MP



Une collection dirigée par
Sylvain Rondy

Fiches-méthodes

Maths

Exercices corrigés

Maxime Bailleul
Jean-Paul Bonnet
Franck Nguyen Van Sang
Denis Petrequin

ellipses

Maths

MP



Une collection dirigée
par **Sylvain Rondy**

Maths

Maxime Bailleul
Professeur au lycée Robespierre à Arras

Jean-Paul Bonnet
Professeur au lycée Wallon à Valenciennes

Franck Nguyen Van Sang
Professeur au lycée Raspail à Paris

Denis Petrequin
Professeur au lycée Chateaubriand à Rennes

ellipses



Une collection dirigée
par **Sylvain Rondy**

Retrouvez tous les livres de la collection sur www.editions-ellipses.fr

La maquette de cet ouvrage a été adaptée en Latex par Stéphane Préteseille.

ISBN 9782340-033283
© Ellipses Édition Marketing S.A., 2019
32, rue Bargue 75740 Paris cedex 15

DANGER
LE
PHOTOCOPILLAGE
TUE LE LIVRE

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5.2° et 3°a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective », et d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).
Cette représentation ou reproduction, par quelque procédé que ce soit constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

www.editions-ellipses.fr

Sommaire

Algèbre générale

1 Reconnaitre un groupe, un anneau ou un corps par les axiomes 9
2 Montrer qu'une application est un morphisme de groupe ou un morphisme d'anneaux 14
3 Montrer qu'une partie d'un groupe (d'un anneau) est un sous-groupe (un sous-anneau) 17
4 Calculer et utiliser l'ordre d'un élément dans un groupe 21
5 Montrer qu'une partie d'un anneau est un idéal 26
6 Faire des calculs dans Z/nZ 30
7 Utiliser le théorème chinois 34

Algèbre linéaire

8 Montrer qu'une somme est directe 41
9 Montrer que des sous-espaces sont supplémentaires en dimension quelconque 45
10 Montrer que des sous-espaces sont supplémentaires en dimension finie 51

Réduction des endomorphismes

11 Calculer un polynôme caractéristique 57
12 Déterminer le spectre d'une matrice carrée sans le polynôme caractéristique 63
13 Montrer qu'un sous espace vectoriel est stable par un endomorphisme 68
14 Montrer qu'un endomorphisme (une matrice carrée) est diagonalisable « à la main » 74
15 Montrer qu'un endomorphisme (une matrice carrée) est trigonalisable et trigonaliser (cas n = 2 et n = 3) 81
16 Montrer qu'un endomorphisme (une matrice) est nilpotent(e) et l'utiliser 87
17 Calculer le polynôme minimal d'un endomorphisme (d'une matrice carrée) 92
18 Utiliser un polynôme annulateur d'un endomorphisme (d'une matrice carrée) 97
19 Montrer qu'un endomorphisme est diagonalisable en utilisant des polynômes annulateurs 102
20 Mettre en œuvre le lemme de décomposition des noyaux 107

Fonctions convexes

21 Montrer qu'une fonction est convexe 115
22 Utiliser les fonctions convexes pour démontrer des inégalités 118

Espaces vectoriels normés

23 Montrer qu'une partie d'un espace vectoriel est convexe 123
24 Montrer qu'une application est une norme 126
25 Montrer qu'une suite d'éléments d'un espace vectoriel normé converge ou diverge 131
26 Montrer que des normes sont équivalentes 136
27 Montrer qu'un ensemble est ouvert (ou fermé) avec définition ou stabilité 140
28 Calculer l'intérieur et l'adhérence d'un ensemble 145
29 Montrer qu'une partie est dense dans un ensemble 150
30 Montrer qu'une application est continue 155
31 Montrer qu'une partie est ouverte (ou fermée) avec une fonction continue 160
32 Montrer qu'une application linéaire est continue 163
33 Utiliser une fonction polynomiale en ses coordonnées 167
34 Montrer qu'une partie est compacte 170
35 Utiliser la compacité. Lien avec les applications continues 174
36 Montrer qu'un ensemble est connexe par arcs 178

Algèbre bilinéaire

37 Montrer qu'une application est un produit scalaire 183
38 Déterminer le projeté orthogonal sur un sous-espace vectoriel de dimension finie 187
39 Mettre en place le procédé d'orthonormalisation de Gram-Schmidt 194
40 Montrer qu'un endomorphisme d'un espace préhilbertien est symétrique 199
41 Montrer qu'un endomorphisme d'un espace préhilbertien est orthogonal 204
42 Utiliser le théorème spectral 208
43 Réduire une isométrie en dimension 3 212

Dénombrabilité et familles sommables

44 Montrer qu'un ensemble est dénombrable (ou pas) 221
45 Montrer qu'une famille est sommable et calculer sa somme 224

Séries numériques

46 Étudier la nature d'une série à termes positifs 231
47 Étudier la nature d'une série alternée 236
48 Étudier la nature d'une série qui n'est pas de signe constant 242
49 Utiliser le critère de d'Alembert 246

50 Reconnaitre un produit de Cauchy 250
51 Utiliser une comparaison suite-série 255
52 Mettre en place une comparaison série intégrale 260
53 Utiliser la sommation des relations de comparaison 268

Suites et séries de fonctions

54 Déterminer la limite simple d'une suite de fonctions. Cas des séries de fonctions 275
55 Étudier la convergence uniforme d'une suite de fonctions 279
56 Montrer qu'une série de fonctions converge uniformément en utilisant la convergence normale 284
57 Montrer qu'une série de fonctions qui ne converge pas normalement converge uniformément 288
58 Montrer que la limite d'une suite de fonctions est continue. Cas des séries de fonctions 292
59 Calculer des limites d'une fonction définie comme une somme de série 296
60 Intervertir une limite et une intégrale sur un segment par convergence uniforme 300
61 Intervertir une somme et une intégrale sur un segment par convergence uniforme 304
62 Montrer que la limite d'une suite de fonctions est de classe C1. Cas des séries de fonctions 308

Séries entières

63 Déterminer le rayon de convergence d'une série entière 317
64 Calculer la somme d'une série entière 323
65 Montrer qu'une fonction est développable en série entière et calculer son développement 329
66 Utiliser des séries entières pour résoudre des équations différentielles 334
67 Déterminer un développement en série entière en utilisant une équation différentielle 340

Intégration

68 Déterminer la nature d'une intégrale 349
69 Montrer qu'une fonction est (ou n'est pas) intégrable 355
70 Calculer une intégrale impropre à l'aide d'une intégration par parties 359
71 Calculer une intégrale impropre à l'aide d'un changement de variables 363
72 Utiliser l'intégration des relations de comparaison 368
73 Utiliser le théorème de convergence dominée 373
74 Utiliser le théorème d'intégration terme à terme 377
75 Étudier la continuité et la dérivabilité d'une intégrale à paramètre 383

Compléments de probabilité

76 Montrer qu'un ensemble est un événement 393
77 Utiliser la continuité d'une probabilité ; événements négligeables ou presque sûrs 396
78 Utiliser un système complet d'événements et la formule des probabilités totales 402
79 Utiliser la formule de Bayes 408
80 Utiliser les lois usuelles pour modéliser une expérience aléatoire 412
81 Montrer qu'une variable aléatoire admet une espérance finie et la calculer 418
82 Utiliser la formule de transfert pour calculer une espérance 424
83 Montrer qu'une variable aléatoire admet une variance et la calculer 428
84 Calculer la covariance de deux variables aléatoires 434
85 Calculer l'espérance et la variance d'une somme de variables aléatoires 437
86 Utiliser les inégalités de Markov et de Bienaymé-Tchebychev 442
87 Déterminer et utiliser une fonction génératrice 446

Exponentielle de matrices et équations différentielles

88 Résoudre un système différentiel linéaire homogène à coefficients constants 455
89 Résoudre une équation différentielle linéaire scalaire d'ordre 2 à l'aide d'une variation des constantes 461
90 Résoudre une équation différentielle linéaire scalaire d'ordre 2 à l'aide d'une indication 467
91 Calculer l'exponentielle d'une matrice 472
92 Utiliser la variation des constantes pour un système différentiel linéaire 478
93 Recoller des solutions d'une équation différentielle 482

Calcul différentiel

94 Calculer la dérivée en un point selon un vecteur ; calculer des dérivées partielles 491
95 Montrer qu'une fonction est différentiable et calculer une différentielle 496
96 Calculer les dérivées partielles d'une composée d'applications différentiables. Règle de la chaine 502
97 Rechercher les extrema d'une fonction 507
98 Résoudre une équation différentielle aux dérivées partielles 512

Algèbre générale



Reconnaitre un groupe, un anneau ou un corps par les axiomes



Quand on ne sait pas !

- On appelle groupe tout couple $(G, \star)$ où G est un ensemble et $\star$ est une loi de composition interne telle que
  - — La loi est associative
  - — Il existe un élément e appelé élément neutre de G tel que pour tout x de G,
  $$x \star e = e \star x = x$$
  - — Pour tout élément x, il existe un élément y tel que $x \star y = y \star x = e$.
  L'élément y est le symétrique de x

  Si de plus, la loi $\star$ est commutative, on dit que $(G, \star)$ est un groupe commutatif ou un groupe abélien.
- On appelle anneau tout triplet $(A, +, \times)$ où A est un ensemble et $+$ et $\times$ des lois de composition internes telles que
  - — $(A, +)$ soit un groupe abélien dont le neutre se note 0_A et s'appelle l'élément nul.
  - — La loi $\times$ est associative
  - — Il existe un élément 1_A tel que pour tout $x \in A$, $1_A \times x = x \times 1_A = x$
  - — La multiplication est distributive par rapport à l'addition, c'est-à-dire :
  $$\forall (x, y, z) \in A^3, x \times (y+z) = (x \times y) + (x \times z) \text{ et } (y+z) \times x = (y \times x) + (z \times x)$$

  Si $(A, +, \times)$ est un anneau et que la loi $\times$ est commutative, on dit que c'est un anneau commutatif.
- On appelle corps tout anneau commutatif $(A, +, \times)$ tel que tout élément non nul x de A admette un inverse, c'est-à-dire, un élément y tel que $x \times y = 1_A$.

Que faire ?

- Quand on veut démontrer que $(G, \star)$ (ou $(A, +, \times)$) est un groupe (ou un anneau), la meilleure méthode est de démontrer que c'est un sous-groupe (ou un sous-anneau) d'un groupe (ou anneau) connu. Cela sera abordé dans la fiche 3.

- Pour montrer, en revenant aux axiomes que $(G, \star)$ est un groupe, il faut vérifier que la loi est associative (ce qui est souvent assez formel), trouver l'élément neutre de la loi et, pour tout élément x exhiber son symétrique.

  EXEMPLE 1 Rappelons un exemple du cours. On veut montrer que si X est un ensemble, l'ensemble S_X des bijections de X dans X est un groupe pour la composition.

  — On vérifie que la loi $\circ$ est une loi interne de S_X. En effet si f et g sont des bijections de X dans X alors $f \circ g$ aussi.

