2 = b\,, \quad x_2 - x_1 = c\,, \quad x_0 - x_3 = d$$

donc

$$x_0 = \frac{a+d}{2}\,, \quad x_1 = \frac{b-c}{2}\,, \quad x_2 = \frac{b+c}{2}\,, \quad x_3 = \frac{a-d}{2}\,.$$

On a

$$D(X) = ad - bc = x_0^2 + x_1^2 - x_2^2 - x_3^2\,,$$

$$J^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$

et on démontre de même que $K^2 = L^2 = I$, $J.K = -K.J = L$ et $L.J = I$, $J.L = -K$.

2) Pour démontrer que R est un homomorphisme de $\mathbf{T}$ dans $\mathscr{A}$, il faut démontrer que si θ, θ' sont deux éléments de $\mathbf{T}$, on a $R(\theta).R(\theta') = R(\theta + \theta')$. Or,

$$R(\theta).R(\theta') = [\cos\theta.I + \sin\theta.J]\,[\cos\theta'.I + \sin\theta'.J]$$

et comme $J^2 = -I$ on a

$$R(\theta).R(\theta') = \cos(\theta + \theta').I + \sin(\theta + \theta')\,.J = R(\theta + \theta')\,.$$

Cherchons le noyau de cet homomorphisme. Soit θ un élément de $\mathbf{T}$ tel que $R(\theta) = I$, alors $\cos\theta = 1$, $\sin\theta = 0$; il en résulte que $\theta = 0$ donc R est injectif.

J commute avec I et J donc avec $\cos\frac{\theta}{2}\cdot I + \sin\frac{\theta}{2}\cdot J$, par suite

$$R\left(-\frac{\theta}{2}\right).J.R\left(\frac{\theta}{2}\right) = R\left(-\frac{\theta}{2}\right).R\left(\frac{\theta}{2}\right).J = R(0)\,.J = I.J = J\,.$$

Nous avons

$$R\left(-\frac{\theta}{2}\right).K = \cos\frac{\theta}{2}I.K - \sin\frac{\theta}{2}J.K = K\left(\cos\frac{\theta}{2}I + \sin\frac{\theta}{2}J\right)$$

car $J.K = -K.J$, donc

$$R\left(-\frac{\theta}{2}\right).K = K.R\left(\frac{\theta}{2}\right),$$

par suite

$$R\left(-\frac{\theta}{2}\right).K.R\left(\frac{\theta}{2}\right) = K.R\left(\frac{\theta}{2}\right).R\left(\frac{\theta}{2}\right) = K.R(\theta).$$

Effectuons le produit membre à membre des deux relations démontrées, nous obtenons

$$R\left(-\frac{\theta}{2}\right).J.R\left(\frac{\theta}{2}\right).R\left(-\frac{\theta}{2}\right).K.R\left(\frac{\theta}{2}\right) = J.K.R(\theta),$$

d'où

$$R\left(-\frac{\theta}{2}\right).J.K.R\left(\frac{\theta}{2}\right) = J.K.R(\theta);$$

comme $J.K = L$ nous avons

$$R\left(-\frac{\theta}{2}\right).L.R\left(\frac{\theta}{2}\right) = L.R(\theta).$$

Pour prouver que U est un homomorphisme de $\mathbf{R}_+^* \times \mathbf{T}$ dans $\mathscr{A}$, il suffit de vérifier la relation $U(ss', \theta + \theta') = U(s, \theta).U(s', \theta')$ or on a

$$\begin{aligned} U(s, \theta).U(s', \theta') &= s.R(\theta).s'.R(\theta') = s.s'.R(\theta).R(\theta') \\ &= s.s'.R(\theta + \theta') = U(ss', \theta + \theta'). \end{aligned}$$

Cherchons le noyau de cet homomorphisme. Soit (s, θ) un élément de $\mathbf{R}_+^* \times \mathbf{T}$ tel que $U(s, \theta) = s.R(\theta) = I$. Nous avons

$$s\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

soit $s\cos\theta = 1$ et $\sin\theta = 0$ d'où $\theta = 0$ et $s = 1$; par suite (s, θ) est l'élément neutre du groupe produit $\mathbf{R}_+^* \times \mathbf{T}$ et U est injectif.

On a $K.U(s, \theta).K = K.s.R(\theta).K = s.K.R(\theta).K$ or

$$R\left(-\frac{\theta}{2}\right).K = K.R\left(\frac{\theta}{2}\right)$$

étant vrai pour tout élément θ de $\mathbf{T}$, on a $R(\theta).K = K.R(-\theta)$ donc

$$K.U(s, \theta).K = sK.K.R(-\theta) = s.R(-\theta) = U(s, -\theta).$$

3) Nous avons

$$J.X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ -a & -b \end{pmatrix}$$

$$X.J = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$$

par suite on a $J.X = X.J$ si et seulement si $a = d$ et $b = -c$ soit d'après les relations démontrées en (1), si et seulement si $x_3 = 0$ et $x_2 = 0$. Si X est solution de l'équation (1), on a $D(X) = x_0^2 + x_1^2$.