  — La loi $\circ$ est associative. En effet si f, g et h appartiennent à S_X,

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

  — La fonction identité de X notée $\iota : X \to X$ est un élément neutre pour $\circ$ car, pour tout $x \in X$,

  $$(f \circ \iota)(x) = f(\iota(x)) = f(x) \text{ et } (\iota \circ f)(x) = \iota(f(x)) = f(x)$$

  — Toute fonction f de S_X admet un symétrique puisque, comme f est bijective, il existe une fonction g, elle même bijective vérifiant $f \circ g = g \circ f = \iota$. Il suffit de prendre pour g la bijection réciproque de f.

  On a bien montré que $(S_X, \circ)$ était un groupe. Notons que ce n'est pas un groupe abélien sauf si X a strictement moins de 3 éléments.

Conseils

Dans le cas des groupes, il ne faut pas se mélanger entre les notations additives et les notations multiplicatives. Plus précisément :

- quand on note un groupe additivement (le plus souvent dans le cas des groupe abéliens), l'élément neutre est noté 0 et le symétrique de x, que l'on appelle l'opposé se note $-x$. C'est le cas par exemple du groupe $(\mathbb{Z}, +)$.
- quand on note un groupe multiplicativement, l'élément neutre est noté 1 et le symétrique de x, que l'on appelle l'inverse se note x^{-1}. C'est le cas par exemple du groupe $(\mathrm{GL}_n(\mathbb{K}), \times)$.

Exemple traité

On considère l'opération $\top$ sur $X = \mathbb{R} \setminus \{-1\}$ définie par

$$\forall (x, y) \in X^2, x \top y = x + y + xy$$

1 Montrer que pour tout (x, y) dans X^2, $x \top y = (1 + x)(1 + y) - 1$.

2 Montrer que $(\mathbb{R}, \top)$ est un groupe.

SOLUTION

1 Soit x, y dans X, $(1+x)(1+y) = 1+x+y+xy = 1+x\top y$. La relation voulue s'en déduit.

2 Montrons les axiomes des groupes.

- On commence par remarquer que la loi $\top$ est une loi interne à X. En effet si x et y appartiennent à X alors $(1+x) \neq 0$ et $(1+y) \neq 0$ donc $(1+x)(1+y) \neq 0$ et de ce fait, $x\top y \neq -1$.
- Montrons que la loi $\top$ est associative. Soit x, y et z dans X, en utilisant le calcul précédent,

$$\begin{aligned}(x\top y)\top z &= (1+x\top y)(1+z)-1\\ &= (1+x)(1+y)(1+z)-1\\ &= (1+x)(1+y\top z)-1\\ &= x\top(y\top z)\end{aligned}$$

  La loi est bien associative
- On remarque que 0 est un élément neutre pour $\top$ car pour tout $x \in X$,

$$x\top 0 = 0\top x = x$$

- Pour $x \in X$, on cherche $y \in X$ tel que $x\top y = 0$. On est ramené à résoudre (en y) l'équation $x+y+xy = 0$. Elle est équivalente à $(1+x)y = -x$. Comme x est supposé dans X, $1+x \neq 0$ et ainsi l'unique solution est $y = -\frac{x}{1+x}$ qui appartient bien à X car $x \neq 1+x$. On vérifie de plus que, en posant $y = -\frac{x}{1+x}$, $y\top x = 0$.
  Finalement $y = -\frac{x}{1+x}$ est le symétrique de x pour la loi $\top$.

On a bien montré tous les axiomes du groupe donc $(X, \top)$ est un groupe (qui est abélien).

Exercices

EXERCICE 1.1 Soit A un ensemble, on considère $P = \mathcal{P}(A)$ l'ensemble des parties de l'ensemble A. Pour toutes parties X et Y de A, on appelle différence symétrique de X et Y et on note $X\Delta Y$ l'ensemble $(X \cup Y) \setminus (X \cap Y)$.
Si X est une partie de A, on note 1_X la fonction caractéristique de X :

$$1_X : \begin{array}{ccc} A & \mapsto & \{0,1\} \\ x & \mapsto & \begin{cases} 1 & \text{si } x \in X \\ 0 & \text{sinon} \end{cases} \end{array}$$

On pourra utiliser le fait que pour deux parties X et Y de A, $X = Y$ si et seulement si $1_X = 1_Y$.

1 Soit X et Y dans P. Montrer que $1_{X\Delta Y} = 1_X + 1_Y - 2 \times 1_X 1_Y$.
2 En déduire que (P, Δ) est un groupe abélien.
3 Soit X et Y dans P. Montrer que $1_{X\cap Y} = 1_X 1_Y$.
4 En déduire que $(P, \Delta, \cap)$ est un anneau commutatif.
5 Montrer que si A n'a pas qu'un seul élément alors $(P, \Delta, \cap)$ n'est pas un corps.

Pour vous aider à démarrer

EXERCICE 1.1

1 On pourra, pour un élément x de A, séparer selon que $x \in A \cap B$, $x \in A \setminus B, \ldots$
2 Utiliser la question précédente pour montrer l'associativité de Δ.
3 Faire le calcul.
4 Utiliser les applications caractéristiques pour montrer la distributivité.
5 Il suffit de montrer que si $X \neq A$ et $X \neq \varnothing$ alors il n'existe pas Y tel que $X \cap Y$ soit le neutre pour $\cap$.

Solutions des exercices

EXERCICE 1.1

1 Soit $x \in A$.
- Si $x \in X \cap Y$ (c'est-à-dire que x est dans X et dans Y), $1_X(x) = 1_Y(x) = 1$ et donc
$$(1_X + 1_Y - 2 \times 1_X 1_Y)(x) = 1 + 1 - 2 = 0 = 1_{X\Delta Y}(x)$$
En effet, x n'appartient pas à $X\Delta Y$.
- Si $x \in X \setminus Y$ (c'est-à-dire que x est dans X et pas dans Y), $1_X(x) = 1$ et $1_Y(x) = 0$ et donc
$$(1_X + 1_Y - 2 \times 1_X 1_Y)(x) = 1 + 0 - 0 = 1 = 1_{X\Delta Y}(x)$$
En effet, x appartient à $X\Delta Y$.
- On traite de même les cas où $x \in Y \setminus X$ et les cas où x n'est ni dans X ni dans Y.

2 Montrons les axiomes des groupes.
- Il est clair que Δ est une loi interne sur P.
- Montrons l'associativité. Soit $(X, Y, Z) \in P^3$.
On veut montrer que $(X\Delta Y)\Delta Z = X\Delta(Y\Delta Z)$. Pour cela, il suffit de montrer que $1_{(X\Delta Y)\Delta Z} = 1_{X\Delta(Y\Delta Z)}$. Or, d'après la question précédente :
$$\begin{aligned} 1_{(X\Delta Y)\Delta Z} &= 1_{X\Delta Y} + 1_Z - 2 \times 1_{X\Delta Y} 1_Z \\ &= 1_X + 1_Y - 2 \times 1_X 1_Y + 1_Z - 2(1_X + 1_X - 2 \times 1_X 1_Y)1_Z \\ &= 1_X + 1_Y + 1_Z - 2(1_X 1_Y + 1_Y 1_Z + 1_X 1_Z) + 4 \times 1_X 1_Y 1_Z \end{aligned}$$

Il suffit alors de calculer $1_{X\Delta(Y\Delta Z)}$ et de vérifier que l'on trouve la même expression.

- Comme l'union et l'intersection sont commutatives, la différence symétrique aussi.
- Vérifions que $\varnothing$ est un élément neutre pour Δ. Soit $X \in P$,

$$X\Delta\varnothing = (X \cup \varnothing) \setminus (X \cap \varnothing) = X \setminus \varnothing = X$$

De même, $\varnothing\Delta X = X$ donc $\varnothing$ est bien un élément neutre pour Δ.

- Soit $X \in P$. On cherche son symétrique Y tel que $X\Delta Y = \varnothing$. On remarque que

$$X\Delta X = (X \cup X) \setminus (X \cap X) = X \setminus X = \varnothing$$

On vient donc de voir que le symétrique de X est X lui même.

On a bien montré que (P, Δ) est un groupe abélien.

3 Soit X et Y dans P et $x \in A$,

$$x \in X \cap Y \iff x \in X \text{ et } x \in Y \iff 1_X(x) = 1_Y(x) = 1 \iff (1_X 1_Y)(x) = 1$$

Cela prouve que $1_{X\cap Y} = 1_X 1_Y$.

4 On a déjà vu que (P, Δ) était un groupe abélien. Montrons les axiomes qui restent.

- On sait que la relation $\cap$ est associative et commutative (on peut aussi le démontrer en utilisant la question précédente).
- La partie A elle même est un élément neutre pour $\cap$ car pour tout $X \in P$,

$$X \cap A = A \cap X = X.$$

- Soit X, Y et Z dans P, on veut montrer que $X\Delta(Y \cap Z) = (X\Delta Y) \cap (X\Delta Z)$. Pour cela, on va passer par les applications caractéristiques.

$$\begin{aligned} 1_{X\cap(Y\Delta Z)} &= 1_X 1_{Y\Delta Z} \\ &= 1_X(1_Y + 1_Z - 2 \times 1_Y 1_Z) \\ &= 1_X 1_Y + 1_X 1_Z - 2 \times 1_X 1_Y 1_Z \end{aligned}$$

D'autre part

$$\begin{aligned} 1_{(X\cap Y)\Delta(X\cap Z)} &= 1_{X\cap Y} + 1_{X\cap Z} - 2 \times 1_{X\cap Y} 1_{X\cap Z} \\ &= 1_X 1_Y + 1_X 1_Z - 2 \times 1_X^2 1_Y 1_Z \\ &= 1_X 1_Y + 1_X 1_Z - 2 \times 1_X 1_Y 1_Z \end{aligned}$$

La dernière égalité venant du fait que 1_X étant à valeur dans $\{0, 1\}$, $1_X^2 = 1_X$.

Finalement $(P, \Delta, \cap)$ est bien un anneau commutatif.

5 Soit X qui n'est ni A, ni vide (qui existe bien car A n'a pas qu'un seul élément). Pour tout $Y \in P$, $(X \cap Y) \subset X \subsetneq A$. On en déduit que $(X \cap Y) \neq A$ et donc que X n'est pas inversible dans l'anneau $(P, \Delta, \cap)$. On a exhibé un élément non nul qui n'est pas inversible donc l'anneau considéré n'est pas un corps.



2 Montrer qu'une application est un morphisme de groupe ou un morphisme d'anneaux

Quand on ne sait pas !

- Soit $(G, \star)$ et $(G', \top)$ deux groupes. Une application $f : G \to G'$ est un morphisme de groupes si pour tout $(g_1, g_2) \in G^2$, $f(g_1 \star g_2) = f(g_1) \top f(g_2)$.
- Soit $(A, +, \times)$ et $(A', +, \times)$ deux anneaux. Une application $f : A \to A'$ est un morphisme d'anneaux si
  - $\forall (x_1, x_2) \in A^2, f(x_1 + x_2) = f(x_1) + f(x_2)$
  - $\forall (x_1, x_2) \in A^2, f(x_1 \times x_2) = f(x_1) \times f(x_2)$
  - $f(1_A) = f(1_B)$ où 1_A est l'élément neutre pour la multiplication de A et 1_B l'élément neutre pour celle de B.

Un morphisme de groupes (ou d'anneaux) est donc une application qui est compatible avec les opérations des ensembles de départ et d'arrivée.

Que faire ?

Dans la très grande majorité des cas, aussi bien dans le cas des groupes que dans le cas des anneaux, il suffit juste de vérifier les axiomes de la définition.

EXEMPLE 1 Soit $n \geq 2$. On considère le groupe S_n des permutations de n éléments. Soit σ une permutation de S_n, on considère $\varphi : S_n \to S_n$ définie par $\varphi : \tau \mapsto \sigma\tau\sigma^{-1}$. On veut montrer que φ est un morphisme de groupes.
Pour tout $(\tau_1, \tau_2) \in S_n^2$,

$$\varphi(\tau_1)\varphi(\tau_2) = \sigma\tau_1\sigma^{-1}\sigma\tau_2\sigma^{-1} = \sigma\tau_1\tau_2\sigma^{-1} = \varphi(\tau_1\tau_2)$$

On a bien montré que φ est un morphisme de groupes.

EXEMPLE 2 Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ l'anneau des polynômes à coefficients dans $\mathbb{K}$.
Soit $\alpha \in \mathbb{K}$, on considère l'application ε d'évaluation en α.

$$\begin{array}{rccc} \varepsilon : & \mathbb{K}[X] & \to & \mathbb{K} \\ & P & \mapsto & P(\alpha) \end{array}$$

On veut vérifier que ε_α est un morphisme d'anneaux.

- Soit $(P_1, P_2) \in (\mathbb{K}[X])^2$,

$$\varepsilon(P_1 + P_2) = (P_1 + P_2)(\alpha) = P_1(\alpha) + P_2(\alpha) = \varepsilon(P_1) + \varepsilon(P_2)$$

- Soit $(P_1, P_2) \in (\mathbb{K}[X])^2$,

$$\varepsilon(P_1 \times P_2) = (P_1 \times P_2)(\alpha) = P_1(\alpha) \times P_2(\alpha) = \varepsilon(P_1) \times \varepsilon(P_2)$$

- L'unité de $\mathbb{K}[X]$ est le polynôme constant égal à $1_{\mathbb{K}}$ que l'on va noter $\mathbf{1}$. On a alors,

$$\varepsilon(\mathbf{1}) = \mathbf{1}(\alpha) = 1_{\mathbb{K}}$$

On a bien montré que ε était un morphisme d'anneaux.

Conseils

Il faut faire attention aux opérations des ensembles de départ et d'arrivée. Par exemple le logarithme néperien est un morphisme de groupes de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$ car pour tout x, y réels strictement positifs, $\ln(x \times y) = \ln(x) + \ln(y)$.

Exercices

EXERCICE 2.1

On considère les applications φ et ψ définies de $\mathbb{Z}$ dans $\mathcal{M}_2(\mathbb{C})$ par

$$\varphi : n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \text{ et } \psi : n \mapsto \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}.$$

1 **a.** Montrer que pour tout entier relatif n, $\varphi(n)$ est inversible.

b. Montrer que φ est un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(\mathrm{GL}_2(\mathbb{C}), \times)$.

2 L'application ψ est-elle un morphisme d'anneaux de $(\mathbb{Z}, +, \times)$ dans $(\mathcal{M}_2(\mathbb{C}), +, \times)$?

Pour vous aider à démarrer

EXERCICE 2.1

1 **a.** On pourra, par exemple, calculer le déterminant de $\varphi(n)$ pour $n \in \mathbb{Z}$.

b. Vérifier les axiomes d'un morphisme de groupes.

2 Bien penser à essayer de vérifier tous les axiomes d'un morphisme d'anneaux.

EXERCICE 2.1

1 **a.** Soit $n \in \mathbb{Z}$. On a

$$\det(\varphi(n)) = \begin{vmatrix} 1 & n \\ 0 & 1 \end{vmatrix} = 1 \neq 0$$

On en déduit que $\varphi(n)$ est inversible.

b. Soit n, m deux entiers relatifs,

$$\varphi(n) \times \varphi(m) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix} = \varphi(n+m)$$

Cela montre que φ est un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(\mathcal{M}_2(\mathbb{C}), \times)$.

2 Un calcul simple montre que ψ vérifie les deux premiers axiomes des morphismes d'anneaux ; en effet pour n, m deux entiers relatifs

$$\psi(n) + \psi(m) = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n+m & 0 \\ 0 & 0 \end{pmatrix} = \psi(n+m)$$

et

$$\psi(n) \times \psi(m) = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} nm & 0 \\ 0 & 0 \end{pmatrix} = \psi(nm)$$

Cependant, ce n'est pas un morphisme d'anneaux car $\psi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq I_2$. Donc l'image par ψ du neutre pour la multiplication de $\mathbb{Z}$ n'est pas le neutre pour celle de $\mathcal{M}_2(\mathbb{C})$.

Montrer qu'une partie d'un groupe (d'un anneau) est un sous-groupe (un sous-anneau)



Quand on ne sait pas !

- Soit $(G, \star)$ un groupe. Un sous-groupe de G est une partie H stable par la loi $\star$ et qui est un groupe pour la loi induite par $\star$.
- Soit $(A, +, \times)$ un anneau. Un sous-anneau de A est une partie B telle que $(B, +)$ soit un sous-groupe de $(A, +)$, qui contient 1_A et qui est stable par multiplication.

Que faire ?

Il y a deux méthodes principales pour montrer qu'une partie H est un sous-groupe d'un groupe G.

- On peut montrer qu'une partie H est un sous-groupe d'un groupe G en utilisant la caractérisation suivante : une partie H est un sous-groupe si H n'est pas vide et que pour x, y dans H, $xy^{-1} \in H$. Noter qu'ici, on a utilisé une notation multiplicative du groupe ; dans le cas d'un groupe noté additivement il faut montrer que si x et y appartiennent à H alors $x - y \in H$.

  EXEMPLE 1 Soit n un entier naturel non nul, on note $U_n = \{z \in \mathbb{C}\ ,\ z^n = 1\}$ l'ensemble des racines n-ièmes de l'unité. On va montrer que c'est un sous-groupe du groupe $(\mathbb{C}^*, \times)$ où $\mathbb{C}^*$ est l'ensemble des nombres complexes non nuls.

  Il est clair que $U_n \subset \mathbb{C}^*$ puisque $0^n = 0 \neq 1$.

  On montre que U_n n'est pas vide car $1 \in U_n$ puisque $1^n = 1$.

  Maintenant, soit z_1, z_2 dans U_n,

$$\left(\frac{z_1}{z_2}\right)^n = \frac{z_1^n}{z_2^n} = \frac{1}{1} = 1$$

  On a donc $z_1 z_2^{-1} \in U_n$ et de ce fait, $(U_n, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$
- On sait que si G et H sont deux groupes et $\varphi : G \to H$ un morphisme de groupes alors le noyau Ker (φ) est un sous-groupe de G et l'image Im (φ) est un sous-groupe de H. On peut donc, quand on cherche à montrer qu'une partie d'un groupe est un sous-groupe, essayer de l'écrire comme une image ou un noyau d'un morphisme de groupes.

EXEMPLE 2 Soit n un entier non nul. L'ensemble $\mathrm{SL}_n(\mathbb{C})$ des matrices de déterminant 1 est un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$. En effet, c'est le noyau de l'application déterminant

$$\det : (\mathrm{GL}_n(\mathbb{C}), \times) \to (\mathbb{C}, \times)$$

qui est un morphisme de groupes.

Conseils

- Quand on cherche à montrer qu'une partie H est un sous-groupe de G, pour vérifier qu'elle n'est pas vide, le plus simple est souvent de montrer que l'élément neutre de G appartient à H.
- Pour montrer qu'une partie est un sous-anneau, on ne peut pas, comme dans le cas des groupes, montrer que c'est le noyau d'un morphisme d'anneaux car un tel noyau a une structure d'idéal et non de sous-anneau - voir la fiche 5.

Exemple traité

Soit $n \geq 1$. On note T_n l'ensemble des matrices triangulaires supérieures de $\mathcal{M}_n(\mathbb{C})$. Pour tout $(i,j) \in [\![1,n]\!]^2$ on considère $E_{i,j}^*$ l'application linéaire définie de $\mathcal{M}_n(\mathbb{C})$ dans $\mathbb{C}$ qui associe à une matrice M son coefficient $[M]_{i,j}$ placé à la i-ème ligne et j-ème colonne.

1 Caractériser T_n à l'aide des application $E_{i,j}^*$. En déduire que T_n est un sous-groupe de $(\mathcal{M}_n(\mathbb{C}), +)$

2 Montrer que T_n est un sous-anneau de $(\mathcal{M}_n(\mathbb{C}), +, \times)$.

SOLUTION

1 Par définition, pour toute matrice M de $\mathcal{M}_n(\mathbb{C})$,

$$M \in T_n \iff \forall i \in [\![2,n]\!], \forall j \in [\![1,i-1]\!], E_{i,j}^*(M) = 0.$$

On peut donc écrire que $T_n = \bigcap_{1 \leq j < i \leq n} \mathrm{Ker}\, E_{i,j}^*$.

Or, les applications $E_{i,j}^*$ sont linéaires donc ce sont des morphismes de groupes (pour la loi $+$). On en déduit que pour tout $(i,j) \in [\![1,n]\!]^2$, $\mathrm{Ker}\, E_{i,j}^*$ est un sous-groupe de $(\mathcal{M}_n(\mathbb{C}), +)$. Une intersection de sous-groupes étant aussi un sous-groupe, T_n est un sous-groupe de $(\mathcal{M}_n(\mathbb{C}), +)$.

2 Pour montrer que T_n est un sous-anneau de $(\mathcal{M}_n(\mathbb{C}), +, \times)$, on doit de plus montrer que l'élément neutre (multiplicatif) de $\mathcal{M}_n(\mathbb{C})$ est dans T_n et que T_n est stable par multiplication.

- L'élément neutre pour la multiplication est la matrice identité I_n qui est bien un élément de T_n.

- Soit M, N deux éléments de T_n. On veut montrer que $MN \in T_n$. Soit $(i,j) \in [\![1,n]\!]^2$ tels que $i > j$,

$$[MN]_{i,j} = \sum_{k=1}^{n} [M]_{i,k}[N]_{k,j}$$

or, pour $k > j$, $[N]_{k,j} = 0$ et, pour $k \leq j < i$, $[M]_{i,k} = 0$. On obtient alors que $[MN]_{i,j} = 0$ et donc que $MN \in T_n$.

On a bien montré que T_n est un sous-anneau de $(\mathcal{M}_n(\mathbb{C}), +, \times)$. Notons de fait, que c'est même une sous-algèbre.