Soit (s, θ) un élément de $\overline{\mathbf{R}}_+^* \times \overline{\mathbf{T}}$; démontrons que $U(s, \theta)$ est solution de l'équation (2). Nous avons

$$U(s, \theta) = s[\cos\theta.I + \sin\theta.J]$$

donc d'après ce qui précède $J.U(s, \theta) = U(s, \theta).J$; comme $D(U(s, \theta)) = s^2$, $U(s, \theta)$ est inversible et son inverse est $U\left(\frac{1}{s}, -\theta\right)$; par suite $U(s, \theta)$ vérifie $[U(s, \theta)]^{-1}.J.U(s, \theta) = J$ donc est solution de (2).

Réciproquement soit X une solution de l'équation (2) ; alors X est inversible et $J.X = X.J$ donc $x_2 = x_3 = 0$ et $x_0^2 + x_1^2 \neq 0$. Posons $s = \sqrt{x_0^2 + x_1^2}$, alors

$$X = s\left(\frac{x_0}{s} I + \frac{x_1}{s} J\right)$$

et on sait qu'il existe un élément θ de $\mathbf{T}$ et un seul, tel que

$$\cos\theta = \frac{x_0}{s} \qquad \text{et} \qquad \sin\theta = \frac{x_1}{s},$$

donc $X = s.R(\theta) = U(s, \theta)$; or U est injectif, par conséquent U établit une bijection entre $\mathbf{R}_+^* \times \mathbf{T}$ et l'ensemble des solutions de (2).

4) Pour démontrer que S est un homomorphisme il suffit d'établir que $S(t).S(t') = S(t + t')$ si t, t' sont deux nombres réels. Or

$$\begin{aligned} S(t).S(t') &= [\operatorname{ch} t.I + \operatorname{sh} t.K][\operatorname{ch} t'.I + \operatorname{sh} t'.K] \\ &= [(\operatorname{ch} t.\operatorname{ch} t' + \operatorname{sh} t.\operatorname{sh} t')\, I + (\operatorname{ch} t.\operatorname{sh} t' + \operatorname{sh} t.\operatorname{ch} t').K] \\ &= [\operatorname{ch}(t + t').I + \operatorname{sh}(t + t').K] = S(t + t')\,. \end{aligned}$$

Si t est un nombre réel, t appartient au noyau de S si et seulement si $S(t) = I$ soit $\operatorname{ch} t = 1$ et $\operatorname{sh} t = 0$ soit encore $t = 0$, donc S est un homomorphisme injectif.

Si σ, σ' sont deux éléments de $\mathbf{R}^*$, on a

$$T(\sigma).T(\sigma') = \begin{pmatrix} 1 & 0 \\ 0 & \sigma \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \sigma' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \sigma\sigma' \end{pmatrix} = T(\sigma\sigma')\,,$$

donc T est un homomorphisme. Comme $T(\sigma) = I$ si et seulement si $\sigma = 1$, T est injectif.

Soit (t, σ) un élément de $\mathbf{R} \times \mathbf{R}^*$; on a

$$[V(t, \sigma)]^{-1} = [S(t).T(\sigma)]^{-1} = [T(\sigma)]^{-1}.[S(t)]^{-1} = T\left(\frac{1}{\sigma}\right) S(-t)\,,$$

et un calcul direct montre que

$$J_{t,\sigma} = \begin{pmatrix} \operatorname{sh} 2t & \sigma \operatorname{ch} 2t \\ -\dfrac{1}{\sigma} \operatorname{ch} 2t & -\operatorname{sh} 2t \end{pmatrix}.$$

5) Si $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a

$$X^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 + bc & ab + bd \\ ac + dc & cb + d^2 \end{pmatrix}.$$

Si X vérifie l'équation (3), on a

$$a^2 + bc = -1, \quad cb + d^2 = -1, \quad b(a + d) = 0 \quad \text{et} \quad c(a + d) = 0.$$

Comme il est impossible que b ou c soit nul (car alors $a^2 = -1$ et $d^2 = -1$) nous avons $a + d = 0$; par suite, si X est solution de l'équation (3), X est de la forme $X = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ où $a^2 + bc = -1$. Nous savons qu'il existe un nombre réel t et un seul, tel que $a = \operatorname{sh} 2t$; posons $\sigma = \dfrac{b}{\operatorname{ch} 2t}$, alors comme $a^2 + bc = -1$, on a $\operatorname{sh}^2 2t + bc = -1$ donc

$$bc = \operatorname{ch}^2 2t \qquad \text{et} \qquad c = \frac{1}{\sigma}\operatorname{ch} 2t.$$

X s'écrit donc, de manière unique, sous la forme

$$X = \begin{pmatrix} \operatorname{sh} 2t & \sigma \operatorname{ch} 2t \\ -\dfrac{1}{\sigma}\operatorname{ch} 2t & -\operatorname{sh} 2t \end{pmatrix}.$$

L'application ω définie par $\omega(t, \sigma) = J_{t,\sigma}$ est une bijection de $\mathbf{R} \times \mathbf{R}^*$ sur $\mathscr{S}$ car $J_{t,\sigma}$ est une solution de l'équation (3) et réciproquement, toute solution X de l'équation (3) s'écrit d'une manière et d'une seule sous la forme $X = J_{t,\sigma}$.