Exercices

EXERCICE 3.1

Soit $(G, \star)$ un groupe d'élément neutre e. Pour (x,y) dans G^2, on notera xy pour $x \star y$. On appelle centre du groupe et on note $Z(G)$ l'ensemble défini par

$$Z(G) = \{x \in G, \forall y \in G, xy = yx\}$$

1 Montrer que $Z(G)$ est un sous-groupe en utilisant la caractérisation des sous-groupes.

2 **a.** Soit $y \in G$, montrer que $\varphi_y : G \to G$ défini par $\varphi_y : x \mapsto yxy^{-1}$ est un morphisme de groupes

b. Montrer que si f et g sont deux morphismes de groupes de G dans G alors

$$K = \{x \in G, f(x) = g(x)\}$$

est un sous-groupe de G.

c. En utilisant les deux questions précédentes, remontrer que $Z(G)$ est un sous-groupe de G.

EXERCICE 3.2

On considère l'ensemble $A = \mathbb{Z}[i]$ défini par

$$\mathbb{Z}[i] = \{a + ib, (a,b) \in \mathbb{Z}^2\}$$

Montrer que A est un sous-anneau de $\mathbb{C}$.

Pour vous aider à démarrer

EXERCICE 3.1

1 Commencer en trouvant un élément de $Z(G)$

2 **a.** Revenir à la définition.

b. Utiliser la caractérisation classique des sous-groupes.

c. On pourra considérer l'application identité qui est un morphisme de G dans G.

EXERCICE 3.1

1 On remarque que $Z(G)$ n'est pas vide car l'élément neutre e de G appartient à $Z(G)$ puisque pour tout y dans G, $ey = ye = y$.
Maintenant si x et y appartiennent à $Z(G)$. Pour tout $z \in G$, on sait que $yz = zy$ et donc, en multipliant par y^{-1} à droite et à gauche des deux cotés, $zy^{-1} = y^{-1}z$. On en déduit que

$$xy^{-1}z = xzy^{-1} = zxy^{-1}$$

et donc $xy^{-1} \in Z(G)$.
En conclusion $Z(G)$ est un sous-groupe de G.

2 **a.** Soit $y \in G$, pour tous x, x' dans G,

$$\varphi_y(xx') = yxx'y^{-1} = yxy^{-1}yx'y^{-1} = \varphi_y(x)\varphi_y(x')$$

On a bien montré que φ_y est un morphisme de groupes.

b. Soit f et g deux morphismes de G dans G et notons $K = \{x \in G, f(x) = g(x)\}$.
On sait que $f(e) = e$, en effet, $f(e) = f(ee) = f(e)f(e)$.
On en déduit que $e \in K$ car $f(e) = e = g(e)$. De ce fait, $K \neq \varnothing$.
De plus, pour $(x, y) \in K^2$,

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

donc $xy^{-1} \in K$. On a bien vérifié que K était un sous-groupe de G.

c. Soit $y \in G$, on regarde les morphismes de groupes φ_y et l'identité. On constate alors que $K_y = \{x \in G, \varphi_y(x) = \mathrm{id}_G(x)\} = \{x \in G, yxy^{-1} = x\}$ est un sous-groupe de G. Il suffit ensuite de réécrire que $K_y = \{x \in G, yx = xy\}$ et de voir que

$$Z(G) = \bigcap_{y \in G} K_y$$

pour conclure que $Z(G)$ est un sous-groupe de G comme intersection de sous-groupes de G.

EXERCICE 3.2

On vérifie pour commencer que $(A, +)$ est un sous-groupe abélien de $(\mathbb{C}, +)$.

- Comme $0 = 0 + 0i \in A$, $A \neq \varnothing$.
- Soit $x = a + ib$ et $x' = a' + ib'$ des éléments de A où a, a', b et b' sont des entiers relatifs, $x - x' = (a - a') + i(b - b') \in A$.

De plus l'élément neutre pour la multiplication de $\mathbb{C}$ appartient à A car $1 = 1 + 0i$. Pour finir, si x et x' appartiennent à A, en reprenant les notations ci-dessus,

$$xx' = (a + ib) \times (a' + ib') = (aa' - bb') + (ab' + a'b)i \in A$$

On a bien montré que $(A, +, \times)$ était un sous-anneau de $(\mathbb{C}, +, \times)$.

Calculer et utiliser l'ordre d'un élément dans un groupe



Dans cette fiche $(G, \times)$ désigne un groupe. L'élément neutre sera noté e.

Quand on ne sait pas !

Soit x un élément de G.

- On dit que x est d'ordre fini s'il existe un entier $n \geq 1$ tel que $x^n = e$.
- Si x est d'ordre fini, on appelle ordre de x le plus petit entier n strictement positif tel que $x^n = e$.
- Si x est d'ordre fini et d'ordre n, pour tout entier m, $x^m = e \iff n|m$.
- Le théorème de Lagrange affirme que, si G est fini, l'ordre de x divise le cardinal de G.

Que faire ?

- Pour déterminer l'ordre d'un élément x, il faut trouver un entier n tel que $x^n = e$ et que, pour tout entier k compris entre 1 et $n-1$, $x^k \neq e$.

  EXEMPLE 1 On considère le groupe multiplicatif $\mathbb{U}_6 = \{\exp(\frac{2ik\pi}{6}) \ , \ k \in [\![0, 5]\!]\}$ des racines 6-ièmes de l'unité dans $\mathbb{C}$. L'élément $j = \exp(\frac{2i\pi}{3})$ est d'ordre fini car $j^6 = 1$ (ici l'élément neutre pour $\times$ est 1) par définition. Cependant, j n'est pas d'ordre 6 car $j^3 = 1$. On en déduit que j est d'ordre 3 car $j \neq 1$ et $j^2 \neq 1$.
- On peut utiliser l'ordre d'un élément x pour calculer les puissances de x. En effet si x est d'ordre n, la valeur de x^m ne dépend que de la congruence modulo n de m.

  EXEMPLE 2 Si on reprend l'exemple de $j \in \mathbb{C}$. Il est d'ordre 3, de ce fait, j^m ne dépend que de la congruence de m modulo 3.

$$j^m = \begin{cases} 1 & \text{si } m \equiv 0 \ [3] \\ j & \text{si } m \equiv 1 \ [3] \\ j^2 & \text{si } m \equiv 2 \ [3] \end{cases}$$

Conseils

- Pour déterminer l'ordre d'un élément x on peut commencer par trouver un entier m tel que $x^m = e$. On cherche alors l'ordre de x parmi les diviseurs de m.
- Pour déterminer l'ordre d'un élément x, on peut écrire x comme produit d'éléments **commutant entre eux**.

Exemple traité

On considère dans S_9 la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 9 & 1 & 2 & 3 & 4 & 6 & 8 \end{pmatrix}$$

1 Déterminer l'ordre de σ.

2 En déduire σ^{2000}.

SOLUTION

1 On commence en décomposant σ en produit de cycles **à supports disjoints**. On pose $\gamma_1 = (1, 7, 4)$, $\gamma_2 = (2, 5)$ et $\gamma_3 = (3, 9, 8, 6)$. On a alors $\sigma = \gamma_1 \circ \gamma_2 \circ \gamma_3$ où les trois cycles γ_1, γ_2 et γ_3 commutent car ils ont des supports deux à deux disjoints. De ce fait, pour tout entier m, $\sigma^m = \gamma_1^m \circ \gamma_2^m \circ \gamma_3^m$.

Maintenant, γ_1 est un 3-cycle, il est d'ordre 3, γ_2 est une transposition qui est d'ordre 2 et γ_3 est un 4-cycle qui est d'ordre 4. On en déduit finalement que, en notant id l'élément neutre de S_9,

$$\sigma^m = \text{id} \iff (3|m \text{ et } 2|m \text{ et } 4|m) \iff (3 \vee 2 \vee 4)|m \iff 12|m$$

On obtient que σ est d'ordre 12.

2 On réalise la division euclidienne de 2000 par 12 : $2000 = 166 \times 12 + 8$. On en déduit que

$$\sigma^{2000} = \sigma^8 = \gamma_1^8 \circ \gamma_2^8 \circ \gamma_3^8 = \gamma_1^2$$

Finalement, $\sigma^{2000} = (1, 4, 7)$.

Exercices

EXERCICE 4.1

On considère dans $\mathcal{M}_n(\mathbb{C})$ la matrice

$$J = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & & & \ddots & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{pmatrix}$$

On note $u : \mathbb{C}^n \to \mathbb{C}^n$ l'endomorphisme canonique associé à J ainsi que $(e_0, \ldots, e_{n-1})$ la base canonique de $\mathbb{C}^n$.

1. Soit $i \in [\![0, n-1]\!]$, calculer $u^n(e_i)$.
2. Déterminer alors l'ordre de J dans le groupe $\mathrm{GL}_n(\mathbb{C})$.
3. En déduire que J est diagonalisable.

EXERCICE 4.2

On considère $(G, \times)$ un groupe commutatif. Soit x et y deux éléments de G. On suppose que x est d'ordre n et y est d'ordre m.

1. On suppose dans cette question que n et m sont premiers entre eux. Montrer que xy est d'ordre nm.
2. Montrer qu'il existe un élément d'ordre $n \vee m$.
3. Le résultat de la question 1. est-il encore vrai si le groupe n'est plus supposé commutatif?

Pour vous aider à démarrer

EXERCICE 4.1

1. Commencer en calculant $u(e_0)$, $u^2(e_0)$ ...
2. Déduire la valeur de J^n de la question précédente.
3. Utiliser un polynôme annulateur.

EXERCICE 4.2

1. Montrer que $(xy)^{nm} = e$ et que si k est un entier tel que $(xy)^k = e$ alors $n|k$ et $m|k$.
2. Commencer par montrer que, pour tout diviseur d de n ou de m, il existe un élément d'ordre d puis utiliser la décomposition en produit de nombres premiers de n et m.
3. On pourra travailler dans le groupe S_3 qui n'est pas commutatif.

EXERCICE 4.1

1 Avec les notations de l'énoncé, on a : $\forall i \in [\![0, n-1]\!]$, $u(e_i) = \begin{cases} e_{i-1} & \text{si } i \geq 1 \\ e_{n-1} & \text{si } i = 0 \end{cases}$

En recommençant, $u^2(e_i) = u(u(e_i)) = \begin{cases} e_{i-2} & \text{si } i \geq 2 \\ e_{n-2+i} & \text{sinon} \end{cases}$

En composant encore avec u plusieurs fois, on obtient, si $k \in [\![1, n-1]\!]$:

$$u^k(e_i) \begin{cases} e_{i-k} & \text{si } i \geq k \\ e_{n-k+i} & \text{sinon} \end{cases}$$

Finalement, $u^n(e_i) = e_{n-n+i} = e_i$.

2 La matrice J^n est la matrice de l'endomorphisme u^n dans la base canonique. Comme u^n est l'identité de $\mathbb{C}^n$, on obtient : $J^n = I_n$.

Pour justifier alors que l'ordre de J dans le groupe $\mathrm{GL}_n(\mathbb{C})$ est égal à n, il reste à montrer que si $k \in [\![1, n-1]\!]$, la matrice J^k n'est pas égal à I_n, ce qui revient à montrer que u^k n'est pas l'endomorphisme identité. Il suffit pour cela de remarquer que $u^k(e_{n-1}) = e_{n-1-k} \neq e_{n-1}$.

Finalement J est une matrice d'ordre n.

3 D'après la question précédente, $J^n = I_n$. Cela signifie que le polynôme $X^n - 1$ annule la matrice J. On sait, en notant $\omega = \exp(\frac{2i\pi}{n})$ que $X^n - 1 = \prod_{k=0}^{n-1} (X - \omega^k)$.

On a donc montré que J était annulé par un polynôme scindé à racines simples. Cela implique que J est diagonalisable.

EXERCICE 4.2

1 On commence par vérifier que $(xy)^{nm} = (x^n)^m \times (y^m)^n = e$ puisque le groupe G est supposé commutatif.

Maintenant, soit k un entier tel que $(xy)^k = e$. On a alors $x^k = y^{-k}$. De ce fait, $x^{km} = (y^m)^{-k} = e$ car y est d'ordre m. On en déduit, comme x est d'ordre n, que n divise km mais comme n et m sont premiers entre eux, $n|k$ d'après le lemme de Gauss. Par symétrie, on montre aussi que $m|k$ et donc que $nm|k$ car n et m sont premiers entre eux.

Finalement, on en déduit que xy est d'ordre nm.

2 Soit d un diviseur de n. Par définition, il existe un entier k tel que $n = kd$. Montrons alors que $z = x^k$ est d'ordre d. En effet $z^d = (x^k)^d = x^{kd} = x^n = e$. De plus pour tout $d' \in [\![1, d-1]\!]$, $z^{d'} = x^{kd'} \neq e$ car $1 \leq kd' < kd = n$.

De même, si d est un diviseur de m, on peut trouver une puissance de y qui est d'ordre m.

Notons maintenant,

$$n = \prod_{i=1}^{s} p_i^{\alpha_i} \text{ et } m = \prod_{i=1}^{s} p_i^{\beta_i}$$

les décompositions en produit de nombres premiers de n et m où α_i et β_i appartiennent à $\mathbb{N}$ (on a $\alpha_i = 0$ si p_i ne divise pas n et de même $\beta_i = 0$ si p_i ne divise pas m).

On sait alors que $n \vee m = \prod_{i=1}^{s} p_i^{\gamma_i}$ où $\gamma_i = \max(\alpha_i, \beta_i)$. Or, pour tout entier i compris entre 1 et s, $p_i^{\gamma_i}$ divise n ou m. Il existe donc un élément z_i de G d'ordre $p_i^{\gamma_i}$. En utilisant alors la question 1. et le fait que pour i et j distincts dans $[\![1, s]\!]$, $p_i^{\gamma_i}$ et $p_j^{\gamma_j}$ sont premiers entre eux, on en déduit que $z_1 \times z_2 \times \cdots \times z_s$ est d'ordre $n \vee m$.

3 Le résultat n'est plus vrai. Par exemple dans S_3, si on prend pour x la transposition $(1, 2)$ et pour y le 3-cycle, $(1, 2, 3)$ qui sont d'ordre 2 et 3 respectivement. Le calcul montre que $x \circ y$ est la transposition $(2, 3)$ qui est d'ordre 2 et non 6.



5 Montrer qu'une partie d'un anneau est un idéal

Quand on ne sait pas !

Soit $(A, +, \times)$ un anneau commutatif.

Une partie I de A est un idéal de A si

- $(I, +)$ est un sous-groupe de $(A, +)$.
- Pour tout $x \in I$ et tout $a \in A$, $ax \in I$ (ou si l'on veut $xa \in I$).

Que faire ?

- Pour montrer qu'une partie I d'un anneau est un idéal, on montre qu'elle vérifie les deux axiomes.

  EXEMPLE 1 Soit A l'anneau des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ muni des lois usuelles. Précisément, pour toutes fonctions f et g dans A, les fonctions $f + g$ et $f \times g$ sont définies par :

  $$\forall x \in \mathbb{R}, (f + g)(x) = f(x) + g(x) \text{ et } (f \times g)(x) = f(x) \times g(x)$$

  On considère alors $\alpha \in \mathbb{R}$ et I_α l'ensemble des fonctions qui s'annulent en α. Montrons que c'est un idéal de A

  On vérifie pour commencer que c'est un sous-groupe (pour la loi $+$). En effet, $I_\alpha \neq \varnothing$ car la fonction nulle appartient à I_α. De plus, si f et g appartiennent à I_α, $f - g$ aussi, en effet :

  $$(f - g)(\alpha) = f(\alpha) - g(\alpha) = 0 - 0 = 0$$

  On vérifie alors la deuxième condition. Si $f \in I_\alpha$ et g est une fonction quelconque de A, $f \times g \in I_\alpha$ car

  $$(f \times g)(\alpha) = f(\alpha) \times g(\alpha) = 0 \times g(\alpha) = 0$$

  On a bien vérifié que I_α était un idéal de A.
- Si A et B sont deux anneaux et que $\varphi : A \to B$ est un morphisme d'anneaux, on peut vérifier aisément que le noyau $\text{Ker}(\varphi) = \{x \in A \ , \ \varphi(x) = 0_B\}$ est un idéal de A. De ce fait, pour montrer qu'une partie I de A est un idéal, on peut essayer d'exhiber un morphisme d'anneaux dont c'est le noyau.

EXEMPLE 2 Si on reprend les notations de l'exemple ci-dessus, on peut considérer l'application d'évaluation ε définie par

$$\begin{array}{rccc} \varepsilon : & A & \to & \mathbb{R} \\ & f & \mapsto & f(\alpha) \end{array}$$

Il est clair que $I_\alpha = \{f \in A\ ,\ f(\alpha) = 0\} = \text{Ker}\ (\varepsilon)$. Comme ε est un morphisme d'anneaux, on retrouve que I_α est un idéal de A.

Conseils

Il est important de ne pas confondre idéal et sous-anneau (voir fiche 3). Dans les deux cas, ce sont des sous-groupes additifs de l'anneau, cependant :

- On impose une condition de stabilité pour la multiplication plus forte dans le cas de l'idéal, en effet, on demande qu'un produit soit un élément de l'idéal dès que l'un des deux éléments appartient à l'idéal.
- On impose que l'élément neutre de la multiplication de l'anneau (l'unité) appartienne au sous-anneau, ce qui n'est pas le cas pour les idéaux. De fait, il n'existe qu'un seul idéal qui contienne l'unité de l'anneau, c'est l'anneau dans sa totalité.

Exemple traité

Soit $(A, +, \times)$ un anneau commutatif. Soit I et J deux idéaux de A.
Montrer que $I + J = \{a + b, (a, b) \in I \times J\}$ et $I \cap J$ sont des idéaux de A.

SOLUTION

- Montrons que $I + J$ est un idéal. Comme I et J ne sont pas vides, $I + J$ n'est pas vide. De plus soit $x_1 = a_1 + b_1$ et $x_2 = a_2 + b_2$ des éléments de $I + J$ où a_1, a_2 appartiennent à I et b_1, b_2 appartiennent à J,

$$x_1 - x_2 = (a_1 - a_2) + (b_1 - b_2) \in I + J$$

car $a_1 - a_2 \in I$ et $b_1 - b_2 \in J$.
De plus, soit $x = a + b \in I + J$ et $c \in A$, $ca \in I$ et $cb \in J$ car ce sont des idéaux donc $cx \in I + J$.
On a bien montré que $I + J$ était un idéal de A.
- Montrons que $I \cap J$ est un idéal. Comme $0 \in I$ et $0 \in J$ alors $0 \in I \cap J$ donc $I \cap J \neq \varnothing$.
Soit x_1 et $x_2 \in I \cap J$, alors x_1 et x_2 appartiennent à I et donc $x_1 - x_2 \in I$. De même, $x_1 - x_2 \in J$. Finalement, $x_1 - x_2 \in I \cap J$.
De plus, pour $x \in I \cap J$ et $c \in A$, $cx \in I$ et $cx \in J$ car I et J sont des idéaux et donc $cx \in I \cap J$.
On a bien montré que $I \cap J$ était un idéal.

Exercices

EXERCICE 5.1

On considère l'anneau commutatif $(\mathbb{Z}, +, \times)$. On rappelle que pour tout idéal I de $\mathbb{Z}$, il existe un unique entier positif a tel que

$$I = a\mathbb{Z} = \{am, m \in \mathbb{Z}\}$$

1 Montrer que si I et J sont deux idéaux de $\mathbb{Z}$ alors $IJ = \{ab, (a, b) \in I \times J\}$ est un idéal.

2 Trouver deux idéaux I et J tels que $I \cup J$ ne soit pas un idéal.

EXERCICE 5.2

Soit $(A, +, \times)$ un anneau commutatif. Soit I un idéal de A, on appelle radical de I et on note $\sqrt{I}$ l'ensemble

$$\sqrt{I} = \{x \in A, \exists n \in \mathbb{N}^*, x^n \in I\}$$

1 Montrer que $\sqrt{I}$ est un idéal.

2 En déduire que $N = \{x \in A, \exists n \in \mathbb{N}^*, x^n = 0\}$ l'ensemble des éléments nilpotents de A est un idéal.

3 Déterminer $\sqrt{I}$ dans le cas où $A = \mathbb{Z}$ et $I = 18\mathbb{Z}$.

Pour vous aider à démarrer

EXERCICE 5.1

1 On pourra commencer par écrire $I = a\mathbb{Z}$ et $J = b\mathbb{Z}$.

2 Considérer $2\mathbb{Z} \cup 3\mathbb{Z}$.

EXERCICE 5.2

1 Afin de montrer que $\sqrt{I}$ est un sous-groupe, on pourra utiliser la formule du binôme de Newton.

2 Déterminer un idéal I tel que $N = \sqrt{I}$.

3 Penser à la décomposition en facteurs premiers.

Solutions des exercices

EXERCICE 5.1

1 D'après la structure des idéaux de $\mathbb{Z}$, il existe des entiers a et b tels que $I = a\mathbb{Z}$ et $J = b\mathbb{Z}$. De ce fait, tout élément de IJ est de la forme $am \times am'$ où m et m' sont des entiers donc $IJ \subset ab\mathbb{Z}$. Réciproquement tout élément x de $ab\mathbb{Z}$ s'écrit sous la forme

$$x = abm = a(bm)$$

où $m \in \mathbb{Z}$. De ce fait, $x \in IJ$ car $a \in I$ et $bm \in J$.
Finalement, $IJ = ab\mathbb{Z}$ qui est un idéal.

2 On pose $I = 2\mathbb{Z}$ et $J = 3\mathbb{Z}$. L'ensemble $I \cup J$ est l'ensemble des éléments divisibles par 2 ou par 3. De ce fait, $2 \in I \cup J$ et $3 \in I \cup J$ mais $2 + 3 = 5 \notin I \cup J$. Donc $I \cup J$ n'est pas un idéal de $\mathbb{Z}$ car ce n'est pas un sous-groupe de $(\mathbb{Z}, +)$.