6) Soit A un élément de $\mathscr{A}$. A est inversible et nous avons

$$(A^{-1} JA)(A^{-1} JA) = A^{-1} J^2 A = -I,$$

donc $A^{-1}.J.A$ est une solution de (3) ; par suite il existe un élément (t, σ) de $\mathbf{R} \times \mathbf{R}^*$ et un seul, tel que

$$A^{-1}.J.A = J_{t,\sigma} = [V(t, \sigma)]^{-1}.J.V(t, \sigma),$$

alors

$$[V(t, \sigma)].A^{-1}.J.A.[V(t, \sigma)]^{-1} = J$$

donc $A.[V(t, \sigma)]^{-1}$ est solution de l'équation (2), par conséquent il existe un élément (s, θ) de $\mathbf{R}_+^* \times \mathbf{T}$ et un seul tel que $A.[V(t, \sigma)]^{-1} = U(s, \theta)$ soit $A = U(s, \theta).V(t, \sigma)$. En conclusion, toute matrice A de $\mathscr{A}$ s'écrit, d'une manière et d'une seule sous la forme $A = U(s, \theta).V(t, \sigma)$.
Il est clair que

$$R(\theta + \pi) = -R(\theta).$$

donc si

$$A = U(s, \theta)\, V(t, \sigma) = s.R(\theta).V(t, \sigma)$$

on a

$$-A = sR(\theta + \pi).V(t, \theta)$$

soit

$$-A = U(s, \theta + \pi).V(t, \sigma)\,.$$

9.7

Les matrices considérées sont à coefficients réels. Une matrice à m lignes et n colonnes sera dite matrice de type (m, n). Nous identifierons une matrice de type (1, 1) à son unique coefficient. Si U, V sont des matrices de type $(m, 1)$, ${}^tV.U = {}^tU.V$ est donc considéré comme un nombre réel.

Dans l'espace vectoriel sur $\mathbf{R}$ des matrices de type $(m, 1)$ nous considérons la norme définie par $\| U \| = \sqrt{{}^tU.U}$ (où U est une matrice de type $(m, 1)$).

Si A et D sont respectivement des matrices de type (m, n) et $(m, 1)$, une matrice X de type $(n, 1)$ est appelée une *pseudosolution* de l'équation en X

$$AX - D = 0 \qquad \text{(E)}$$

si pour toute matrice Z de type $(n, 1)$, on a

$$\| AX - D \| \leqslant \| AZ - D \|\,.$$

1) Montrer que si l'équation (E) a des solutions, les pseudosolutions de (E) coïncident avec les solutions de (E).

2) Montrer que si X et Y sont des matrices de type $(n, 1)$ et λ un nombre réel, on a

$$\| A(X + \lambda Y) - D \|^2 = \| AX - D \|^2 + 2\lambda\, {}^tY\, {}^tA(AX - D) + \lambda^2 \| AY \|^2\,.$$

En déduire que les pseudosolutions de (E) sont les solutions de l'équation en X

$${}^tAAX = {}^tAD\,.$$

3) Montrer que si X est une pseudosolution de (E), alors

$$\| AX - D \|^2 = \| D \|^2 - {}^tX\, {}^tAD\,.$$

4) Montrer que si X est une matrice de type $(n, 1)$ les deux équations en X

$${}^tAAX = 0 \qquad \text{et} \qquad AX = 0$$

ont les mêmes solutions.

5) Démontrer les propriétés suivantes :

(α) Si X_1 et X_2 sont deux pseudosolutions de (E),

$$A(X_1 - X_2) = 0\,.$$

(β) Si M, N sont deux matrices de type (n, p), on a ${}^tAAM = {}^tAAN$ si et seulement si $AM = AN$.

(γ) Le rang de ${}^tAA$ est égal au rang de A.

(δ) L'équation (E) a toujours des pseudosolutions. (On pourra considérer l'ensemble $\mathscr{S}$ des matrices ${}^tA.U$ où U est une matrice quelconque de type $(m, 1)$, et l'ensemble $\mathscr{S}'$ des matrices ${}^tAAW$ où W est une matrice de type $(n, 1)$.)

6) On suppose que le rang de la matrice A est égal à n. Montrer que l'équation (E) a une pseudosolution unique X et déterminer en fonction de A une matrice B telle que $X = BD$. Vérifier que BA est la matrice unité et AB une matrice symétrique.

Solution 1) Soit X une solution de (E). Pour toute matrice Z de type $(n, 1)$ on a

$$\| AZ - D \| \geqslant \| AX - D \| = 0$$

donc X est une pseudosolution de (E).

Soit X' une pseudosolution de (E) et X une solution. On a

$$\| AX' - D \| \leqslant \| AX - D \| = 0$$

donc

$$\| AX' - D \| = 0 \qquad \text{et} \qquad AX' - D = 0,$$

par suite X' est solution de (E).

2) $\| A(X + \lambda Y) - D \|^2 =$

$= {}^t[A(X + \lambda Y) - D][A(X + \lambda Y) - D]$

$= [{}^t(AX - D) + \lambda\, {}^t(AY)][(AX - D) + \lambda AY]$

$= {}^t(AX - D).(AX - D) + \lambda\, {}^tY\, {}^tA(AX - D) +$

$+ \lambda\, {}^t(AX - D)\, AY + \lambda^2\, {}^t(AY)\, (AY)$

$= \| AX - D \|^2 + \lambda\, {}^tY\, {}^tA(AX - D) + \lambda\, {}^t({}^t(AX - D)\, AY) + \lambda^2 \| AY \|^2$

$= \| AX - D \|^2 + 2\lambda\, {}^tY\, {}^tA(AX - D) + \lambda^2 \| AY \|^2 .$

Pour que X soit une pseudosolution de (E) il faut et suffit que pour tout Y, le trinôme du second degré en λ atteigne son minimum pour $\lambda = 0$. En effet, on a alors, $\| AX - D \|^2 \leqslant \| A(X + \lambda Y) - D \|$ pour tout λ et tout Y. Cette condition est équivalente à ${}^tY\, {}^tA(AX - D) = 0$ pour tout Y, ou encore ${}^tA(AX - D) = 0$. On voit donc que X est pseudosolution de (E) si et seulement si ${}^tAAX = {}^tAD$.

3) Soit X une pseudosolution de (E), alors

$$\| AX - D \|^2 = {}^t(AX - D)(AX - D) = ({}^tX\, {}^tA - {}^tD)(AX - D)$$
$$= {}^tX\, {}^tAAX - {}^tX\, {}^tAD - {}^tDAX + {}^tDD,$$

or ${}^tDAX$ est un nombre réel, donc

$$\| AX - D \|^2 = {}^tX({}^tAAX - {}^tAD) + \| D \|^2 - {}^t({}^tDAX) = \| D \|^2 - {}^tX\, {}^tAD .$$

4) Il est évident que si $AX = 0$ on a ${}^tAAX = 0$. Soit X une matrice de type $(n, 1)$ telle que ${}^tAAX = 0$. On a alors ${}^tX\,{}^tAAX = 0 = \| AX \|^2$ donc $AX = 0$.

5) (α) Soient X_1 et X_2 deux pseudosolutions de (E). D'après (2) X_1 et X_2 vérifient ${}^tAAX_1 = {}^tAD = {}^tAAX_2$ d'où en appliquant (4) on déduit

$$ {}^tAA(X_2 - X_1) = 0 \qquad \text{et} \qquad A(X_2 - X_1) = 0 . $$

(β) L'implication $AM = AN$ entraîne ${}^tAAM = {}^tAAN$ est immédiate. Supposons que ${}^tAAM = {}^tAAN$ et soit U une matrice de type $(p, 1)$. On a alors

$$ {}^tAA(MU) = {}^tAA(NU) . $$

Mais MU et NU sont deux matrices de type $(n, 1)$, on peut donc appliquer (4) et on obtient $AMU = ANU$. Cette égalité étant vraie pour toute matrice U de type $(p, 1)$ on en déduit que $AM = AN$.

(γ) Soit f (resp. g) l'application linéaire de $\mathbf{R}^n$ dans $\mathbf{R}^m$ (resp. de $\mathbf{R}^n$ dans $\mathbf{R}^n$) définie par la matrice A (resp. ${}^tAA$) relativement aux bases canoniques de $\mathbf{R}^n$ et $\mathbf{R}^m$. A la question (4), nous avons montré que si x est un élément de $\mathbf{R}^n$, alors on a $f(x) = 0$ si et seulement si $g(x) = 0$ donc $\operatorname{Ker} f = \operatorname{Ker} g$, par suite $\operatorname{rg} A = \dim \operatorname{Im} f = n - \dim \operatorname{Ker} f = n - \dim \operatorname{Ker} g = \dim \operatorname{Im} g = \operatorname{rg} {}^tAA$.

(δ) Soit h l'application linéaire de $\mathbf{R}^m$ dans $\mathbf{R}^n$, rapportés à leurs bases canoniques, dont la matrice est ${}^tA$. Alors $\mathscr{I} = \operatorname{Im} h$ et $\mathscr{I}' = \operatorname{Im} g$, où g est l'application définie en (γ). Comme $\operatorname{rg} A = \operatorname{rg} {}^tA$ (*cf.* Q., Ch. 8, § III, n° 162), $\dim \operatorname{Im} h = \dim \operatorname{Im} f = \dim \operatorname{Im} g$, donc $\dim \mathscr{I} = \dim \mathscr{I}'$. D'autre part, comme $g = h \circ f$, on a $\mathscr{I} \subset \mathscr{I}'$, donc $\mathscr{I} = \mathscr{I}'$.