EXERCICE 5.2

1 On veut montrer que $\sqrt{I}$ est un idéal. On remarque d'abord que $\sqrt{I}$ est non vide car I est non vide et $I \subset \sqrt{I}$ (il suffit de prendre $n = 1$ dans la définition de $\sqrt{I}$).
Soit x, y dans $\sqrt{I}$, par définition il existe n_x et n_y des entiers naturels non nuls tels que $x^{n_x} \in I$ et $y^{n_y} \in I$. On peut poser N le maximum de n_x et de n_y de telle sorte que x^N et y^N appartiennent à I. On calcule alors à l'aide de la formule du binôme de Newton :

$$(x-y)^{2N} = \sum_{k=0}^{2N} (-1)^{2N-k} \binom{2N}{k} x^k y^{2N-k}$$

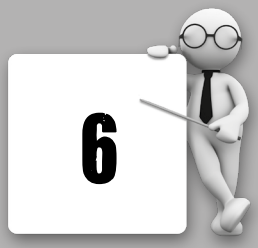
Si $k \geq N$, comme $x^N \in I$ alors $x^k = x^N x^{k-N} \in I$ puisque I est un idéal. Finalement, $\binom{2N}{k} x^k y^{2N-k}$ appartient à I. Par contre, si $k < N$ alors $2N - k \geq N$ et donc, en procédant de même, $y^{2N-k} \in I$ donc $\binom{2N}{k} x^k y^{2N-k} \in I$.
On en déduit que tous les termes de la somme appartiennent à I, donc $(x-y)^{2N} \in I$ ce qui implique que $(x-y) \in \sqrt{I}$. Donc $\sqrt{I}$ est un sous-groupe de $(A, +)$.
Soit $x \in \sqrt{I}$ et $a \in A$, il existe un entier naturel n non nul tel que $x^n \in I$, dès lors, en utilisant le fait que I est un idéal, $(ax)^n = a^n x^n \in I$ et donc $ax \in \sqrt{I}$.
Finalement, $\sqrt{I}$ est un idéal.

2 Il suffit de voir que $I = \{0\}$ est un idéal et que $N = \sqrt{I}$.

3 Soit $x \in \mathbb{Z}$ supposé non nul, on peut décomposer x en produit de facteurs premiers : $x = \pm \prod_{i=1}^{d} p_i^{\alpha_i}$, où $p_1, \ldots, p_d$ sont des nombres premiers (si $x = \pm 1$ on prend $d = 0$).
Dès lors, pour tout entier $n \in \mathbb{N}^*$,

$$x^n = \pm \prod_{i=1}^{d} p_i^{n\alpha_i}$$

On cherche des conditions pour qu'il existe un entier n tel que 18 divise x^n. Comme $18 = 2 \times 3^2$, il suffit que les nombres premiers 2 et 3 apparaissent dans la factorisation en facteurs premiers de x car dans ce cas, 18 divise x^2. On en déduit que $\sqrt{18\mathbb{Z}} = 6\mathbb{Z}$.



6 Faire des calculs dans Z/nZ

Quand on ne sait pas !

Soit n un entier strictement supérieur à 1.

- Les opérations de $\mathbb{Z}$ permettent de définir des opérations sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes de congruences modulo n. Cela signifie que si x et y sont deux classes de congruences modulo n et si x_1, x_2 sont des représentants de x cet y_1, y_2 des représentants de y c'est-à-dire que x_1 est congru à x_2 et y_1 est congru à y_2 modulo n alors $x_1 + y_1$ et $x_2 + y_2$ ont la même classe de congruence modulo n. De même $x_1 \times y_1$ et $x_2 \times y_2$ ont la même classe.
- L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni des deux opérations $+$ et $\times$ a une structure d'anneau commutatif.
- Soit $m \in \mathbb{Z}$, la classe de m est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si n et m sont premiers entre eux. En particulier, il y a $\varphi(n)$ éléments inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ où φ est la fonction indicatrice d'Euler.
- Dans le cas où p est un nombre premier (et uniquement dans ce cas), $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps.

Afin de faire la différence entre les éléments de $\mathbb{Z}$ et ceux de $\mathbb{Z}/n\mathbb{Z}$ on notera pour $x \in \mathbb{Z}$, $\dot{x}$ la classe de x dans $\mathbb{Z}/n\mathbb{Z}$ de sorte que si, par exemple, $n = 11$, alors $\dot{3} = \dot{25} = \dot{(-8)}$.
On représentera souvent une classe de $\mathbb{Z}/n\mathbb{Z}$ par son unique représentant compris entre 0 et $n - 1$.

Que faire ?

- Pour calculer dans $\mathbb{Z}/n\mathbb{Z}$ on peut le plus souvent prendre des représentants pour les classes, faire l'opération dans $\mathbb{Z}$ et prendre la classe du résultat du calcul.

  EXEMPLE 1 On fixe $n = 14$. On veut calculer $f(x) = \dot{7}x^2 + \dot{3}$ pour $x = \dot{6}$. On fait le calcul dans $\mathbb{Z}$ en calculant $7 \times 6^2 + 3 = 7 \times 2 \times 3 \times 6 + 3 = 14 \times 18 + 3$. On a donc $f(x) = \dot{3}$.
- Pour calculer des puissances dans $\mathbb{Z}/n\mathbb{Z}$ on peut utiliser le fait que le groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un groupe fini et donc, que tout élément est d'ordre fini (divisant l'ordre du groupe d'après le théorème de Lagrange).

EXEMPLE 2 On fixe $n = 7$. On veut calculer $(\dot{5})^{2000}$. On peut calculer les première puissances de $x = 5$:

k	1	2	3	4	5	6
x^k	$\dot{5}$	$\dot{4}$	$\dot{6}$	$\dot{2}$	$\dot{3}$	$\dot{1}$

On voit donc que $x^6 = \dot{1}$.
Il reste alors à faire la division euclidienne de 2000 par 6 : $2000 = 333 \times 6 + 2$. On obtient

$$x^{2000} = (x^6)^{333} \times x^2 = \dot{1} \times (\dot{5})^2 = \dot{4}.$$

Conseils

- L'ensemble $\mathbb{Z}/n\mathbb{Z}$ a n éléments. Dans le cas où n est petit on peut essayer de faire des calculs sur certaines, voire toutes les valeurs possibles.
- Il peut être intéressant d'utiliser le lemme chinois pour ramener les calculs dans $\mathbb{Z}/n\mathbb{Z}$ à des calculs dans $\mathbb{Z}/m\mathbb{Z}$ où $m < n$. Voir la fiche 7.

Exemple traité

On considère l'équation

$$x^2 - \dot{6}x + \dot{7} = \dot{0}$$

1 Montrer que pour tout $a \in \mathbb{Z}/11\mathbb{Z}$, $a^2 \neq \dot{2}$. En déduire que l'équation n'a pas de solutions dans $\mathbb{Z}/11\mathbb{Z}$.

2 Résoudre l'équation dans $\mathbb{Z}/17\mathbb{Z}$.

SOLUTION

1 Les éléments de $\mathbb{Z}/11\mathbb{Z}$ peuvent se noter $\{\dot{0}, \dot{1}, \dot{2}, \ldots, \dot{10}\}$ ou $\{\dot{0}, \dot{1}, -\dot{1}, \dot{2}, -\dot{2}, \ldots, \dot{5}, -\dot{5}\}$.
On calcule alors les carrés de ces éléments :

x	$\dot{0}$	$\pm\dot{1}$	$\pm\dot{2}$	$\pm\dot{3}$	$\pm\dot{4}$	$\pm\dot{5}$
x^2	$\dot{0}$	$\dot{1}$	$\dot{4}$	$\dot{9}$	$\dot{5}$	$\dot{3}$

On voit que si a appartient à $\mathbb{Z}/11\mathbb{Z}$, $a^2 \neq \dot{2}$.
On procède alors à une mise sous forme canonique,

$$x^2 - \dot{6}x + \dot{7} = (x - \dot{3})^2 - \dot{9} + \dot{7} = (x - \dot{3})^2 - \dot{2}$$

On a finalement

$$x^2 - \dot{6}x + \dot{7} = 0 \iff (x - \dot{3})^2 - \dot{2} = \dot{0} \iff (x - \dot{3})^2 = \dot{2}$$

D'après ce qui précède, cette équation n'a donc aucune solution.

2 Comme ci-dessus,

$$x^2 - \dot{6}x + \dot{7} = (x - \dot{3})^2 - \dot{9} + \dot{7} = (x - \dot{3})^2 - \dot{2}$$

On cherche alors dans $\mathbb{Z}/17\mathbb{Z}$ les éléments a tel que $a^2 = \dot{2}$. Les éléments de $\mathbb{Z}/17\mathbb{Z}$ peuvent se noter $\{\dot{0}, \dot{1}, \dot{2}, \ldots, \dot{16}\}$ ou $\{\dot{0}, \dot{1}, -\dot{1}, \dot{2}, -\dot{2}, \ldots, \dot{8}, -\dot{8}\}$.
On calcule alors les carrés de ces éléments :

x	$\dot{0}$	$\pm\dot{1}$	$\pm\dot{2}$	$\pm\dot{3}$	$\pm\dot{4}$	$\pm\dot{5}$	$\pm\dot{6}$	$\pm\dot{7}$	$\pm\dot{8}$
x^2	$\dot{0}$	$\dot{1}$	$\dot{4}$	$\dot{9}$	$\dot{16}$	$\dot{8}$	$\dot{2}$	$\dot{15}$	$\dot{13}$

On a finalement

$$\begin{aligned} x^2 - \dot{6}x + 7 = 0 &\iff (x - \dot{3})^2 - \dot{2} = \dot{0} \\ &\iff (x - \dot{3})^2 = \dot{2} \\ &\iff x - \dot{3} = \pm\dot{6} \\ &\iff x = \dot{9} \text{ ou } x = -\dot{3} = \dot{14} \end{aligned}$$

Exercices

EXERCICE 6.1

On considère $\mathbb{Z}/26\mathbb{Z}$.

1 Combien il y a-t-il d'éléments inversibles dans $\mathbb{Z}/26\mathbb{Z}$?

2 Justifier que $\dot{7}$ est inversible et calculer son inverse dans $\mathbb{Z}/26\mathbb{Z}$.

Pour vous aider à démarrer

EXERCICE 6.1

1 On pourra utiliser l'indicatrice d'Euler.

2 On pourra chercher à calculer, après avoir justifié leur existence, des entiers u et v tels que $26u + 7v = 1$.

Solutions des exercices

EXERCICE 6.1

1 D'après le cours, le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$ est $\varphi(n)$ où φ est la fonction indicatrice d'Euler. Or

$$\varphi(26) = \varphi(2 \times 13) = \varphi(2) \times \varphi(13) = 1 \times 12 = 12$$

Il y a 12 éléments inversibles dans $\mathbb{Z}/26\mathbb{Z}$.