La matrice ${}^tAD$ appartient à $\mathscr{I}$ donc aussi à $\mathscr{I}'$, par suite il existe une matrice X de type $(n, 1)$ telle que ${}^tAAX = {}^tAD$. Cette matrice X est une pseudosolution de (E), donc l'équation (E) possède toujours des pseudosolutions.

6) D'après (5, δ) nous savons que E a au moins une pseudosolution. Si le rang de A est n, l'application f définie en (5, γ) est injective. Si X_1, X_2 sont deux pseudosolutions de (E), d'après (5, α) on a

$$ A(X_2 - X_1) = 0 \quad \text{ou} \quad f(X_2 - X_1) = 0 \quad \text{donc} \quad X_1 = X_2 . $$

Il existe donc une matrice X et une seule telle que

$$ {}^tAAX = {}^tAD . $$

La matrice ${}^tAA$ est carrée d'ordre n et son rang qui est celui de A, (5, γ) est n. La matrice ${}^tAA$ est donc inversible et on a

$$ X = ({}^tAA)^{-1}\,{}^tAD \quad \text{donc} \quad B = ({}^tAA)^{-1}.{}^tA . $$

On a

$$ B.A = ({}^tAA)^{-1}.{}^tAA = I_n \quad \text{et} \quad AB = A({}^tAA)^{-1}\,{}^tA $$

donc

$$ {}^t(AB) = A\,{}^t[({}^tAA)^{-1}]\,{}^tA = A({}^tAA)^{-1}\,{}^tA = AB ; $$

la matrice AB étant égale à sa transposée, est symétrique.

9.8 I. On désigne par E l'ensemble des matrices de la forme

$$M(a, b, c) = \begin{pmatrix} a & c & b \\ b & a + c & b + c \\ c & b & a + c \end{pmatrix}$$

où a, b, c sont des nombres rationnels.

a) Démontrer que toute matrice de E s'écrit de manière unique sous la forme $aI + bJ + cK$ où I désigne la matrice unité de $\mathcal{M}_3(\mathbf{Q})$ et J, K deux matrices de $\mathcal{M}_3(\mathbf{Q})$ indépendantes de a, b, c.

b) En déduire que E est un sous-espace vectoriel de $\mathcal{M}_3(\mathbf{Q})$, considéré comme espace vectoriel sur $\mathbf{Q}$. Quelle est la dimension de E ?

c) Calculer J^2, JK, KJ, K^2 ; montrer que $J^3 = J + I$.

d) En déduire que E est un sous-anneau de l'anneau $\mathcal{M}_3(\mathbf{Q})$.

II. On pose $A(X) = X^3 - X - 1$.

a) Démontrer que si le nombre rationnel représenté par la fraction rationnelle p/q ($p \in \mathbf{N}$, $q \in \mathbf{Z}^*$) est racine du polynôme

$$B(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n$$

à coefficients entiers, alors p divise a_n et q divise a_0. En déduire que le polynôme A n'a aucune racine rationnelle.

b) Démontrer que le polynôme A admet une seule racine réelle, désignée dans toute la suite par ω.

c) Démontrer que le polynôme A est premier avec tout polynôme non nul de $\mathbf{Q}[X]$ de degré inférieur ou égal à deux.

d) En déduire que les nombres réels 1, ω, ω^2 sont linéairement indépendants dans $\mathbf{R}$ considéré comme espace vectoriel sur $\mathbf{Q}$.

e) On désigne par F l'ensemble des nombres réels de la forme $P(\omega)$ où $P(X)$ est un polynôme de $\mathbf{Q}[X]$. Démontrer que F est un sous-espace vectoriel de $\mathbf{R}$ considéré comme espace vectoriel sur $\mathbf{Q}$ et que $(1, \omega, \omega^2)$ est une base de F.

f) Démontrer que F est un sous-corps de $\mathbf{R}$.

III. Soit $\alpha = a + b\omega + c\omega^2$ un élément de l'ensemble F. On désigne par f_α l'application de F dans F définie pour tout élément ξ de F par

$$\xi' = f_\alpha(\xi) = \alpha\xi .$$

a) Démontrer que f_α est un endomorphisme de l'espace vectoriel F, et que c'est un automorphisme si et seulement si $\alpha \neq 0$.

b) Calculer la matrice M de f_α relativement à la base $(1, \omega, \omega^2)$.

c) Démontrer que l'application φ de F dans E définie par

$$\varphi(a + b\omega + c\omega^2) = M(a, b, c)$$

est à la fois un isomorphisme d'espaces vectoriels et un isomorphisme d'anneaux, puis que E est un corps commutatif.

d) Trouver une condition nécessaire et suffisante pour que le déterminant de la matrice $M(a, b, c)$ soit nul.

Solution I. *a*) Si on pose

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad J = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad K = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

il est évident que $M(a, b, c) = aI + bJ + cK$. D'autre part si

$$aI + bJ + cK = a' I + b' J + c' K$$

on a $a = a'$, $b = b'$, et $c = c'$, donc la décomposition de M en combinaison linéaire à coefficients dans $\mathbf{Q}$ de I, J, K est unique.

b) Soient $M(a, b, c)$ et $M(a', b', c')$ deux éléments de E, et r un nombre rationnel ; alors on a

$$M(a, b, c) - M(a', b', c') = M(a - a', b - b', c - c')$$

et

$$r.M(a, b, c) = M(ra, rb, rc),$$

donc (*cf.* Q., Ch. 7, § II, n° 128) E est un sous-espace vectoriel de $\mathscr{M}_3(\mathbf{Q})$ Comme tout élément de E est de manière unique combinaison linéaire des matrices I, J, K, ces trois matrices forment une base de E qui est donc de dimension 3.

c)

$$J^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = K,$$

$$J.K = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = I + J,$$

$$K.J = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = I + J,$$

$$K^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix} = J + K.$$

Enfin on a $J^3 = J.J^2 = J.K = J + I$.

d) Nous savons déjà que E est un sous-groupe additif de $\mathcal{M}_3(\mathbf{Q})$. Il reste à vérifier que E est stable pour la multiplication des matrices. Soient $M(a, b, c)$, $M(a', b', c')$ deux éléments de E ; alors on a

$$\begin{aligned}
&M(a, b, c).M(a', b', c') = \\
&= (aI + bJ + cK)(a' I + b' J + c' K) \\
&= aa' I + ab' J + ac' K + ba' J + bb' J^2 + bc' JK + \\
&\qquad + ca' K + cb' KJ + cc' K^2 \\
&= aa' I + ab' J + ac' K + ba' J + bb' K + bc'(I + J) + \\
&\qquad + ca' K + cb'(I + J) + cc'(J + K) \\
&= (aa' + bc' + cb') I + (ab' + ba' + bc' + cb' + cc') J + \\
&\qquad + (ac' + ca' + bb' + cc') K \\
&= M(aa' + bc' + cb', ab' + ba' + bc' + cb' + cc', ac' + ca' + bb' + cc') .
\end{aligned}$$

Comme $I.J = J.I = J$, $I.K = K.I = K$ et $J.K = K.J$, E est un sous-anneau commutatif de $\mathcal{M}_3(\mathbf{Q})$.

II. *a*) Si p/q est racine de B on a

$$a_0 \frac{p^n}{q^n} + a_1 \frac{p^{n-1}}{q^{n-1}} + \cdots + a_n = 0$$

donc

$$a_0 p^n + a_1 p^{n-1} q + \cdots + a_n q^n = 0 .$$

Par suite on a

$$a_0 p^n = - q(a_1 p^{n-1} + \cdots + a_n q^{n-1}) .$$

Comme q divise le second membre, q divise $a_0 p^n$. La fraction p/q étant irréductible, p^n et q sont premiers entre eux donc q divise a_0. De l'égalité

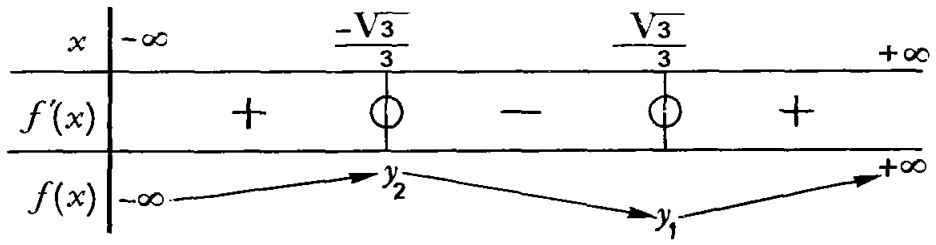
$$a_n q^n = - p(a_0 p^{n-1} + \cdots + a_{n-1} q^{n-1})$$

on déduit de la même manière que p divise a_n. D'après cette propriété, pour qu'un nombre rationnel p/q soit racine de $X^3 - X - 1$ il faut que p et q divisent 1. Les seules possibilités sont $p/q = 1$ et $p/q = -1$, or ni 1 ni -1 ne sont racines de $A(X)$, par suite $A(X)$ ne possède aucune racine rationnelle.

b) Faisons une étude sommaire de la fonction réelle d'une variable réelle, $f(x) = x^3 - x - 1$. Sa dérivée $f'(x) = 3x^2 - 1$ s'annule pour

$$x_1 = \frac{\sqrt{3}}{3} \quad \text{et} \quad x_2 = -\frac{\sqrt{3}}{3}$$

et on a le tableau de variations suivant :



avec

$$y_1 = f\left(\frac{\sqrt{3}}{3}\right) < -1,$$

$$y_2 = f\left(-\frac{\sqrt{3}}{3}\right) = -\frac{1}{3\sqrt{3}} - \frac{1}{\sqrt{3}} - 1 < 0 \quad \text{et} \quad f(0) = -1$$