2 Comme 7 est premier avec 26, $\dot{7}$ est inversible dans $\mathbb{Z}/26\mathbb{Z}$.
On sait alors qu'il existe une relation de Bézout de la forme $26u + 7v = 1$ avec u et v dans $\mathbb{Z}$. Pour les déterminer on met en place l'algorithme d'Euclide étendu. On commence avec les deux relations suivantes :

$$26 \times 1 + 7 \times 0 = 26 \qquad (L_1)$$

$$26 \times 0 + 7 \times 1 = 7 \qquad (L_2)$$

Par division euclidienne, $26 = 3 \times 7 + 5$ ce qui s'écrit aussi $5 = 1 \times 26 - 3 \times 7$. On réalise alors la combinaison linéaire $1 \times L_1 - 3 \times L_2$ et on obtient

$$26 \times 1 + 7 \times (-3) = 5 \qquad (L_3)$$

Maintenant, $7 = 1 \times 5 + 2$ ce qui s'écrit aussi $2 = 1 \times 7 - 1 \times 5$. On réalise alors la combinaison linéaire $1 \times L_2 - 1 \times L_3$ et on obtient

$$26 \times (-1) + 7 \times 4 = 2 \qquad (L_4)$$

En utilisant le fait que $5 = 2 \times 2 + 1$ ce qui s'écrit aussi $1 = 1 \times 5 - 2 \times 2$. On réalise alors la combinaison linéaire $1 \times L_3 - 2 \times L_4$ et on obtient

$$26 \times 3 + 7 \times (-11) = 1 \qquad (L_5)$$

On en déduit, en prenant les classes de congruences modulo 26 que $\dot{7} \times (\dot{-11}) = \dot{1}$ donc $(\dot{-11}) = \dot{15}$ est l'inverse de $\dot{7}$ dans $\mathbb{Z}/26\mathbb{Z}$.



7 Utiliser le théorème chinois

Quand on ne sait pas !

Soit n et m deux entiers premiers entre eux, l'application naturelle de $\mathbb{Z}/(nm)\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est un isomorphisme d'anneau

L'application est définie en associant à la classe modulo nm d'un entier x le couple $(\dot{x}, \overline{x})$ où $\dot{x}$ est la classe de x modulo n et $\overline{x}$ est la classe de x modulo m.

Que faire ?

Soit n et m deux entiers premiers entre eux, on utilise souvent le théorème chinois pour, chercher les entiers relatifs x tels que

$$\left\{ \begin{array}{rcl} x & = & a\,[n] \\ x & = & b\,[m] \end{array} \right.$$

où a et b sont des entiers fixés.
Le théorème chinois affirme qu'il y a toujours des solutions et que l'ensemble des solutions est une unique classe de congruence modulo nm.

EXEMPLE 1

On cherche les entiers x tels que

$$\left\{ \begin{array}{rcl} x & = & 0\,[7] \\ x & = & 2\,[5] \end{array} \right.$$

Il est clair que 7 est une solution. Comme 5 et 7 sont premiers entre eux, l'ensemble des solutions est la classe de 7 modulo 35. On a donc

$$S = \{7 + 35k\ ,\ k \in \mathbb{Z}\}$$

Conseils

- Il est important de vérifier que n et m soient premiers entre eux.

- Dans l'exemple ci-dessus, il était simple de trouver une solution particulière, dans le cas général, on peut commencer, en utilisant la relation de Bézout, par déterminer des entiers x_1 et x_2 vérifiant les systèmes :

$$\begin{cases} x_1 &= 1\,[n] \\ x_1 &= 0\,[m] \end{cases} \quad ; \quad \begin{cases} x_2 &= 0\,[n] \\ x_2 &= 1\,[m] \end{cases}$$

On peut alors conclure par linéarité. Cela va être illustré dans l'exemple ci-dessous.

Exemple traité

On cherche les entiers x tels que

$$\begin{cases} x &= 4\,[22] \\ x &= 2\,[13] \end{cases}$$

1 Déterminer des entiers u et v tels que $22u + 13v = 1$.

2 En déduire des entiers x_1 et x_2 tels que

$$\begin{cases} x_1 &= 1\,[22] \\ x_1 &= 0\,[13] \end{cases} \quad \text{et} \quad \begin{cases} x_2 &= 0\,[22] \\ x_2 &= 1\,[13] \end{cases}$$

3 Résoudre l'équation initiale.

SOLUTION

1 On applique l'algorithme d'Euclide étendu. On sait que

$$22 \times 1 + 13 \times 0 = 22 \qquad (\mathrm{L}_1)$$

$$22 \times 0 + 13 \times 1 = 13 \qquad (\mathrm{L}_2)$$

Par division euclidienne, $22 = 1 \times 13 + 9$ ce qui s'écrit aussi $9 = 1 \times 22 - 1 \times 13$. On réalise alors la combinaison linéaire $1 \times \mathrm{L}_1 - 1 \times \mathrm{L}_2$ et on obtient

$$22 \times 1 + 13 \times (-1) = 9 \qquad (\mathrm{L}_3)$$

Maintenant, $13 = 1 \times 9 + 4$ ce qui s'écrit aussi $4 = 1 \times 13 - 1 \times 9$. On réalise alors la combinaison linéaire $1 \times \mathrm{L}_2 - 1 \times \mathrm{L}_3$ et on obtient

$$22 \times (-1) + 13 \times 2 = 4 \qquad (\mathrm{L}_4)$$

En utilisant le fait que $9 = 2 \times 4 + 1$ ce qui s'écrit aussi $1 = 1 \times 9 - 2 \times 4$. On réalise alors la combinaison linéaire $1 \times \mathrm{L}_3 - 2 \times \mathrm{L}_4$ et on obtient

$$22 \times 3 + 13 \times (-5) = 1 \qquad (\mathrm{L}_5)$$

On peut poser $u = 3$ et $v = -5$.

2 L'égalité L_5 affirme que si on pose $x_1 = -5 \times 13 = -65$ et $x_2 = 3 \times 22 = 66$ alors

$$\begin{cases} x_1 &= 1\,[22] \\ x_1 &= 0\,[13] \end{cases} \quad \text{et} \quad \begin{cases} x_2 &= 0\,[22] \\ x_2 &= 1\,[13] \end{cases}$$

3 On pose maintenant $x = 4 \times x_1 + 2 \times x_2 = -128$. Par linéarité, c'est une solution de notre équation.

On peut conclure en utilisant le théorème chinois, on sait que l'ensemble des solutions est une classe de congruence modulo $13 \times 22 = 286$. On en déduit que l'ensemble des solutions est

$$S = \{-128 + 286k\ ,\ k \in \mathbb{Z}\} = \{158 + 286k\ ,\ k \in \mathbb{Z}\}$$

Exercices

EXERCICE 7.1

On veut déterminer les entiers x tels que

$$(S) \quad \begin{cases} x &= 1\,[3] \\ x &= 3\,[5] \\ x &= 4\,[7] \end{cases}$$

1 Justifier que le système considéré est équivalent au système

$$(S') \quad \begin{cases} x &= 13\,[15] \\ x &= 4\,[7] \end{cases}$$

2 Résoudre le système.

Pour vous aider à démarrer

EXERCICE 7.1

1 Il suffit de résoudre le système composé des deux premières équations. Ici, il suffit de vérifier que la solution donnée convient.

2 Il suffit d'appliquer la méthode.

EXERCICE 7.1

1 Comme 3 et 5 sont premiers entre eux, d'après le théorème chinois, il existe un élément a dans $\mathbb{Z}$ (défini modulo 15) tel que

$$\left\{ \begin{array}{rcl} x & = & 1\,[3] \\ x & = & 3\,[5] \end{array} \right. \iff x = a[15]$$

Il suffit de vérifier que 13 est bien congru à 1 modulo 3 et à 3 modulo 5 pour conclure que les deux systèmes (S) et (S') sont effectivement équivalents.

2 On applique la méthode précédente au système (S'). C'est possible car 15 et 7 sont premiers entre eux. On cherche des entiers u et v tels que $15u + 7v = 1$. Il n'est pas nécessaire ici d'écrire l'algorithme d'Euclide étendu, $u = 1$ et $v = -2$ conviennent. On en déduit que $x_1 = 15$ et $x_2 = -14$ vérifient

$$\left\{ \begin{array}{rcl} x_1 & = & 1\,[7] \\ x_1 & = & 0\,[15] \end{array} \right. \text{ et } \left\{ \begin{array}{rcl} x_2 & = & 0\,[7] \\ x_2 & = & 1\,[15] \end{array} \right.$$

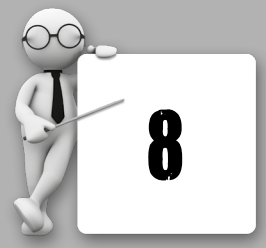
Par linéarité, $x = 13x_2 + 4x_1 = -122$ vérifie le système (S') et donc aussi le système (S). Finalement l'ensemble des solutions est

$$\{-122 + 105k\ ,\ k \in \mathbb{Z}\} = \{88 + 105k\ ,\ k \in \mathbb{Z}\}$$

Algèbre linéaire



Montrer qu'une somme est directe



Quand on ne sait pas !

Soit $p \geq 2$ et $F_1, \cdots, F_p$ des sous-espaces vectoriels d'un espace vectoriel E.

- **(Définition d'une somme directe)**

$$\left[\begin{array}{c}\text{La somme } \displaystyle\sum_{k=1}^{p} F_k \text{ est directe} \\ \text{et l'on note } \displaystyle\bigoplus_{k=1}^{p} F_k\end{array}\right] \iff \left[\begin{array}{c}\text{La décomposition de tout vecteur de } \displaystyle\sum_{k=1}^{p} F_k \\ \text{sous la forme } \displaystyle\sum_{k=1}^{p} u_k, \text{ avec } u_k \in F_k, \text{ est unique}\end{array}\right]$$

On dit alors que les sous-espaces $F_1, \cdots, F_p$ sont en somme directe.

- **(Caractérisation 1)**

$$\text{La somme } \sum_{k=1}^{p} F_k \text{ est directe} \iff \left[\begin{array}{c}\text{Si } 0_E = \displaystyle\sum_{k=1}^{p} u_k \text{ avec } u_k \in F_k, \\ \text{alors tous les } u_k \text{ sont nuls}\end{array}\right]$$

- **(Caractérisation 2)**

$$\text{La somme } \sum_{k=1}^{p} F_k \text{ est directe} \iff \left[\begin{array}{c}\mathscr{B} = (\mathscr{B}_1, \cdots, \mathscr{B}_p) \text{ est une base de } \displaystyle\sum_{k=1}^{p} F_k \\ \text{où les } \mathscr{B}_k \text{ sont des bases de } F_k\end{array}\right]$$

- **(Caractérisation 3 - en dimension finie)**
On suppose de plus que $F_1, \cdots, F_p$ sont de dimension finie.

$$\text{La somme } \sum_{k=1}^{p} F_k \text{ est directe} \iff \dim\left(\sum_{k=1}^{p} F_k\right) = \sum_{k=1}^{p} \dim F_k$$

- **(Cas particulier important : $p = 2$)**

$$\text{La somme } F_1 + F_2 \text{ est directe} \iff F_1 \cap F_2 = \{0_E\}$$

Que faire ?