Il en résulte que pour tout nombre réel x de $\left]-\infty, \frac{\sqrt{3}}{3}\right]$, $f(x) < 0$ et comme $f(x)$ tend vers $+\infty$ lorsque x tend vers $+\infty$, f s'annule une seule fois pour une valeur ω strictement supérieure à $\frac{\sqrt{3}}{3}$. Ce nombre réel ω est donc le seul qui vérifie $\omega^3 = \omega + 1$.

c) Soit $C(X) = r_0 X + r_1$ un polynôme du premier degré de $\mathbf{Q}[X]$. D'après la question précédente, les seuls polynômes de $\mathbf{R}[X]$ qui divisent A, admettent ω pour racine. Si on suppose que C et A ne sont pas premiers entre eux, on a $r_0 \omega + r_1 = 0$ donc $\omega = -\frac{r_1}{r_0}$ donc ω est dans $\mathbf{Q}$, ce qui est faux, donc C et A sont premiers entre eux. Soit maintenant $D(X) = r_0 X^2 + r_1 X + r_2$ un polynôme du second degré de $\mathbf{Q}[X]$. Si D divisait A, le quotient serait un polynôme du premier degré de $\mathbf{Q}[X]$ diviseur de A, ce qui est impossible. Il reste à envisager le cas où A et D auraient un diviseur commun du premier degré ; alors ω est racine de D et on a

$$\omega^2 = -\frac{r_1}{r_0}\omega - \frac{r_2}{r_0} \quad \text{avec} \quad \omega^3 = \omega + 1 = -\frac{r_1}{r_0}\omega^2 - \frac{r_2}{r_0}\omega.$$

Si $r_1 = 0$,

$$\omega + 1 = -\frac{r_2}{r_0}\omega$$

ce qui entraîne $\omega \in \mathbf{Q}$, donc $r_1 \neq 0$ et

$$\omega^2 = \frac{r_0}{r_1}\left(-1 - \frac{r_2}{r_0}\right)\omega - \frac{r_0}{r_1} = -\frac{r_2}{r_1}\omega - \frac{r_0}{r_1}.$$

En comparant les deux valeurs de ω^2 on trouve

$$\frac{r_1}{r_0}\omega - \frac{r_2}{r_0} = \frac{r_2}{r_1}\omega - \frac{r_0}{r_1}$$

et cette relation n'est possible que si $\omega \in \mathbf{Q}$ ou si

$$\frac{r_1}{r_0} = \frac{r_2}{r_1} \quad \text{et} \quad \frac{r_2}{r_0} = \frac{r_0}{r_1};$$

ces deux égalités entraînent

$$r_2 = \frac{r_1^2}{r_0} = \frac{r_0^2}{r_1} \quad \text{d'où} \quad r_1^3 = r_0^3 \quad \text{et} \quad r_0 = r_1 = r_2.$$

Alors $D(X) = r_0(X^2 + X + 1)$, qui est un polynôme irréductible dans $\mathbf{Q}[X]$, donc D ne peut avoir en aucun cas, ω pour racine et A et D sont premiers entre eux.

d) Si r_0, r_1, r_2 sont trois nombres rationnels, on vient de voir que

$$r_0\,\omega^2 + r_1\,\omega + r_2 = 0$$

n'est possible que si $r_0 = r_1 = r_2 = 0$ donc 1, ω, ω^2 sont linéairement indépendants sur $\mathbf{Q}$.

e) Soient $P_1(\omega)$, $P_2(\omega)$ deux éléments de F et r un nombre rationnel. On a

$$P_1(\omega) - P_2(\omega) = (P_1 - P_2)(\omega) \quad \text{et} \quad P_1 - P_2 \in \mathbf{Q}[X],$$
$$r.P_1(\omega) = (rP_1)(\omega) \quad \text{et} \quad r.P_1 \in \mathbf{Q}[X];$$

donc F est un sous-espace vectoriel de $\mathbf{R}$. Nous savons que la famille $(1, \omega, \omega^2)$ est libre, il suffit donc de montrer qu'elle engendre F. Comme tout élément de F est combinaison linéaire à coefficients dans $\mathbf{Q}$ des ω^n $(n \in \mathbf{N})$ il suffit de montrer que ces vecteurs s'écrivent en fonction de 1, ω, ω^2. La propriété est vraie pour $n = 0, 1, 2$. Supposons-la vraie pour $n - 1$, alors il existe trois rationnels r_0, r_1, r_2 tels que $\omega^{n-1} = r_0 + r_1\,\omega + r_2\,\omega^2$; mais alors

$$\omega^n = r_0\,\omega + r_1\,\omega^2 + r_2\,\omega^3 = r_0\,\omega + r_1\,\omega^2 + r_2(\omega + 1) =$$
$$= r_1 + (r_0 + r_2)\,\omega + r_1\,\omega^2,$$

ce qui prouve que ω^n est lui aussi combinaison linéaire de 1, ω, ω^2. Ceci achève de montrer que $(1, \omega, \omega^2)$ est une base de F.

f) Soit $a + b\omega + c\omega^2 = P(\omega)$ un élément non nul de F. Nous savons que le polynôme $P(X) = a + bX + cX^2$ est premier avec $A(X)$; d'après l'égalité de BEZOUT (*cf.* Q., Ch. 11, § II, n° 190) il existe deux polynômes U et V tels que $U.P + A.V = 1$; on a donc $U(\omega)\,P(\omega) + A(\omega)\,V(\omega) = 1$, or $A(\omega) = 0$ donc $U(\omega)\,P(\omega) = 1$; $U(\omega)$ est un élément de F donc $P(\omega)$ est inversible dans F et F est un sous-corps de $\mathbf{R}$.

III. *a*) Soient ξ_1 et ξ_2 deux éléments de F et r un nombre rationnel. Alors on a

$$f_\alpha(\xi_1 + \xi_2) = \alpha(\xi_1 + \xi_2) = \alpha\xi_1 + \alpha\xi_2 = f_\alpha(\xi_1) + f_\alpha(\xi_2)$$

et

$$f_\alpha(r\xi_1) = \alpha r\xi_1 = r(\alpha\xi_1) = rf_\alpha(\xi_1).$$

f_α est donc un endomorphisme de F. Comme F est de dimension finie, pour que f_α soit un automorphisme, il faut et suffit que f_α soit injectif c'est-à-dire que $\alpha\xi_1 = \alpha\xi_2$ entraîne $\xi_1 = \xi_2$. Il est clair que cette condition équivaut à $\alpha \neq 0$.

b) Nous savons que les vecteurs colonne de M sont les images des vecteurs de base (*cf.* Q., Ch. 9, § I, n° 155) ; or on a

$$f_\alpha(1) = \alpha.1 = a + b\omega + c\omega^2 ;$$

$$f_\alpha(\omega) = \alpha\omega = a\omega + b\omega^2 + c\omega^3 = a\omega + b\omega^2 + c(\omega + 1) =$$
$$= c + (a + c)\,\omega + b\omega^2$$

et

$$f_\alpha(\omega^2) = \alpha\omega^2 = a\omega^2 + b\omega^3 + c\omega^4 =$$
$$= a\omega^2 + b(\omega + 1) + c\omega(\omega + 1) = b + (b + c)\,\omega + (a + c)\,\omega^2,$$

donc

$$M = \begin{pmatrix} a & c & b \\ b & a + c & b + c \\ c & b & a + c \end{pmatrix} = M(a, b, c).$$

c) Soit f l'application de F dans $\mathscr{L}(F)$ qui à chaque élément α de F associe $f(\alpha) = f_\alpha$ et soit g l'application de l'ensemble G des fonctions f_α ($\alpha \in F$) dans E, qui à f_α fait correspondre $M(a, b, c)$. On a évidemment $\varphi = g \circ f$. Nous savons (*cf.* Q., Ch. 9, § I, n° 155) que g est un isomorphisme d'espaces vectoriels et d'anneaux. Montrons que f en est un. Soient α, β et ξ des éléments de F et r un nombre rationnel. On a

$$f(\alpha + \beta)(\xi) = f_{\alpha+\beta}(\xi) = (\alpha + \beta)(\xi) = \alpha\xi + \beta\xi =$$
$$= f_\alpha(\xi) + f_\beta(\xi) = \big(f(\alpha) + f(\beta)\big)(\xi)$$

donc $f(\alpha + \beta) = f(\alpha) + f(\beta)$; et

$$f(r\alpha)(\xi) = f_{r\alpha}(\xi) = (r\alpha)\,\xi = r(\alpha\xi) = rf_\alpha(\xi) = rf(\alpha)(\xi),$$

donc $f(r\alpha) = rf(\alpha)$. Par suite f est une application linéaire de F dans G. Supposons que $f(\alpha) = f(\beta)$; alors pour tout élément ξ de F on a

$$f(\alpha)(\xi) = f(\beta)(\xi) = f_\alpha(\xi) = f_\beta(\xi) = \alpha\xi = \beta\xi$$

ce qui n'est possible que si $\alpha = \beta$; donc f est injective. D'autre part, f est surjective par définition de G, donc f est un isomorphisme d'espaces vectoriels. De plus, on a quels que soient les éléments α, β, ξ de F,

$$f(\alpha\beta)(\xi) = f_{\alpha\beta}(\xi) = (\alpha\beta)\,\xi = \alpha(\beta\xi) = f_\alpha(\beta\xi) = f_\alpha\big(f_\beta(\xi)\big) = (f_\alpha \circ f_\beta)(\xi)$$

donc $f(\alpha\beta) = f(\alpha) \circ f(\beta)$, par suite f est aussi un isomorphisme d'anneaux. Il en résulte que $\varphi = g \circ f$ est aussi un isomorphisme d'espaces vectoriels et d'anneaux.

E étant isomorphe en tant qu'anneau à F qui est un corps, est muni aussi d'une structure de corps.

d) Le déterminant de $M(a, b, c)$ est non nul si et seulement si la matrice est inversible. E étant un corps, tous ses éléments sont inversibles sauf 0. Donc $\det M(a, b, c) = 0$ si et seulement si $a = b = c = 0$.