- Pour montrer que les sous-espaces $F_1, \cdots, F_p$ sont en somme directe, on peut utiliser une des méthodes suivantes :
  - **Méthode 1 (en utilisant la caractérisation 1)**
    on suppose que $u_1 + \cdots + u_p = 0_E$ avec $u_k \in F_k$ pour tout $k \in [\![1, p]\!]$, puis on exploite les propriétés des F_k pour montrer que tous les u_k sont nuls.
  - **Méthode 2 (en utilisant la caractérisation 2)**
    on commence par déterminer une base $\mathscr{B}_k$ de F_k pour tout $k \in [\![1, p]\!]$, puis on montre que la famille concaténée $\mathscr{B} = (\mathscr{B}_1, \cdots, \mathscr{B}_p)$ est une base de la somme $F_1 + \cdots + F_p$.
  - **Méthode 3 (en utilisant la caractérisation 3 - valable en dimension finie)**
    on montre que la dimension de la somme des F_k est égale à la somme des dimensions des F_k.
  - **Méthode 4 (uniquement si $p = 2$)**
    on montre que l'intersection $F_1 \cap F_2$ est nulle.
    Dans le cas où $p \geq 3$, ce résultat ne se généralise pas aisément (cf exercice 1).

Conseils

- En pratique, on privilégie les méthodes 1 et 4 pour montrer qu'une somme est directe.
  La méthode 4 est illustrée dans la fiche 10 sur les sous-espaces supplémentaires.
  Les méthodes 1 à 3 sont comparativement illustrées dans la rubrique *Exemple traité*.

Exemple traité

Soit $Q \in \mathbb{K}[X]$ non nul et $p \in \mathbb{N}^*$. Pour tout $k \in [\![1, p]\!]$, on pose $F_k = \text{Vect}(X^k Q)$.
Montrer que les sous-espaces $F_1, \cdots, F_p$ sont en somme directe.

SOLUTION

- **Méthode 1 (en utilisant la caractérisation 1)**
  Soit $(R_1, \cdots, R_p) \in F_1 \times \cdots \times F_p$ tel que $R_1 + \cdots + R_p = 0_{\mathbb{K}[X]} \quad (\star)$.
  Montrons que $R_1 = \cdots = R_p = 0_{\mathbb{K}[X]}$.
  Pour tout $k \in [\![1, p]\!]$, comme $R_k \in F_k$, il existe un scalaire λ_k tel que $R_k = \lambda_k (X^k Q)$.
  On en déduit alors les équivalences suivantes :

$$(\star) \iff \lambda_1 XQ + \lambda_2 X^2 Q + \cdots + \lambda_p X^p Q = 0_{\mathbb{K}[X]} \underset{Q \neq 0_{\mathbb{K}[X]}}{\iff} \lambda_1 X + \lambda_2 X^2 + \cdots + \lambda_p X^p = 0_{\mathbb{K}[X]}$$

  Or la famille $(X^k)_{k \in [\![1,p]\!]}$ est libre, donc tous les λ_k sont nuls, a fortiori les R_k aussi.

- **Méthode 2 (en utilisant la caractérisation 2)**
  Pour tout $k \in [\![1, p]\!]$, la famille $\mathscr{B}_k = (X^k Q)$ est génératrice de F_k et est libre (car

constituée d'un seul vecteur non nul), donc est une base de F_k. Par ailleurs,

$$\sum_{k=1}^{p} F_k = \sum_{k=1}^{p} \text{Vect}(X^k Q) = \text{Vect}((X^k Q)_{k\in[\![1,p]\!]})$$

La famille concaténée $\mathscr{B} = (X^k Q)_{k\in[\![1,p]\!]}$ est génératrice de $F_1 + \cdots + F_p$ et est libre (car constituée de polynômes non nuls de degrés échelonnés), donc est bien une base de $F_1 + \cdots + F_p$.

- **Méthode 3 (en utilisant la caractérisation 3 - valable en dimension finie)**
Pour tout $k \in [\![1, p]\!]$, $\dim F_k = \text{rg}(X^k Q) = 1$ (car Q est non nul). Par ailleurs,

$$\sum_{k=1}^{p} F_k = \sum_{k=1}^{p} \text{Vect}(X^k Q) = \text{Vect}((X^k Q)_{k\in[\![1,p]\!]}), \text{ d'où : } \dim(\sum_{k=1}^{p} F_k) = \text{rg}((X^k Q)_{k\in[\![1,p]\!]})$$

Or la famille $(X^k Q)_{k\in[\![1,p]\!]}$ est constituée de polynômes non nuls de degrés échelonnés donc est libre, d'où :

$$\dim(\sum_{k=1}^{p} F_k) = \text{rg}((X^k Q)_{k\in[\![1,p]\!]}) = \text{Card}((X^k Q)_{k\in[\![1,p]\!]}) = p = \sum_{k=1}^{p} \dim F_k$$

Exercices

EXERCICE 8.1

Soit $p \geq 3$ et $F_1, \cdots, F_p$ des sous-espaces vectoriels d'un espace vectoriel E.

1 On suppose que $F_1 \cap F_2 = \{0_E\}$, $F_1 \cap F_3 = \{0_E\}$ et $F_2 \cap F_3 = \{0_E\}$.
Les sous-espaces F_1, F_2 et F_3 sont-ils nécessairement en somme directe ?

2 Montrer l'équivalence suivante :

$$\text{la somme } \sum_{k=1}^{p} F_k \text{ est directe} \iff \forall k \in [\![1, p-1]\!],\ (\sum_{i=1}^{k} F_i) \cap F_{k+1} = \{0_E\}$$

Pour vous aider à démarrer

EXERCICE 8.1

1 Considérer trois droites judicieusement choisies de $E = \mathbb{R}^3$.

2 Utiliser la méthode 2 pour l'implication $\Leftarrow$.

EXERCICE 8.1

1 Considérons trois droites coplanaires et deux à deux distinctes de $E = \mathbb{R}^3$.

$$F_1 = \text{Vect}((1,0,0)) \quad \text{et} \quad F_2 = \text{Vect}((0,1,0)) \quad \text{et} \quad F_3 = \text{Vect}((1,1,0))$$

Ces trois espaces sont bien deux à deux en somme directe (car d'intersection deux à deux nulle). Par contre, ils ne sont pas en somme directe. En effet :

$$0_{\mathbb{R}^3} = \underbrace{(-1,0,0)}_{\in F_1} + \underbrace{(0,-1,0)}_{\in F_2} + \underbrace{(1,1,0)}_{\in F_3}$$

Ainsi, des sous-espaces qui sont deux à deux d'intersection nulle ne sont pas nécessairement en somme directe.

2 Montrons la double implication :

(⇒) Supposons que la somme $F_1 + \cdots + F_p$ est directe.
Soit $k \in [\![1, p-1]\!]$. Montrons l'égalité ensembliste demandée.

(⊃) Cette inclusion est toujours vraie car une intersection d'espaces vectoriels est un espace vectoriel, donc contient l'élément neutre 0_E.

(⊂) Soit $u \in \left(\sum_{i=1}^{k} F_i\right) \cap F_{k+1}$ i.e. $\begin{cases} \exists (u_1, \cdots, u_k) \in F_1 \times \cdots \times F_k,\ u = u_1 + \cdots + u_k \\ u \in F_{k+1} \end{cases}$
On en déduit l'égalité vectorielle suivante :

$$\underbrace{u_1}_{\in F_1} + \cdots + \underbrace{u_k}_{\in F_k} + \underbrace{(-u)}_{\in F_{k+1}} + \underbrace{0_E}_{\in F_{k+2}} + \cdots + \underbrace{0_E}_{\in F_p} = 0_E$$

Or la somme $F_1 + \cdots + F_p$ est directe, d'où $u_1 = \cdots = u_k = -u = 0_E$.
En particulier, $u = 0_E$.

(⇐) Supposons $\left(\sum_{i=1}^{k} F_i\right) \cap F_{k+1} = \{0_E\}$ pour tout $k \in [\![1, p-1]\!]$.
Montrons que la somme $F_1 + \cdots + F_p$ est directe.
Soit $(u_1, \cdots, u_p) \in F_1 \times \cdots \times F_p$ tel que $u_1 + \cdots + u_p = 0_E$.
On a alors l'équivalence suivante :

$$u_1 + \cdots + u_p = 0_E \iff \underbrace{u_1 + \cdots + u_{p-1}}_{\in F_1 + \cdots + F_{p-1}} = \underbrace{-u_p}_{\in F_p}$$

D'où $u_1 + \cdots + u_{p-1} = -u_p \in (F_1 + \cdots + F_{p-1}) \cap F_p = \{0_E\}$, et on en déduit alors que $u_1 + \cdots + u_{p-1} = u_p = 0_E$.
Sachant que $u_1 + \cdots + u_{p-1} = 0_E$ et $(F_1 + \cdots + F_{p-2}) \cap F_{p-1} = \{0_E\}$, on montre par un raisonnement analogue au précédent que $u_{p-1} = 0_E$.
De proche en proche, on montre que tous les u_k sont nuls.

Ainsi, on a bien montré l'équivalence souhaitée.

Montrer que des sous-espaces sont supplémentaires en dimension quelconque



Quand on ne sait pas !

Soit F et G deux sous-espaces vectoriels d'un $\mathbb{K}$-espace vectoriel E (avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$).

- **(Définition de la supplémentarité)**

$$\left[\ F \text{ et } G \text{ sont supplémentaires dans } E\ \right]$$

$$\Updownarrow$$

$$\left[\begin{array}{c} E = F \oplus G, \text{ c'est-à-dire tout vecteur } u \in E \\ \text{se décompose de manière unique comme la somme} \\ \text{d'un vecteur } u_F \text{ de } F \text{ et d'un vecteur } u_G \text{ de } G \end{array}\right]$$

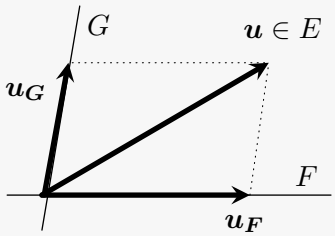


Figure illustrative

On dit aussi que F est UN supplémentaire de G dans E ou que G est UN supplémentaire de F dans E.

- **(Caractérisation de la supplémentarité)**

$$E = F \oplus G \iff \left\{\begin{array}{ll} E = F + G & \leftarrow \textit{garantit l'existence d'une décomposition} \\ F \cap G = \{0_E\} & \leftarrow \textit{garantit son unicité sous réserve d'existence} \end{array}\right.$$

- **(Supplémentarité des éléments caractéristiques d'un projecteur/d'une symétrie)**
  Soit p et s des endomorphismes de E.
  - Si p est un projecteur de E, alors : $E = \mathrm{Ker}(p) \oplus \mathrm{Im}(p)$.
  - Si s est une symétrie de E, alors : $E = \mathrm{Ker}(s - \mathrm{Id}_E) \oplus \mathrm{Ker}(s + \mathrm{Id}_E)$.